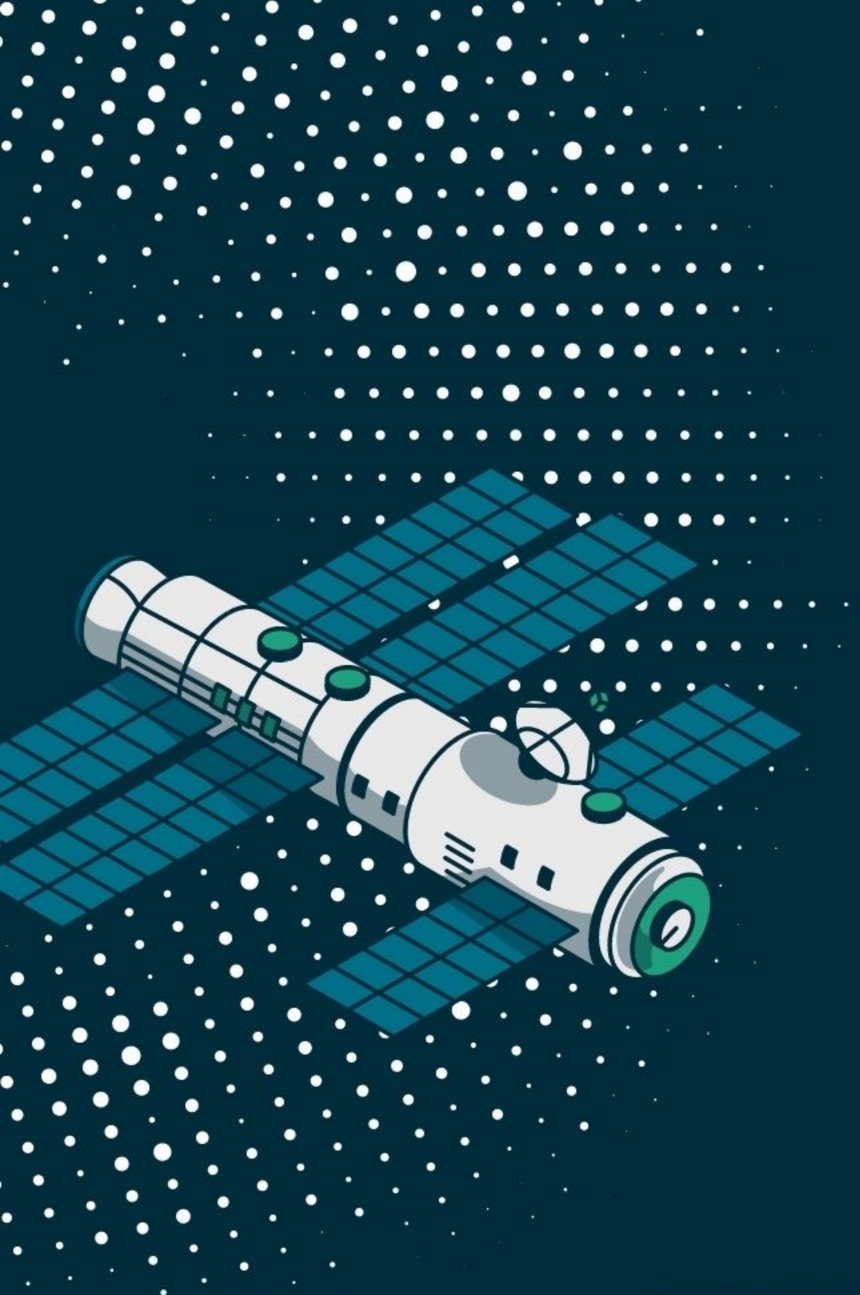
SPACE
ISAC

VALUE OF SPACE SUMMIT 2023

Co-hosted by AEROSPACE

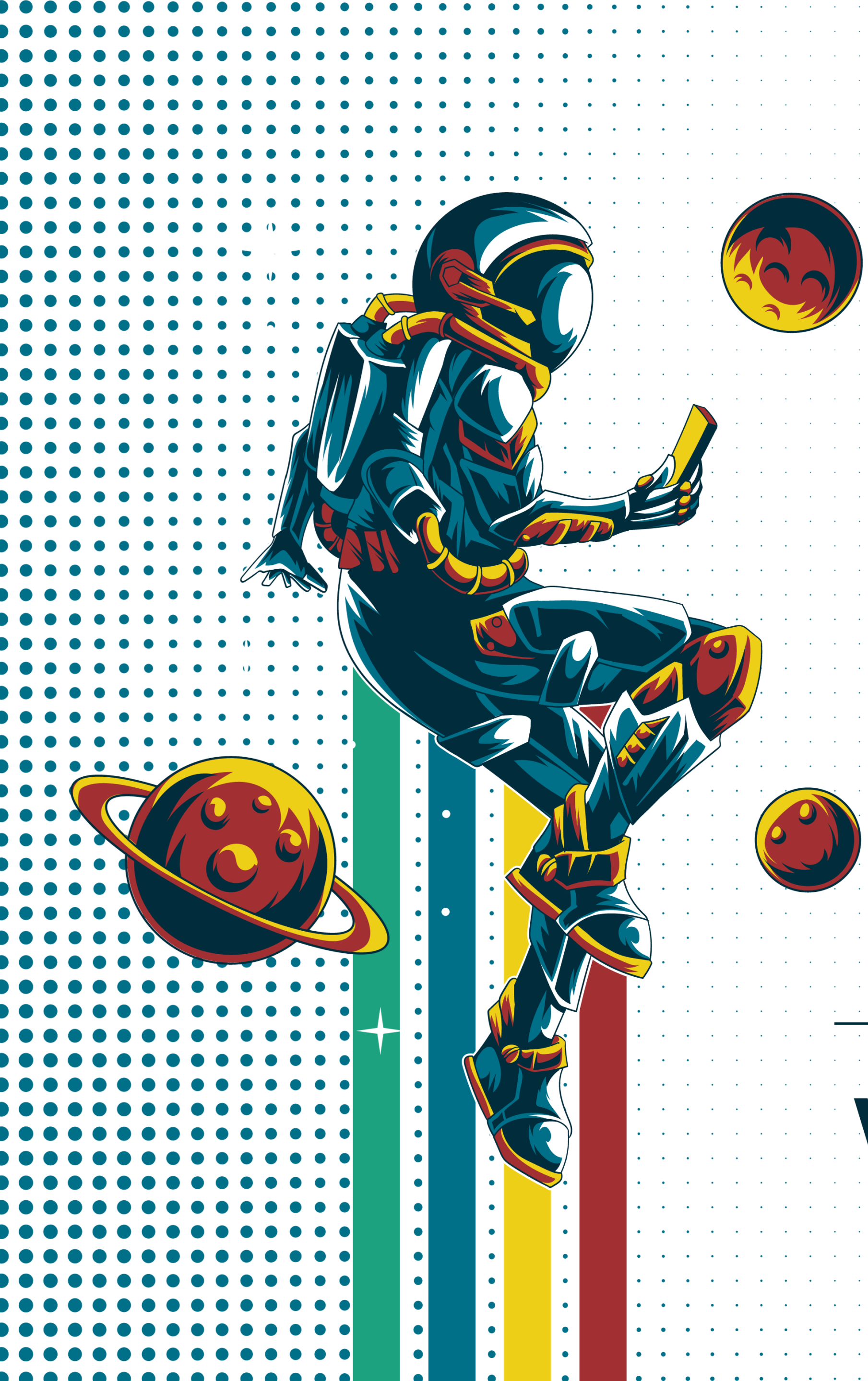
October 17 - 19, 2023
Colorado Springs, CO USA



"The Next Giant Leap: Building Cyber Resilience for the Global Space Industry"

This theme will explore the critical importance of cybersecurity in the rapidly advancing commercial space sector. Drawing parallels between the monumental technological advances that propelled humanity to the moon in the late 1960s and the current state of the space industry, this conference aims to shed light on the profound changes we are experiencing and the urgent need for cyber resilience in the space domain.

Venue Hosts: UCCS University of Colorado Colorado Springs KRATOS® READY FOR WHAT'S NEXT™ Booz | Allen | Hamilton®



WELCOME

SPACE ISAC

Co-hosted by

AEROSPACE

VALUE OF SPACE SUMMIT 2023

VALUE OF SPACE SUMMIT 2023

Sponsors

CYWARE™

KRATOS®
READY FOR WHAT'S NEXT™

Constellation

Deloitte.

RADICL
Nation State Threat Defense

ExoAnalytic
SOLUTIONS

RAPIDASCENT

thinklogical®
A BELDEN BRAND

Cyber Technical Keynote

Robert Metzger

Head of Washington Office

Rogers Joseph O'Donnell

Watch Center 2023 Trends Analysis and Presentation

Joel Francis, Watch Center Lead,

Space ISAC

SPACE ISAC

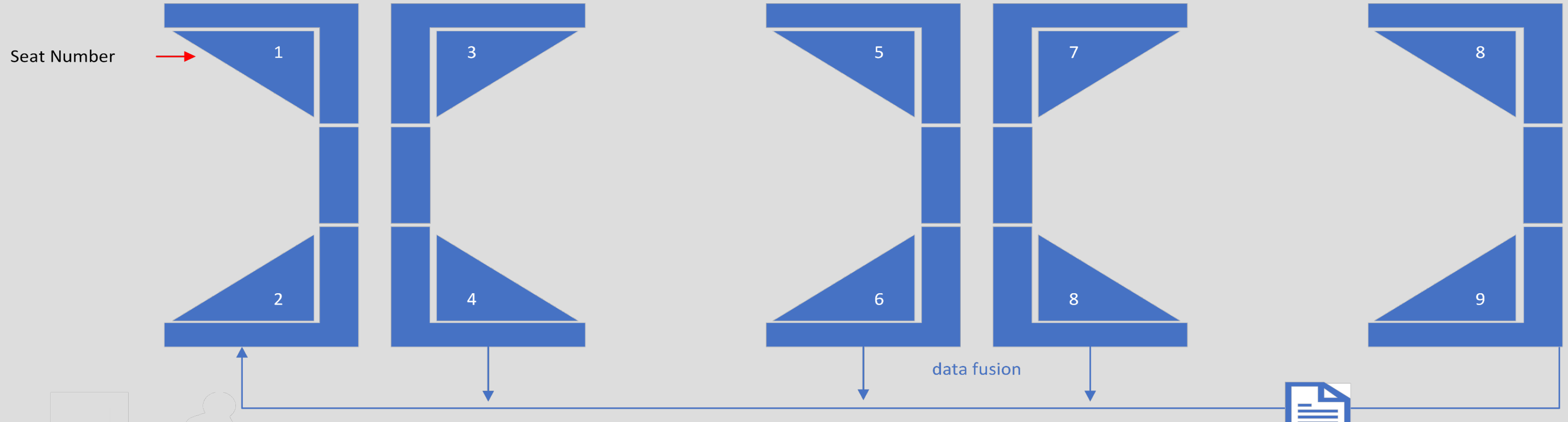
Space Information Sharing and Analysis Center

Watch Center 2023 Trends, Insights, and Observations

2023 Value of Space Summit – Technical Track

Watch Center Cell Functions and Overview

Tools	CSAP Member Portal Communication Tools: Email, Slack, Teams Threat Actor Tracking Matrix (TATM)	CSAP Member Portal Communication Tools Google Alerts HSIN TATM	CSAP Member Portal Communicaiton Tools CTIX (Threat Intel Platform)	CSAP Member Portal Communication Tools Spectrum Viewer Utility (SVU)	CSAP Member Portal Communications Tools RF COP
Scope and Emphasis (Primary and Secondary)	All-Source	Primary: All-Source Secondary: Cyber	Primary: Cyber Secondary: Signals	Primary: Signals Secondary: Space	Primary: Space Secondary: Multi-Domain
Duties and Responsibilities	Review/Approve Engagement Admin Report Curation WC COA	Monitor Track Report Correlate	Monitor Track Report Correlate	Monitor Track Report Correlate	Monitor Track Report Correlate
Threat Scenarios			Nation State Actors CTI Enrichment	RF EMI	Maneuvers
Cell Name	Coordination Cell	All-Source Cell	Terrestrial Cell	Signals Cell	Space Cell



Report correlation flows upward to Coordination Cell for approval

The Watch Center floor is organized by "cells" that correspond to **functional areas** related to use cases, tasking, and responsibilities.

The **Coordination cell** will be focused on facilitating communication between analysts and Space ISAC Members and approving reports.

There is a natural progression of physical and cyber analysis (All-Source) to Multi Domain Operations (MDO) including Signals and Space concepts.

Threat Assessments

CSIS Space Threat Assessment 2023

SPACE THREAT ASSESSMENT 2023

Authors
KARI A. BINGEN
KAITLYN JOHNSON
MAKENA YOUNG

Foreword
JOHN W. "JAY" RAYMOND

Key Takeaways:

- China has continued to grow space and counterspace assets
- Russia has continued to display less advanced capabilities
- Iran has built one of the largest space programs in the middle east
- North Korea has increased space activity, including ISR capabilities

NSSA – Strategic Implications of China's Cislunar Space Activities

NSSA

NATIONAL SECURITY SPACE ASSOCIATION

NATIONAL SECURITY SPACE ASSOCIATION
MOORMAN CENTER FOR SPACE STUDIES

Occasional Paper

Strategic Implications of China's Cislunar Space Activities

Key Takeaways:

- China seeks to supplant the US as the dominant power in space
- Competition has extended from near-earth orbits to cislunar and beyond
- Cislunar ambitions pose political, economic, and military implications
- The exploitation of outer space mirrors is integral to China's national strategy

Microsoft 2023 Digital Defense Report

Microsoft

Microsoft Digital Defense Report

Building and improving cyber resilience

October 2023
Microsoft Threat Intelligence

Key Takeaways:

- Threat actors leverage as-a-service offerings for phishing, identity theft and DDoS attacks
- Significant shift in cybercriminal tactics
- Russia has continued to display less advanced capabilities
- External remote services (RDP & VPNs) are among the most exploited vectors

FBI, NCSC, AFOSI - Safeguarding the US Space Industry

SAFEGUARDING THE US SPACE INDUSTRY

KEEPING YOUR INTELLECTUAL PROPERTY IN ORBIT

THREAT

According to US financial sector estimates, the global space economy is projected to grow from $469 billion in 2021 to more than $1 trillion by 2030. The United States is the main driver of this growth through its role as a global leader in space investment, research, innovation, and production. Space is fundamental to every aspect of our society, including emergency services, energy, financial services, telecommunications, transportation, and food and agriculture. All rely on space services to operate.

Foreign intelligence entities (FIEs) recognize the importance of the commercial space industry to the US economy and national security, including the growing dependence of critical infrastructure on space-based assets. They see US space-related innovation and assets as potential threats as well as valuable opportunities to acquire vital technologies and expertise. FIEs use cyberattacks, strategic investment (including joint ventures and acquisitions), the targeting of key supply chain nodes, and other techniques to gain access to the US space industry.

SPACE EQUITY INVESTMENT 2013-2023 (Q2)

IMPACT

FIE efforts to target and exploit the US space industry can harm US commercial firms and broader US national and economic security in several ways.

Global Competition

- Siphoning intellectual property and other proprietary data from US space firms for the benefit of foreign powers' national security programs.
- Leapfrogging innovation that costs US space firms substantial time and resources to generate.
- Using state-backed resources and unfair business practices to disadvantage US space firms.
- Harming US corporate reputations by proliferating counterfeit products or falsely authenticated reproductions.

National Security

- Collecting sensitive data related to satellite payloads.
- Disrupting and degrading US satellite communications, remote sensing, and imaging capabilities.

Key Takeaways:

- Foreign Intelligence Entities (FIEs) see US space industry as vital to Economy, National Security, and Global competition
- FIEs use cyberattacks, strategic investment, and supply chain exploits
- Indicators include cyber activity and collection tactics

Nation State Actors

- Nation State Actors represent the most dangerous threat to the commercial space industry.
- Cyber actors are funded by state governments to conduct targeted, malicious cyber campaigns
- State-sponsored cyber campaigns typically serve foreign intelligence and military objectives.
- Threat actors from China, Russia, Iran, and North Korea have demonstrated capability and intent to target space companies through a variety of methods.
- Motives are focused on establishing persistence and exfiltrating data for espionage and competitive advantage in the space sector – Living off the Land
- Distinguished from financially motivated groups

CHINA:

- China has doubled its number of satellites in orbit between 2019 and 2021
- Leverages cyber & counterspace capability to target US space sector and critical infrastructure
- China utilizes global investment (ex. BRI) to circumvent sanctions, grow global influence, and target the supply chain

RUSSIA:

- Russia maintains cyber and counterspace capabilities
- Threat actors use a diverse set of TTPs to disrupt organizations
- Cyber campaigns focused on NATO member countries and military support of Ukraine
- Several pro-Russian cybercrime groups have surfaced and routinely threaten the US defense and aerospace sectors

Ransomware and Hacktivism

Ransomware continues to be the leading category of cybercrime across all sectors. Threat groups have shifted to extortion-based tactics

- Increased collaboration among threat actor groups: affiliate programs, as-a-service offerings, and the sale of toolkits to enable brute force attacks
- AI/ML is being leveraged for use in cyber attacks to bolster phishing and BEC attacks
- Compromised accounts are weaponized and constitute one of the most common TTP used to gain initial access
- The majority of ransomware attacks target SMBs, manufacturing and supply chain
- Darkweb marketplaces and clear web forums provide opportunities to advertise and sell stolen data
- Majority of attributed ransomware activity tied to Chinese and Russian state sponsored cyber threat actors

Hacktivists and cybercrime groups routinely leverage DDoS and defacement attacks to target websites and external assets.

- While denial of service attacks are less damaging to organizations, these attacks can be carried out by less sophisticated cybercrime groups
- Disruptive cyber activity in relation to regional conflicts (Russia/Ukraine > Israel/Hamas)
- As-a-service offerings are becoming more prominent for DDoS kits and botnet subscriptions, providing capabilities without the need to maintain botnets

Ransomware:

Top Groups:

- Lockbit 3.0
- BlackBasta
- Royal Ransomware
- Akira
- BlackCat

On the Rise:

↑ 8Base
↑ NoEscape
↑ Cactus
↑ CL0P
↑ Play

Top Cybercrime Orgs:

- Lazarus
- Killnet / Killmilk
- Anonymous Sudan
- SeigedSec
- UserSec
- GhostSec
- Anonymous Russia
- REvil

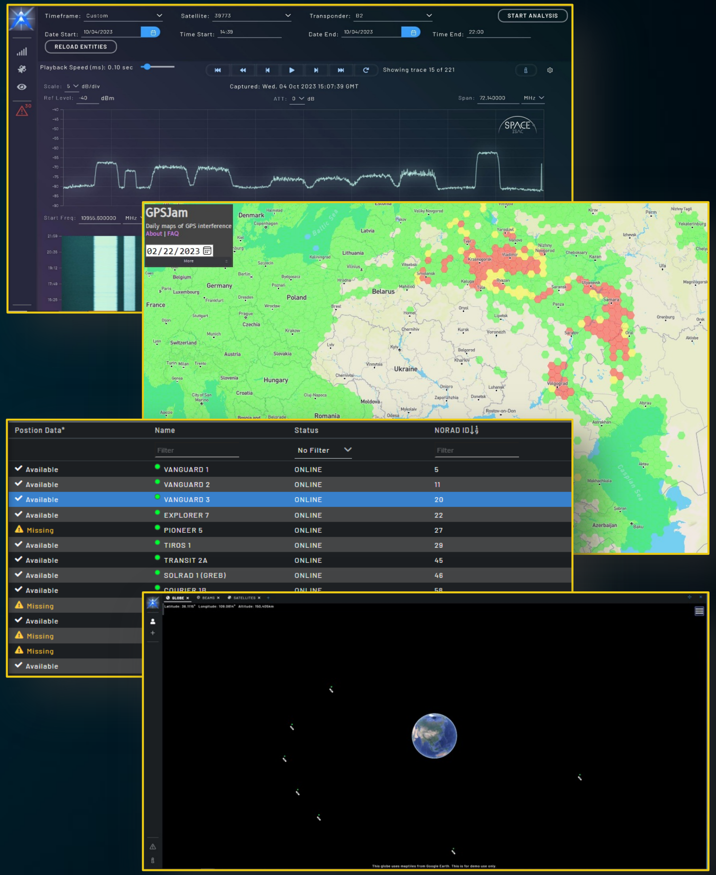
Signals and Space-Based Threats

Signals

- Consistent levels of interference in conflict areas, correlates to internet suppression
- Uptick in interference activities related to geopolitical conflicts (ex. Azerbaijan)
- Insights derived from FAA & ICAO NOTAMS – interference and 5G C-band testing
- Jamming activity near Baltic region, black sea observed from February – August 2023
- Verified uptick in GEO interference observations in October 2023

Space

- Increase in number of global launches, active satellites
- Uptick in Payload to Launch Ratio: '22 = 12.68 / '23 = 13.23
- Proliferation in LEO leading to an increase in conjunction assessment considerations
- Contested environments arise in Cislunar and VLEO
- Notice to Space Operators (NOTSOs) – Majority of maneuvers reported are from PRC owned assets.
- Satellites of interest include **41103** and **40258**
- Increased solar weather in relation to solar maximum, minor impacts to satellites



Timeframe: Custom
Satellite: 39773
Transponder: B2
Date Start: 10/04/2023
Time Start: 14:39
Date End: 10/04/2023
Time End: 22:00
Playback Speed (ms): 0.10 sec
Showing trace 15 of 221
Captured: Wed, 04 Oct 2023 15:07:39 GMT
Scale: 5 dB/div
Ref Level: -40 dBm
ATT: 0 dB
Span: 72.140000 MHz

Postion Data*	Name	Status	NORAD ID
	Filter	No Filter	Filter
✓ Available	VANGUARD 1	ONLINE	5
✓ Available	VANGUARD 2	ONLINE	11
✓ Available	VANGUARD 3	ONLINE	20
✓ Available	EXPLORER 7	ONLINE	22
⚠ Missing	PIONEER 5	ONLINE	27
✓ Available	TIROS 1	ONLINE	29
✓ Available	TRANSIT 2A	ONLINE	45
✓ Available	SOLRAD 1 (GREB)	ONLINE	46
✓ Available	COURIER 1B	ONLINE	58
⚠ Missing			
✓ Available			
⚠ Missing			
⚠ Missing			
✓ Available			

Latitude: 36.1115° Longitude: 109.0814° Altitude: 150,405km

Tactics, Techniques, and Procedures

INITIAL ACCESS

Valid Accounts

Exploit Public Facing Application

Phishing

Supply Chain Compromise

Exploit Public Facing Application

- Attackers have shown the ability to infiltrate networks at the application layer through internet-facing services. This tactic is commonly used due to the prevalence of software vulnerabilities. Other applications include exploitation of VPNs and Firewalls.

Use of Valid Accounts

- Threat actors utilize valid credentials and domain accounts to obfuscate detection. The access and use of valid accounts has increased with the use of information stealers, credential harvesting, and as-a-service toolkits.

Living off the Land

- Techniques that involve using network administration tools fall under this category. Living off the Land TTPs bolster persistent access and defense evasion and are indicative of Advanced Persistent Threats.

Tactics, Techniques, and Procedures

INITIAL ACCESS

Valid Accounts

Exploit Public Facing Application

Phishing

Supply Chain Compromise

CL0P Ransomware group exploited zero-day vulnerabilities in MOVEit file transfer software for initial access, led to the largest string of successful ransomware attacks in 2023

Exploit Public Facing Application

- Attackers have shown the ability to infiltrate networks at the application layer through internet-facing services. This tactic is commonly used due to the prevalence of software vulnerabilities. Other applications include exploitation of VPNs and Firewalls.

Use of Valid Accounts

- Threat actors utilize valid credentials and domain accounts to obfuscate detection. The access and use of valid accounts has increased with the use of information stealers, credential harvesting, and as-a-service toolkits.

Living off the Land

- Techniques that involve using network administration tools fall under this category. Living off the Land TTPs bolster persistent access and defense evasion and are indicative of Advanced Persistent Threats.

Tactics, Techniques, and Procedures

INITIAL ACCESS	Valid Accounts	Exploit Public Facing Application	Phishing	Supply Chain Compromise
PERSISTENCE	External Remote Services	Scheduled Task/Job	Server Software Component	Valid Accounts

Exploit Public Facing Application

- Attackers have shown the ability to infiltrate networks at the application layer through internet-facing services. This tactic is commonly used due to the prevalence of software vulnerabilities. Other applications include exploitation of VPNs and Firewalls.

Use of Valid Accounts

- Threat actors utilize valid credentials and domain accounts to obfuscate detection. The access and use of valid accounts has increased with the use of information stealers, credential harvesting, and as-a-service toolkits.

Living off the Land

- Techniques that involve using network administration tools fall under this category. Living off the Land TTPs bolster persistent access and defense evasion and are indicative of Advanced Persistent Threats.

Tactics, Techniques, and Procedures

INITIAL ACCESS	Valid Accounts	Exploit Public Facing Application	Phishing	Supply Chain Compromise
PERSISTENCE	External Remote Services	Scheduled Task/Job	Server Software Component	Valid Accounts

Peach Sandstorm used commercial remote monitoring service AnyDesk to maintain access to victim networks. This activity was observed in a subset of a larger espionage campaign against satellite and defense sectors.

Exploit Public Facing Application

- Attackers have shown the ability to infiltrate networks at the application layer through internet-facing services. This tactic is commonly used due to the prevalence of software vulnerabilities. Other applications include exploitation of VPNs and Firewalls.

Use of Valid Accounts

- Threat actors utilize valid credentials and domain accounts to obfuscate detection. The access and use of valid accounts has increased with the use of information stealers, credential harvesting, and as-a-service toolkits.

Living off the Land

- Techniques that involve using network administration tools fall under this category. Living off the Land TTPs bolster persistent access and defense evasion and are indicative of Advanced Persistent Threats.

SPACE ISAC

Tactics, Techniques, and Procedures

INITIAL ACCESS	Valid Accounts	Exploit Public Facing Application	Phishing	Supply Chain Compromise
PERSISTENCE	External Remote Services	Scheduled Task/Job	Server Software Component	Valid Accounts
DEFENSE EVASION	Subvert Trust Controls	Hijack Execution Flow	Indicator Removal	Obfuscated Files or information

Exploit Public Facing Application

- Attackers have shown the ability to infiltrate networks at the application layer through internet-facing services. This tactic is commonly used due to the prevalence of software vulnerabilities. Other applications include exploitation of VPNs and Firewalls.

Use of Valid Accounts

- Threat actors utilize valid credentials and domain accounts to obfuscate detection. The access and use of valid accounts has increased with the use of information stealers, credential harvesting, and as-a-service toolkits.

Living off the Land

- Techniques that involve using network administration tools fall under this category. Living off the Land TTPs bolster persistent access and defense evasion and are indicative of Advanced Persistent Threats.

Tactics, Techniques, and Procedures

INITIAL ACCESS	Valid Accounts	Exploit Public Facing Application	Phishing	Supply Chain Compromise
PERSISTENCE	External Remote Services	Scheduled Task/Job	Server Software Component	Valid Accounts
DEFENSE EVASION	Subvert Trust Controls	Hijack Execution Flow	Indicator Removal	Obfuscated Files or information

BlackTech threat actors were observed targeting network devices and modifying router firmware. They utilize custom malware and living off the land tactics to avoid endpoint detection

Exploit Public Facing Application

- Attackers have shown the ability to infiltrate networks at the application layer through internet-facing services. This tactic is commonly used due to the prevalence of software vulnerabilities. Other applications include exploitation of VPNs and Firewalls.

Use of Valid Accounts

- Threat actors utilize valid credentials and domain accounts to obfuscate detection. The access and use of valid accounts has increased with the use of information stealers, credential harvesting, and as-a-service toolkits.

Living off the Land

- Techniques that involve using network administration tools fall under this category. Living off the Land TTPs bolster persistent access and defense evasion and are indicative of Advanced Persistent Threats.

Tactics, Techniques, and Procedures

INITIAL ACCESS	Valid Accounts	Exploit Public Facing Application	Phishing	Supply Chain Compromise
PERSISTENCE	External Remote Services	Scheduled Task/Job	Server Software Component	Valid Accounts
DEFENSE EVASION	Subvert Trust Controls	Hijack Execution Flow	Indicator Removal	Obfuscated Files or information
EXECUTION	Command and Scripting Interpreter	PowerShell	Software Deployment Tools	System Services

Exploit Public Facing Application

- Attackers have shown the ability to infiltrate networks at the application layer through internet-facing services. This tactic is commonly used due to the prevalence of software vulnerabilities. Other applications include exploitation of VPNs and Firewalls.

Use of Valid Accounts

- Threat actors utilize valid credentials and domain accounts to obfuscate detection. The access and use of valid accounts has increased with the use of information stealers, credential harvesting, and as-a-service toolkits.

Living off the Land

- Techniques that involve using network administration tools fall under this category. Living off the Land TTPs bolster persistent access and defense evasion and are indicative of Advanced Persistent Threats.

Tactics, Techniques, and Procedures

INITIAL ACCESS	Valid Accounts	Exploit Public Facing Application	Phishing	Supply Chain Compromise
PERSISTENCE	External Remote Services	Scheduled Task/Job	Server Software Component	Valid Accounts
DEFENSE EVASION	Subvert Trust Controls	Hijack Execution Flow	Indicator Removal	Obfuscated Files or information
EXECUTION	Command and Scripting Interpreter	PowerShell	Software Deployment Tools	System Services

PowerDrop, a malicious PowerShell script, surfaced in June 2023, used by suspected nation-state actors to target the US Aerospace and Defense sectors.

Exploit Public Facing Application

- Attackers have shown the ability to infiltrate networks at the application layer through internet-facing services. This tactic is commonly used due to the prevalence of software vulnerabilities. Other applications include exploitation of VPNs and Firewalls.

Use of Valid Accounts

- Threat actors utilize valid credentials and domain accounts to obfuscate detection. The access and use of valid accounts has increased with the use of information stealers, credential harvesting, and as-a-service toolkits.

Living off the Land

- Techniques that involve using network administration tools fall under this category. Living off the Land TTPs bolster persistent access and defense evasion and are indicative of Advanced Persistent Threats.

Tactics, Techniques, and Procedures

INITIAL ACCESS	Valid Accounts	Exploit Public Facing Application	Phishing	Supply Chain Compromise
PERSISTENCE	External Remote Services	Scheduled Task/Job	Server Software Component	Valid Accounts
DEFENSE EVASION	Subvert Trust Controls	Hijack Execution Flow	Indicator Removal	Obfuscated Files or information
EXECUTION	Command and Scripting Interpreter	PowerShell	Software Deployment Tools	System Services
COMMAND AND CONTROL	Application Layer Protocol	Protocol Tunneling	Encrypted Channel	Proxy

Exploit Public Facing Application

- Attackers have shown the ability to infiltrate networks at the application layer through internet-facing services. This tactic is commonly used due to the prevalence of software vulnerabilities. Other applications include exploitation of VPNs and Firewalls.

Use of Valid Accounts

- Threat actors utilize valid credentials and domain accounts to obfuscate detection. The access and use of valid accounts has increased with the use of information stealers, credential harvesting, and as-a-service toolkits.

Living off the Land

- Techniques that involve using network administration tools fall under this category. Living off the Land TTPs bolster persistent access and defense evasion and are indicative of Advanced Persistent Threats.

SPACE ISAC

Tactics, Techniques, and Procedures

INITIAL ACCESS	Valid Accounts	Exploit Public Facing Application	Phishing	Supply Chain Compromise
PERSISTENCE	External Remote Services	Scheduled Task/Job	Server Software Component	Valid Accounts
DEFENSE EVASION	Subvert Trust Controls	Hijack Execution Flow	Indicator Removal	Obfuscated Files or information
EXECUTION	Command and Scripting Interpreter	PowerShell	Software Deployment Tools	System Services
COMMAND AND CONTROL	Application Layer Protocol	Protocol Tunneling	Encrypted Channel	Proxy

Multiple nation-state actors have exploited vulnerabilities in ManageEngine software and firewalls to target space industry. The threat actors leveraged SSH protocols to communicate with C2 servers

Exploit Public Facing Application

- Attackers have shown the ability to infiltrate networks at the application layer through internet-facing services. This tactic is commonly used due to the prevalence of software vulnerabilities. Other applications include exploitation of VPNs and Firewalls.

Use of Valid Accounts

- Threat actors utilize valid credentials and domain accounts to obfuscate detection. The access and use of valid accounts has increased with the use of information stealers, credential harvesting, and as-a-service toolkits.

Living off the Land

- Techniques that involve using network administration tools fall under this category. Living off the Land TTPs bolster persistent access and defense evasion and are indicative of Advanced Persistent Threats.

SPACE ISAC

Tactics, Techniques, and Procedures

INITIAL ACCESS	Valid Accounts	Exploit Public Facing Application	Phishing	Supply Chain Compromise

CL0P Ransomware group exploited zero-day vulnerabilities in MOVEit file transfer software for initial access, led to the largest string of successful ransomware attacks in 2023

PERSISTENCE	External Remote Services	Scheduled Task/Job	Server Software Component	Valid Accounts

Peach Sandstorm used commercial remote monitoring service AnyDesk to maintain access to victim networks. This activity was observed in a subset of a larger espionage campaign against satellite and defense sectors.

DEFENSE EVASION	Subvert Trust Controls	Hijack Execution Flow	Indicator Removal	Obfuscated Files or information

BlackTech threat actors were observed targeting network devices and modifying router firmware. They utilize custom malware and living off the land tactics to avoid endpoint detection

EXECUTION	Command and Scripting Interpreter	PowerShell	Software Deployment Tools	System Services

PowerDrop, a malicious PowerShell script, surfaced in June 2023, used by suspected nation-state actors to target the US Aerospace and Defense sectors.

COMMAND AND CONTROL	Application Layer Protocol	Protocol Tunneling	Encrypted Channel	Proxy

Multiple nation-state actors have exploited vulnerabilities in ManageEngine software and firewalls to target space industry. The threat actors leveraged SSH protocols to communicate with C2 servers

Exploit Public Facing Application

- Attackers have shown the ability to infiltrate networks at the application layer through internet-facing services. This tactic is commonly used due to the prevalence of software vulnerabilities. Other applications include exploitation of VPNs and Firewalls.

Use of Valid Accounts

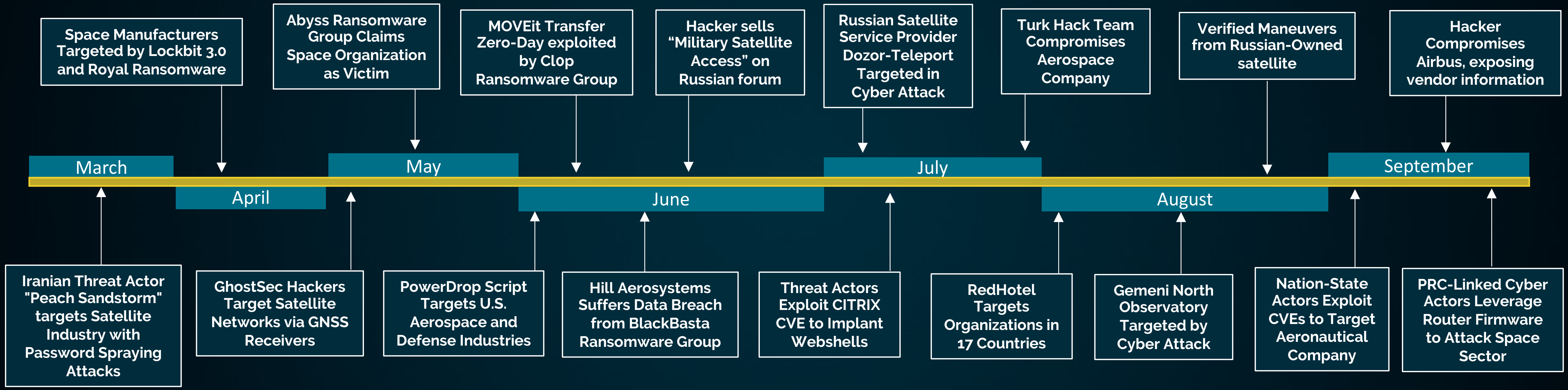
- Threat actors utilize valid credentials and domain accounts to obfuscate detection. The access and use of valid accounts has increased with the use of information stealers, credential harvesting, and as-a-service toolkits.

Living off the Land

- Techniques that involve using network administration tools fall under this category. Living off the Land TTPs bolster persistent access and defense evasion and are indicative of Advanced Persistent Threats.

Timeline of Space Sector Targeting

March – September 2023



March

Iranian Threat Actor "Peach Sandstorm" targets Satellite Industry with Password Spraying Attacks

Space Manufacturers Targeted by Lockbit 3.0 and Royal Ransomware

April

GhostSec Hackers Target Satellite Networks via GNSS Receivers

Abyss Ransomware Group Claims Space Organization as Victim

May

PowerDrop Script Targets U.S. Aerospace and Defense Industries

MOVEit Transfer Zero-Day exploited by Cl0p Ransomware Group

Hill Aerosystems Suffers Data Breach from BlackBasta Ransomware Group

June

Hacker sells "Military Satellite Access" on Russian forum

Russian Satellite Service Provider Dozor-Teleport Targeted in Cyber Attack

Threat Actors Exploit CITRIX CVE to Implant Webshells

July

Turk Hack Team Compromises Aerospace Company

RedHotel Targets Organizations in 17 Countries

Gemeni North Observatory Targeted by Cyber Attack

August

Verified Maneuvers from Russian-Owned satellite

Nation-State Actors Exploit CVEs to Target Aeronautical Company

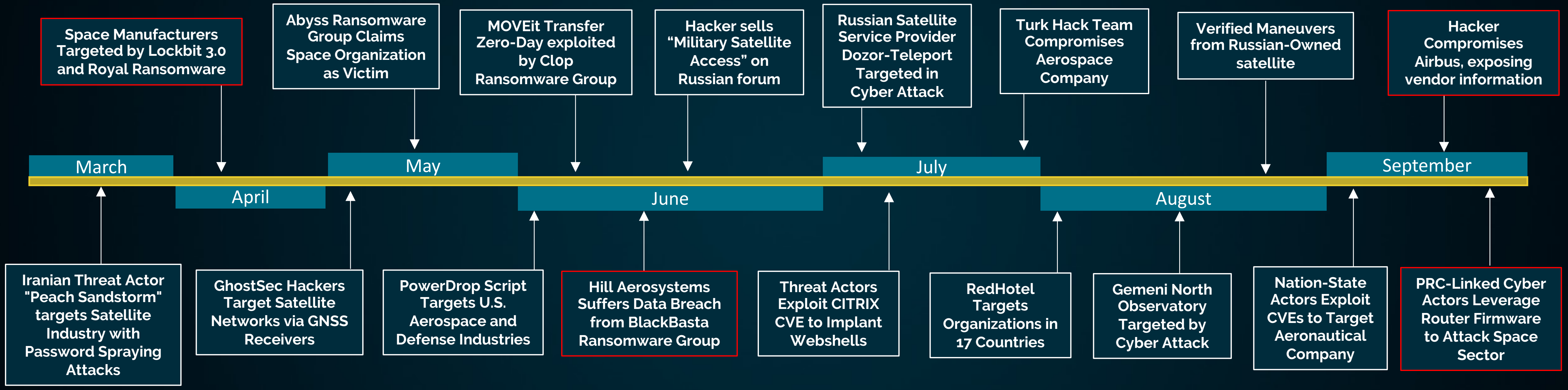
September

Hacker Compromises Airbus, exposing vendor information

PRC-Linked Cyber Actors Leverage Router Firmware to Attack Space Sector

Timeline of Space Sector Targeting

March – September 2023



March

Iranian Threat Actor "Peach Sandstorm" targets Satellite Industry with Password Spraying Attacks

April

Space Manufacturers Targeted by Lockbit 3.0 and Royal Ransomware

GhostSec Hackers Target Satellite Networks via GNSS Receivers

May

Abyss Ransomware Group Claims Space Organization as Victim

June

PowerDrop Script Targets U.S. Aerospace and Defense Industries

MOVEit Transfer Zero-Day exploited by Clop Ransomware Group

Hill Aerosystems Suffers Data Breach from BlackBasta Ransomware Group

Hacker sells "Military Satellite Access" on Russian forum

July

Russian Satellite Service Provider Dozor-Teleport Targeted in Cyber Attack

Threat Actors Exploit CITRIX CVE to Implant Webshells

Turk Hack Team Compromises Aerospace Company

August

RedHotel Targets Organizations in 17 Countries

Gemeni North Observatory Targeted by Cyber Attack

Verified Maneuvers from Russian-Owned satellite

Nation-State Actors Exploit CVEs to Target Aeronautical Company

September

Hacker Compromises Airbus, exposing vendor information

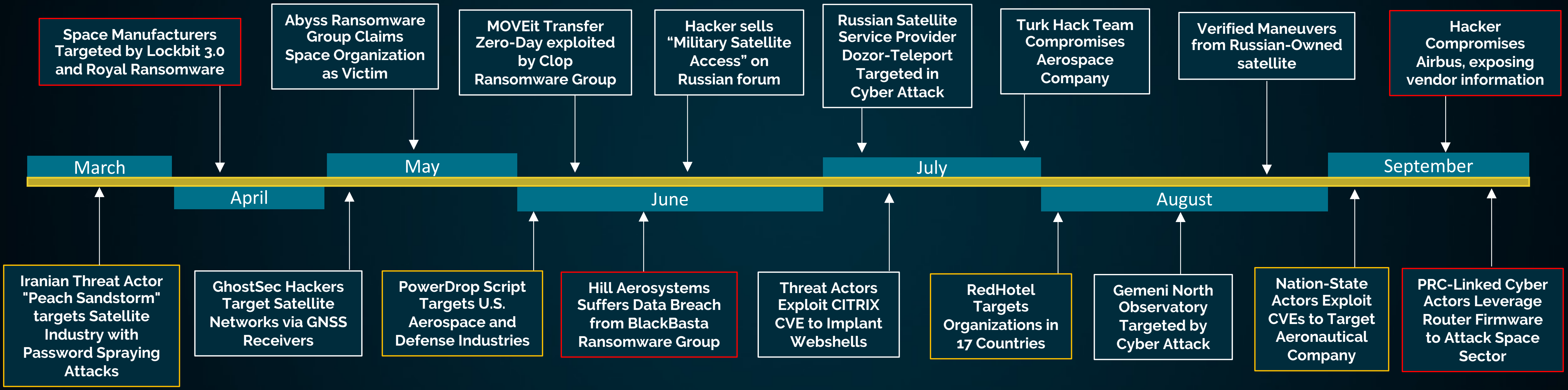
PRC-Linked Cyber Actors Leverage Router Firmware to Attack Space Sector

Trends and Observations:

- Increased targeting of **space supply chain**

Timeline of Space Sector Targeting

March – September 2023



March

Space Manufacturers Targeted by Lockbit 3.0 and Royal Ransomware

Iranian Threat Actor "Peach Sandstorm" targets Satellite Industry with Password Spraying Attacks

April

GhostSec Hackers Target Satellite Networks via GNSS Receivers

Abyss Ransomware Group Claims Space Organization as Victim

May

MOVEit Transfer Zero-Day exploited by Clop Ransomware Group

PowerDrop Script Targets U.S. Aerospace and Defense Industries

Hacker sells "Military Satellite Access" on Russian forum

June

Hill Aerosystems Suffers Data Breach from BlackBasta Ransomware Group

Russian Satellite Service Provider Dozor-Teleport Targeted in Cyber Attack

Threat Actors Exploit CITRIX CVE to Implant Webshells

July

Turk Hack Team Compromises Aerospace Company

RedHotel Targets Organizations in 17 Countries

August

Gemeni North Observatory Targeted by Cyber Attack

Verified Maneuvers from Russian-Owned satellite

Nation-State Actors Exploit CVEs to Target Aeronautical Company

September

Hacker Compromises Airbus, exposing vendor information

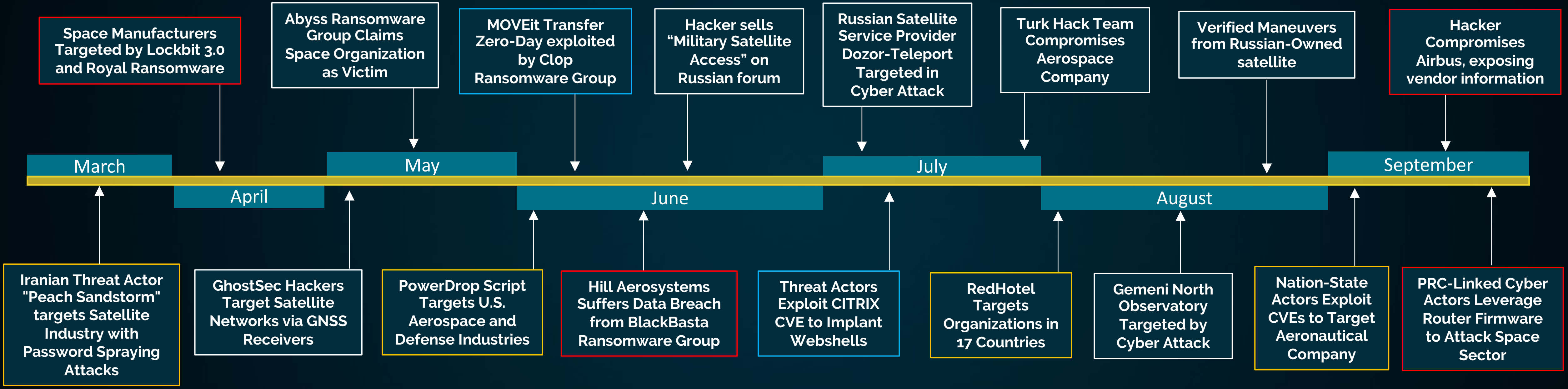
PRC-Linked Cyber Actors Leverage Router Firmware to Attack Space Sector

Trends and Observations:

- Increased targeting of **space supply chain**
- State-sponsored threat actor **targeting**

Timeline of Space Sector Targeting

March – September 2023



Space Manufacturers Targeted by Lockbit 3.0 and Royal Ransomware

Abyss Ransomware Group Claims Space Organization as Victim

MOVEit Transfer Zero-Day exploited by Cl0p Ransomware Group

Hacker sells "Military Satellite Access" on Russian forum

Russian Satellite Service Provider Dozor-Teleport Targeted in Cyber Attack

Turk Hack Team Compromises Aerospace Company

Verified Maneuvers from Russian-Owned satellite

Hacker Compromises Airbus, exposing vendor information

March

April

May

June

July

August

September

Iranian Threat Actor "Peach Sandstorm" targets Satellite Industry with Password Spraying Attacks

GhostSec Hackers Target Satellite Networks via GNSS Receivers

PowerDrop Script Targets U.S. Aerospace and Defense Industries

Hill Aerosystems Suffers Data Breach from BlackBasta Ransomware Group

Threat Actors Exploit CITRIX CVE to Implant Webshells

RedHotel Targets Organizations in 17 Countries

Gemeni North Observatory Targeted by Cyber Attack

Nation-State Actors Exploit CVEs to Target Aeronautical Company

PRC-Linked Cyber Actors Leverage Router Firmware to Attack Space Sector

Trends and Observations:

- Increased targeting of **space supply chain**
- State-sponsored threat actor **targeting**
- Exploitation of public-facing application / software

Impact of Zero Trust Architecture on Space Warfare

Altif Brown, Co-Founder, Constellation Network

Securing the Cosmos

The Integration and Impact of Zero Trust Architecture in Modern Space Warfare

Constellation

SPACE ISAC

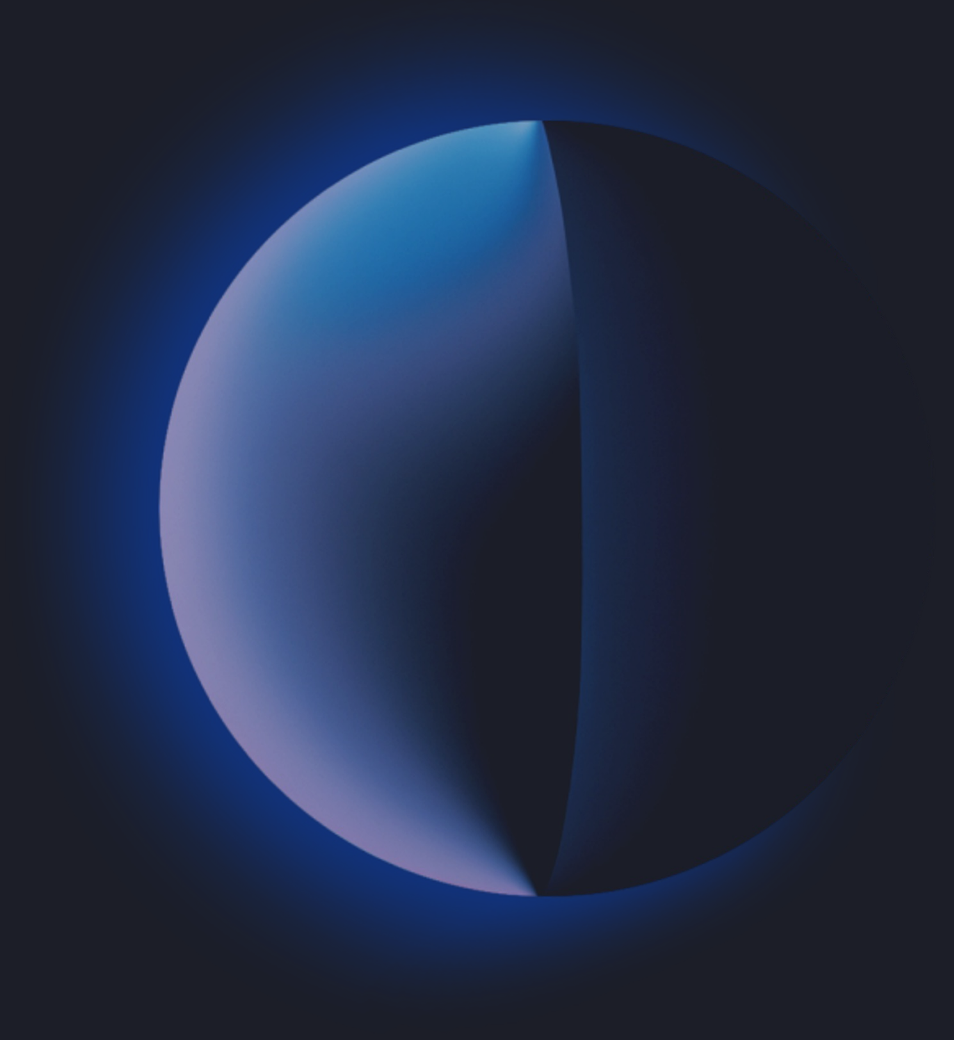
Altif Brown

Co-Founder & Dir, Open Source Community

Constellation Network, Inc.

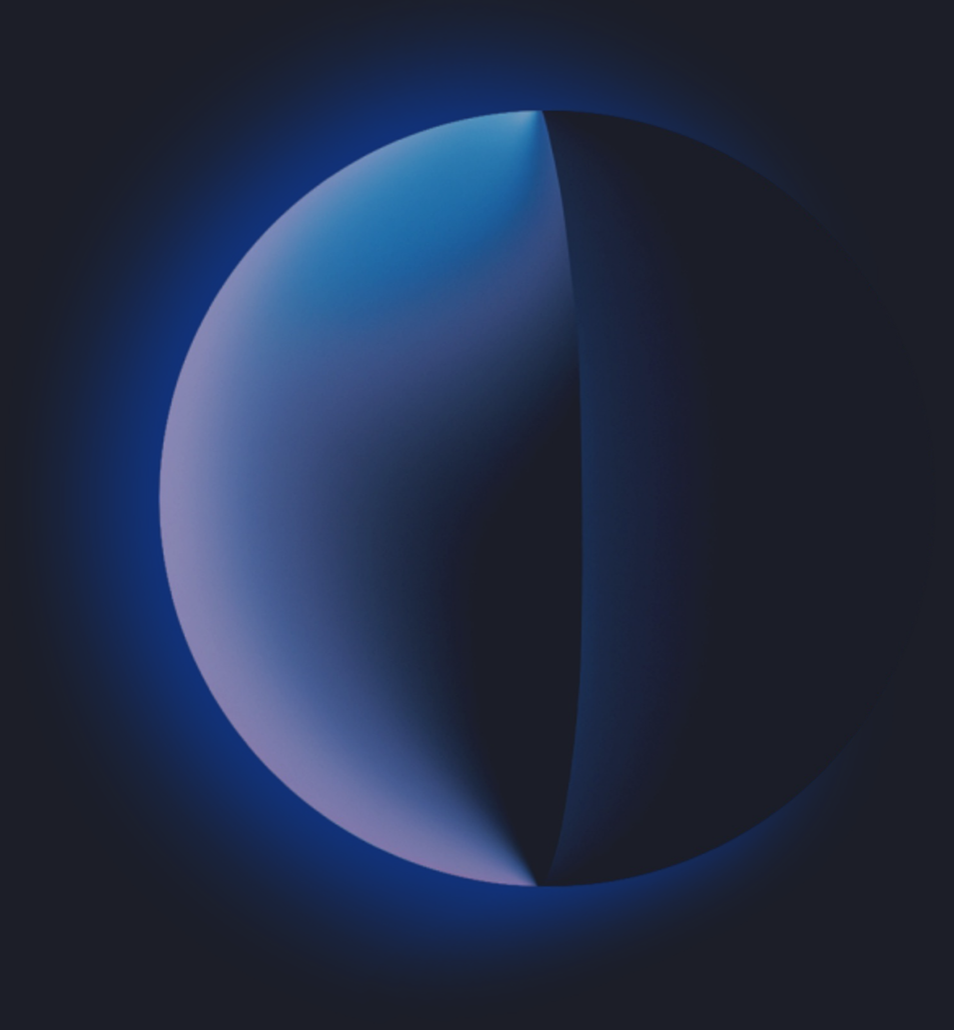
Agenda

- Welcome and Introduction
- Constellation Overview
- Intro to ZTA
- Why ZTA Matters
- Emerging Technologies
- Challenges
- Use Case
- The Way Forward



Remember this number:

11

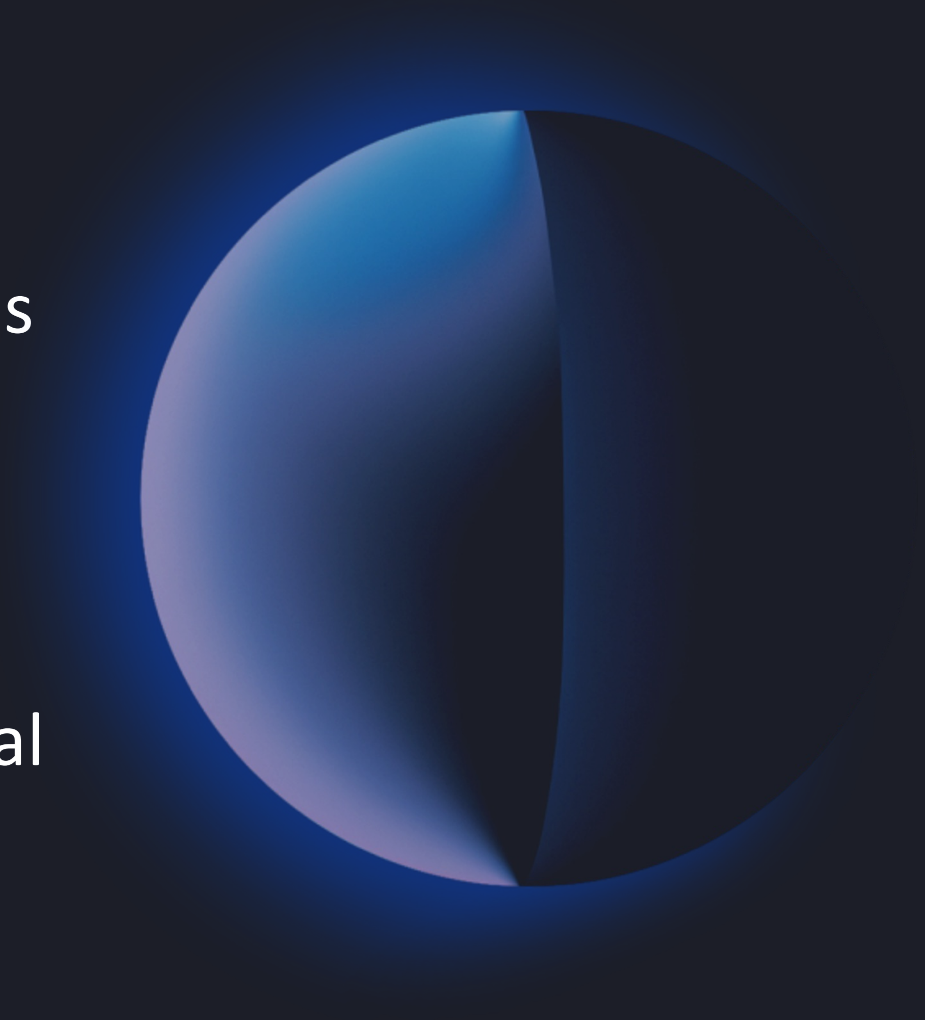


Company Overview

Fall 2023

Constellation

Constellation is a 3rd generation Blockchain infrastructure that fulfills the promise of secure decentralization. We combine fast communications speeds, easy implementation and low operational costs.



Company Highlights

US Based Blockchain Infrastructure Company

Base Layer Protocol - DAG Architecture - Custom Consensus - L0 Interoperability - Open Source

A Feeless & Scalable Network Built Around the Validation & Management of Data

Hypergraph Transfer Protocol (HGTP) - 80k Transaction in 7 Seconds - Highly Energy Efficient

Web3 Tooling for Developers & Support for Legacy Systems

Euclid SDK (Metagraphs) - Stargazer Multi-Currency Wallet - Node Management Support - DeFi Platform

100+ Projects from Legacy to Emerging, Engaged in Building on Constellation

Business Accelerator Program - Web3 Legal LaunchKit - 100k+ Community Members & Wallet Holders

Native Cryptocurrency $DAG - Utility Validates Complex Data and Transactions

#250 Market Cap Ranking - Focused on Complex Data Types VS Basic Transfer of Value (BTC, ETH, Etc.)

Threat Landscape

Changing Landscape of Space Warfare

Increased reliance on digital systems leading to new vulnerabilities.

External Threats

- State-sponsored cyberattacks that target critical space infrastructure.
- Non-state actors/ Independent groups with varied motives.

Internal Threats

- Insider sabotage
- Compromised updates
- Human errors

Development and deployment of anti-space asset weaponry

- Rapid development of anti-satellite weapons by major powers.
- Electronic warfare: jamming, spoofing, and SATCOM interference techniques.
- Dual-use technologies: Commercial tech with potential military applications.

Global Implications

- Disruptions affecting global communication and navigation systems.
- Economic implications: satellite-based services, GPS, supply chains, and more.
- Geopolitical tensions arising from contested space domains.

Introduction to Zero Trust Architecture

Origins

★ Authentication and trust have been foundational for centuries. Ancient civilizations employed seals, symbols, and other methods to validate and authenticate messages.

★ 1980s-1990s: The dawn of digital networking brought a perimeter-based security approach, where everything inside the network was trusted, and external entities were not.

★ 2000s: With the rise of mobile computing and cloud services, the traditional network perimeter began to erode. The need for a new security model became evident.

★ 2010: John Kindervag, while at Forrester Research, introduced the concept of "Zero Trust". It was a revolutionary approach that suggests never trusting and always verifying, regardless of whether the resource is inside or outside the network.

What is Zero Trust Architecture?

1. No Implicit Trust: Trust is not based on location (e.g., inside or outside the corporate network).
2. Least Privilege: Users/access devices are given the minimum access required to perform their tasks.
3. Microsegmentation: Breaks the network into smaller zones to maintain separate access for separate segments.
4. Continuous Verification: Requires validation of all entities and requests, regardless of source.

NEVER TRUST, ALWAYS VERIFY

Why Zero Trust Architecture Matters?

- ★ Enhanced Security: Reduces the attack surface and limits lateral movement.
- ★ Flexibility: Adapts to various digital environments, from cloud to on-premises.
- ★ Improved Compliance: Helps organizations meet stringent regulatory requirements.
- ★ Proactive Defense: Shifts from reactive security measures to proactive defenses.

Executive Order (EO) 14028

The Nexus of ZTA & Emerging Technologies

Do You Remember That Number?

Blockchain/DLT

Decentralization:
No single point of trust. Trust is distributed across the network nodes.

Cryptography:
Every transaction is cryptographically signed. Block hashes ensure data integrity and prevent Tampering.

Consensus Algorithms:
Transactions/data transfers are only added to the blockchain after network consensus, ensuring authenticity and reliability.

Key Takeaways

Trustless Environment: Blockchains are inherently designed to function in a trustless environment. Trust is generated through protocol & math, not through intermediaries.

Security: Zero Trust minimizes attack vectors, and blockchain's inherent zero trust properties add an additional layer of security against malicious actors.

Decentralized Verification: Blockchain's verification process is distributed, ensuring that trust isn't centralized.

Other Emerging Technologies

Quantum Resistance

&

Artificial Intelligence/Machine Learning

- Quantum computing poses threats to current encryption.
- Quantum-resistant algorithms in development to protect against quantum breaches.

- Forefront of threat modeling.
- Predictive analysis & real-time responses.
- AI growth predicted at $1.3 Trillion by 2032.
- **Challenges**: Quality data reliance & space systems integration.

Other Emerging Technologies

Edge Computing

- Process data at its source.
- Advantages: Reduced latency & data exposure alignment with ZTA

&

Remote Security Posture Attestation

- Lightweight, scalable way to implement security across large, dynamic SATCOM ecosystems containing diverse devices with varying capabilities
- Ensures device trustworthiness for risk management in HSN (Hybrid Space Network)
- Not constrained by SWaP

Key Challenges in ZTA Implementation

Real-time Authentication Challenges

Need for instantaneous decisions based on real-time data.
Balancing rigorous ZTA authentication without introducing operation-impeding latencies.

Micro-segmentation in Satellite Networks

Complex interactions among satellites, ground stations, and military assets.
Ensuring a security breach in one segment doesn't compromise the entire system.

Threat of Advanced Persistent Threats (APTs)

APTs: Stealthy and long-term cyberattacks.
Amplified implications in space warfare due to potential for intelligence gathering and large-scale assaults.

Continuous Oversight and Evolution

Post-ZTA deployment isn't the endgame.
Constant surveillance and adaptive security protocols needed to address ever-changing threats.

Synchronizing ZTA with Legacy Infrastructures

Challenges due to extended operational lifecycles of space assets.
Issues range from software incompatibilities to hardware constraints.

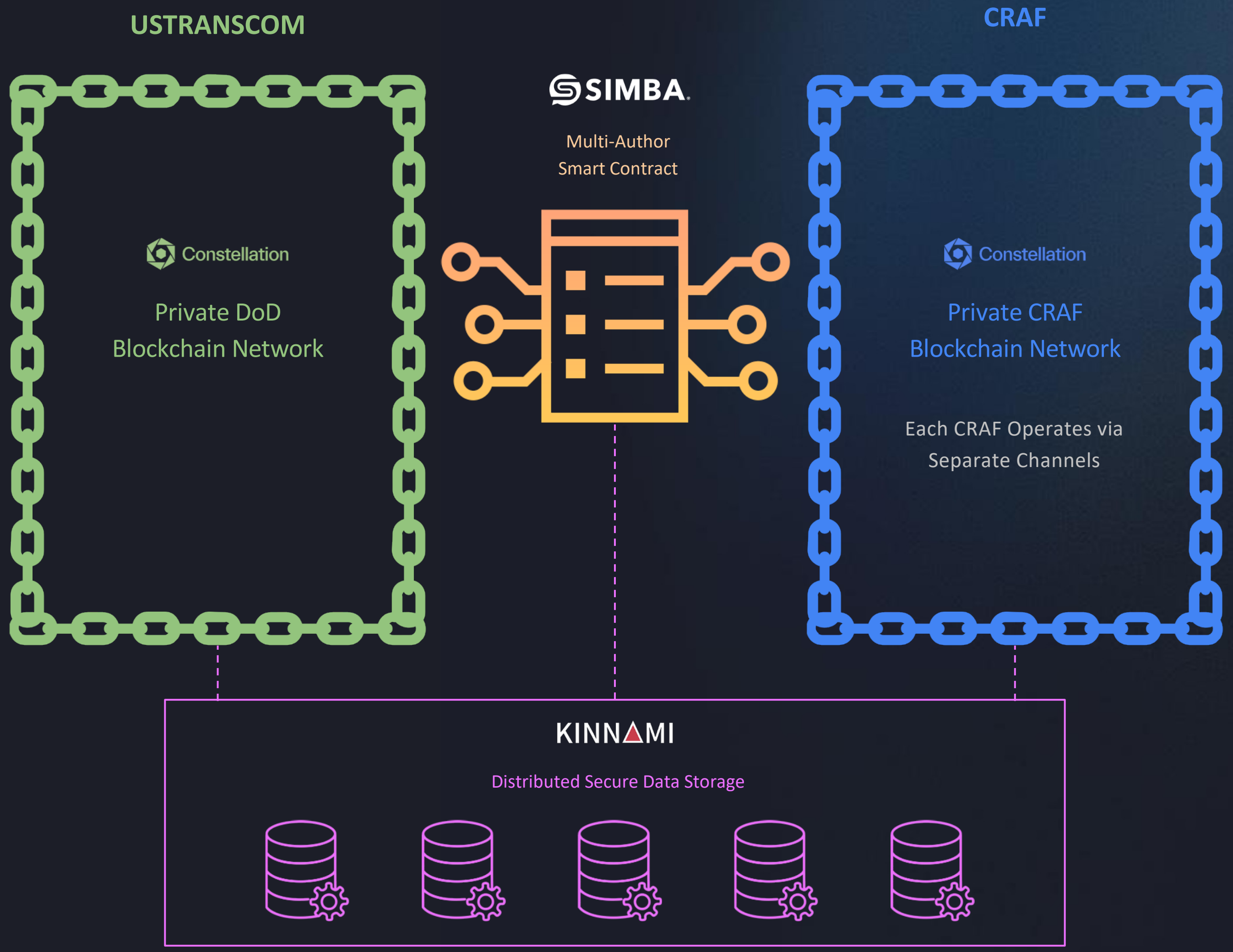
Use Case

Constellation

IRON SPIDR

USAF, AMC, and 618 AOC (the air component to USTRANSCOM) have a national defense-related mission need in the area of securing their legacy and future C2 and mission planning systems and data exchanges with their commercial partners and lay foundation for transition to big data cloud infrastructure using a unique scalable, secure end-to-end, multi-source, smart contracts, and big data Blockchain solution.

Iron SPIDR Deployment Approach



DEPLOYMENT BREAKDOWN

Blockchain to Blockchain Communications with a Smart Contracting Framework Enabling Secure Information Sharing for Mission Execution

- ★ USTRANSCOM Private Permissioned Blockchain Network
- ★ CRAF Private Permissioned Blockchain Network
- ★ Secure Smart Contracting Application for CRAF & TCAQ Communications & Mission Orchestration
- ★ Node Operators (Virtual Machines) Powering Multiple Blockchain Networks Enforcing Security of All Data-in-Transit Transactions
- ★ Data at Rest is Securely Stored Using Kinnami's Encrypted Sharding Approach

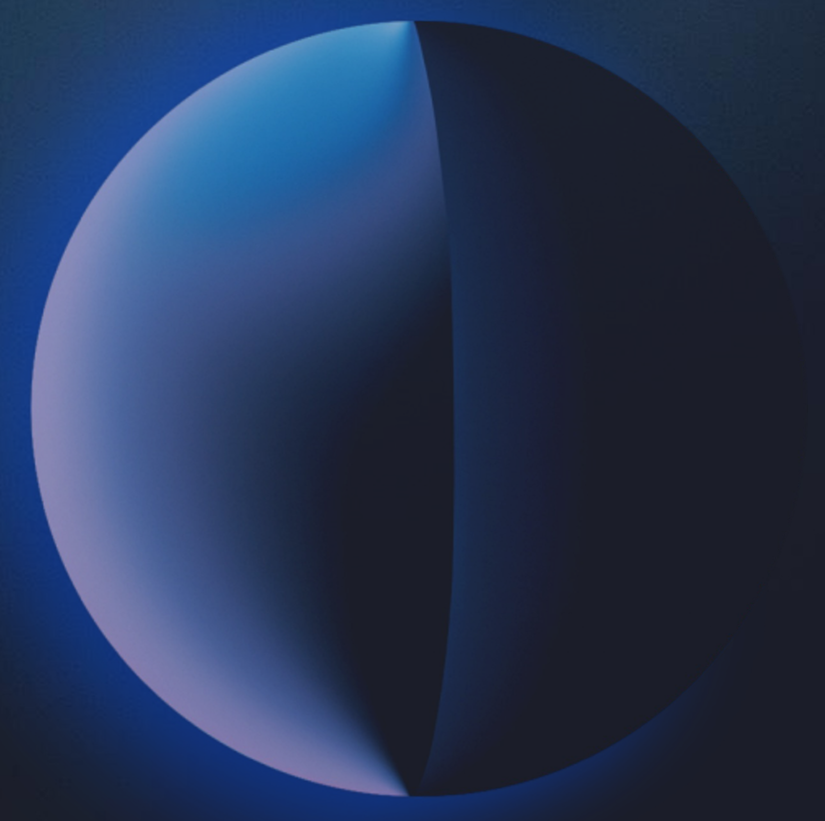
Benefits & Impact

FOR BOTH USTRANSCOM & CRAF

- ★ Secure Intelligence Sharing Between Government and Industry
- ★ Protection from Spoofing, Corruption, Jamming & Man-in-the-Middle Attacks
- ★ Robust Cyber Intelligence to Inform Cyber Actions for Mission
- ★ End-to-End Encrypted Data Transmission and Storage Protection Procedures
- ★ Quantum Attack Protected Communications to Ensure Global Navigation

- ★ Ease of Deployment - Leverages Existing Infrastructure Investments
- ★ Highly Scalable, Fast and Uses Less Energy for Computational Use than Existing Systems
- ★ Real-Time Mission Progress - Secure Monitoring of Content Updates & Mission Movement
- ★ CRAF IP and Data is Protected Using Blockchain to Blockchain with Smart Contracting
- ★ All Contract Events Notarized Providing Proof of Ownership & Advanced Analytics

The Way Forward



The Way Forward

Human Training

- ★ Training & Development: Vital despite ZTA's technological advancements.
- ★ Tailored Programs: From basic ZTA courses to advanced workshops.
- ★ Simulated Environments: Offer hands-on experience, replicating actual space operations.
- ★ Periodic Assessments: Ensure personnel remain updated with ZTA advancements and evolving threats.

Global Collaboration

- ★ Joint R&D: Exploring novel authentication protocols, threat detection, and seamless integration.
- ★ Shared Testing: Establish environments for rigorous evaluations, simulating real-world scenarios.
- ★ Universal Standards: Crucial for consistent ZTA application; should be dynamic and reviewed regularly.
- ★ Collaborative Platforms: Sharing real-time threat intelligence for quick identification & mitigation.

Key Takeaways

Evolving Threat Landscape: Space warfare has transitioned from primarily physical threats to sophisticated cyber threats, requiring adaptive security measures.

Limitations of Traditional Security: Perimeter-based defenses, once effective, now show vulnerabilities against modern cyber threats, especially in the dynamic realm of space.

ZTA's Role: Zero Trust Architecture (ZTA) offers a proactive, adaptive, and granular approach to security, addressing both external and internal threats.

Emerging Technologies: Technologies like blockchain, AI, and quantum-resistant algorithms play a pivotal role in enhancing ZTA's effectiveness in space warfare.

Collaboration is Crucial: Given the global nature of space warfare, international collaboration, shared standards, and joint R&D initiatives are essential for effective ZTA implementation.

Human Element: While technology is vital, training and skill development for personnel are equally crucial to ensure the successful adoption and management of ZTA protocols.

"Trust is a vulnerability."

– John Kindervag

The father of Zero Trust

Thank You

The full length paper will be made available to the full SpaceISAC when this conference concludes.

Feel free to reach out to me:

altif@constellationnetwork.io

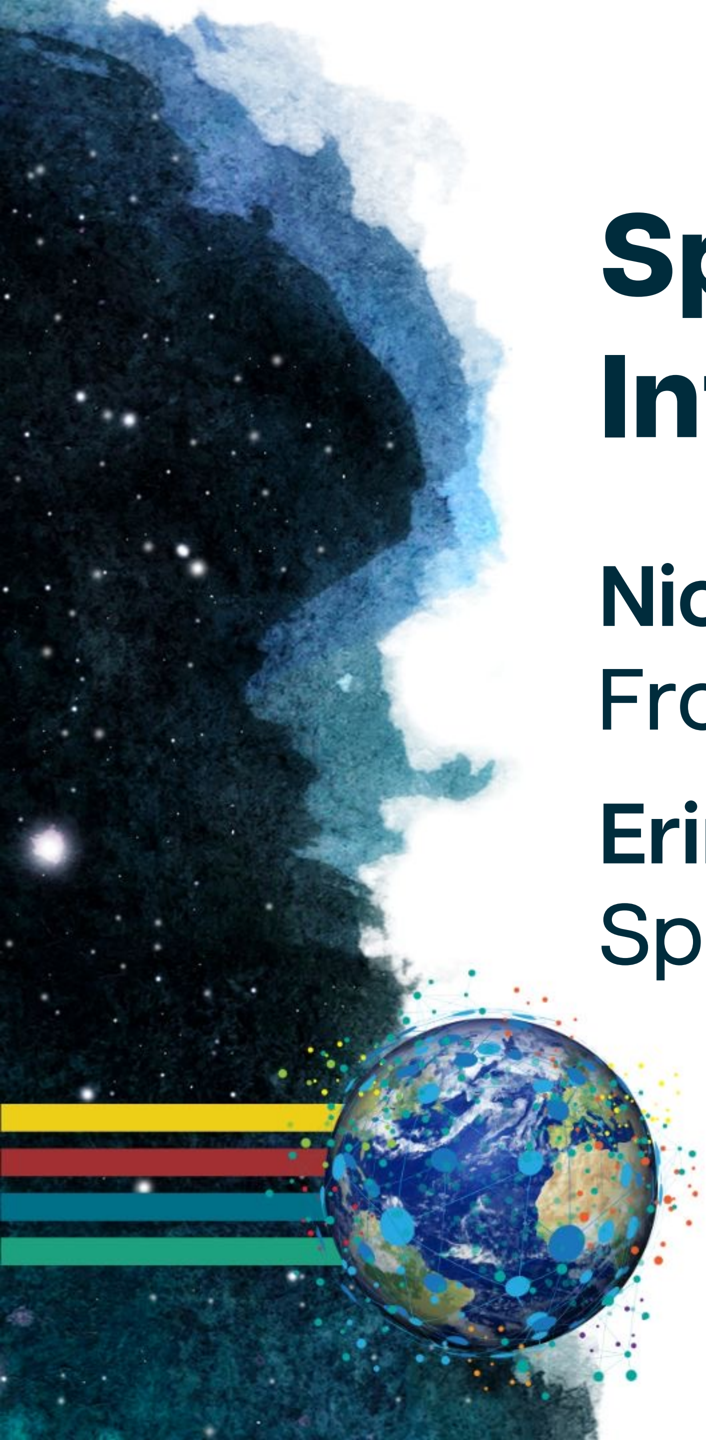
Request Info

Special Thanks to:

Brian Thamm
Sophinea

James Gallegos
Deloitte

William Mattull
Viasat



Space Systems Critical Infrastructure

Nick Reese, Co-Founder and COO, Frontier Foundry

Erin Miller, Executive Director, Space ISAC

Fortifying Space: Building Cyber Resilience with Smart Design Principles

Irby Thompson, Chief Executive Officer (CEO), OP[4]

Fortifying Space: Building Cyber Resilience

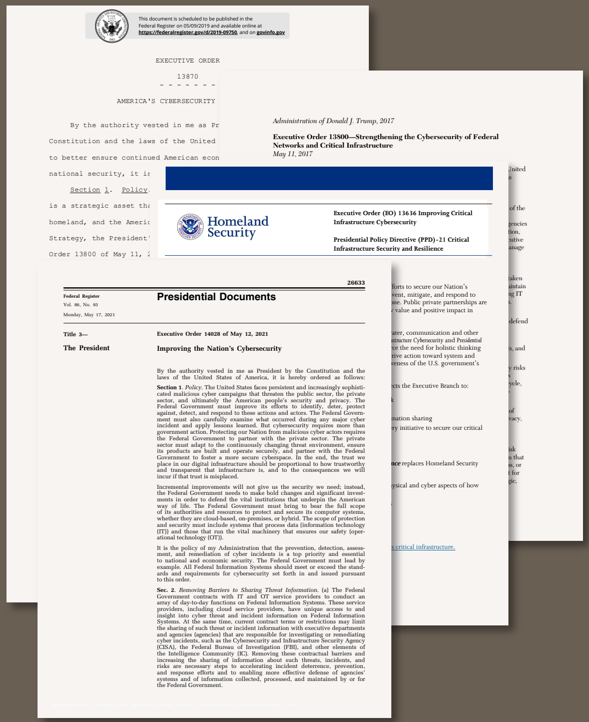
SMART DESIGN PRINCIPLES
FOR SPACE SYSTEMS

https://op4.io
hello@op4.io
[703] 574.0280

Agenda

- The cacophony of cybersecurity
- A lesson from thermodynamics
- Grand unifying theory
- Top 10 Smart design principles for secure space systems
- The path to cyber resilience

The "guidance" is overwhelming



EXECUTIVE ORDER

13870

AMERICA'S CYBERSECURITY

Administration of Donald J. Trump, 2017

Executive Order 13800—Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure

May 11, 2017

Homeland Security

Executive Order (EO) 13636 Improving Critical Infrastructure Cybersecurity

Presidential Policy Directive (PPD)-21 Critical Infrastructure Security and Resilience

Presidential Documents

Executive Order 14028 of May 12, 2021

Improving the Nation's Cybersecurity

Whitehouse Executive Orders

Federal Government Cybersecurity Incident & Vulnerability Response Playbooks

Zero Trust Maturity Model

Cloud Security Technical Reference Architecture

Intelligence Community Information Technology Systems Security Risk Management

Intelligence Community Directive 503 Technical Amendment

CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)

Harmonization of Cyber Incident Reporting to the Federal Government

September 19, 2023

Homeland Security

Office of Strategy,

Department of Defense INSTRUCTION

NUMBER 8500.01

March 14, 2014

Incorporating Change 1, Effective October 7, 2019

DoD CIO

SUBJECT: Cybersecurity

CISA guidance, DOD Instructions, IC Directives

NIST Special Publication 800-218

Secure Software Development Framework (SSDF) Version 1.1:

Recommendations for Mitigating the Risk of Software Vulnerabilities

NIST Special Publication 800-172

Enhanced Security Requirements for Protecting Controlled Unclassified Information

A Supplement to NIST Special Publication 800-171

NIST Special Publication 800-171 Revision 2

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

NIST Special Publication 800-53 Revision 5

Security and Privacy Controls for Information Systems and Organizations

NIST Special Publication 800-37 Revision 2

Risk Management Framework for Information Systems and Organizations

A System Life Cycle Approach for Security and Privacy

NIST Interagency Report NIST IR 8401

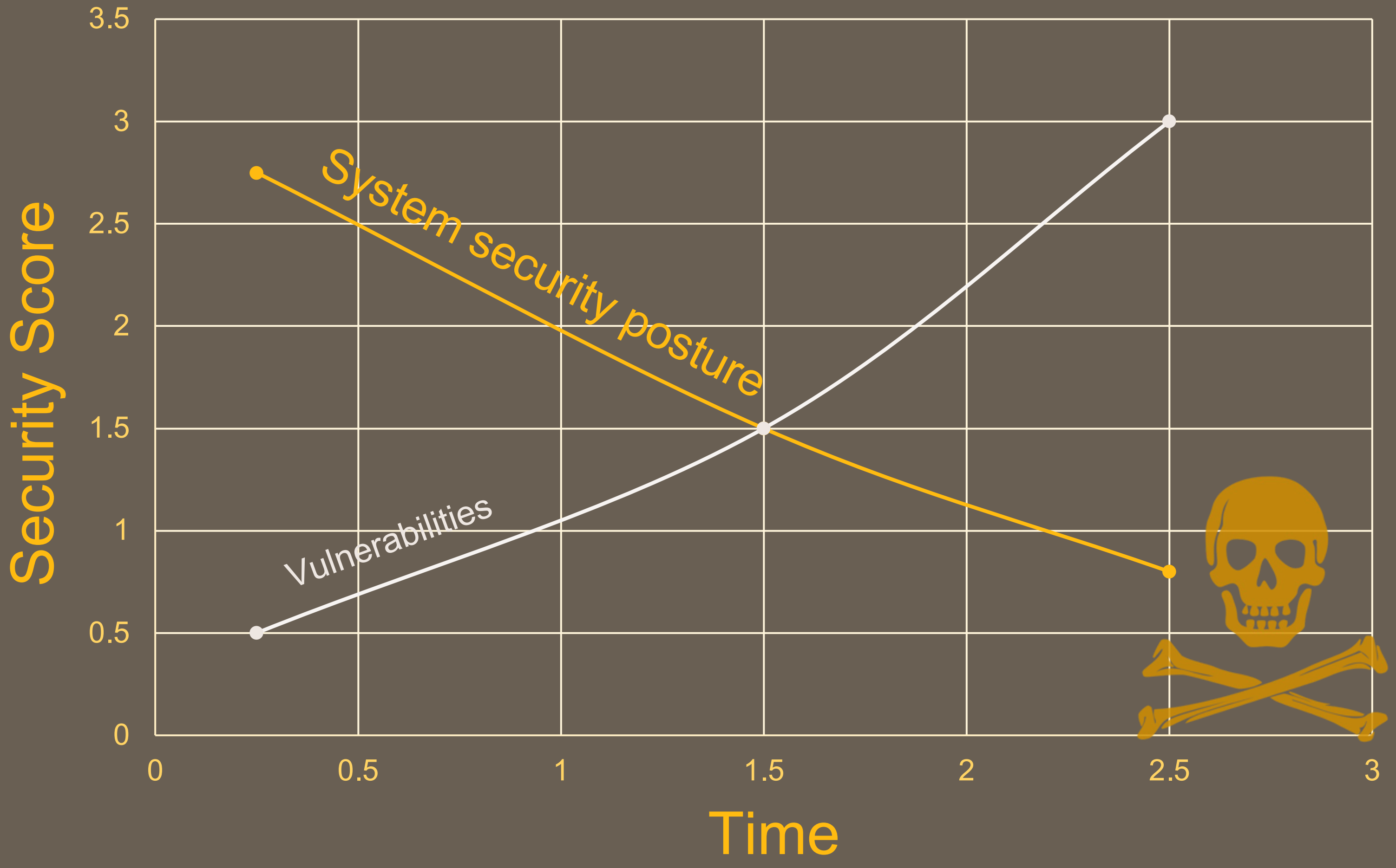
Satellite Ground Segment

Applying the Cybersecurity Framework to Satellite Command and Control

NIST requirements

Thousands of requirements – don't miss one!

And then reality strikes



System security posture naturally degrades over time

The currency of cybersecurity can be summed up in one word

Access

“the ability, right, or permission to approach, enter, speak with, or use”[1]

[1] Definition source: https://dictionary.com

Smart Design Principles for Secure Space Systems

Design

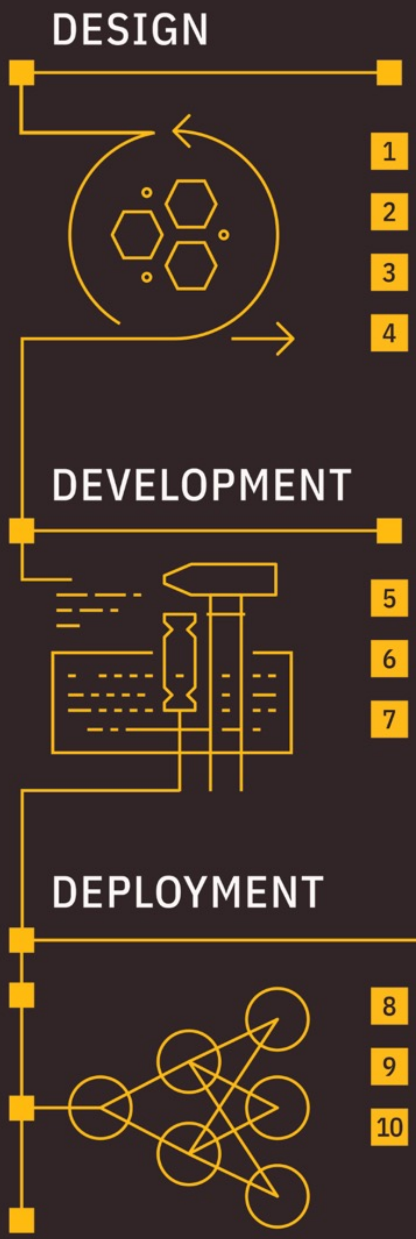
Data-at-Rest Protection
Secure Boot
Compartmentalization
Secure Communications

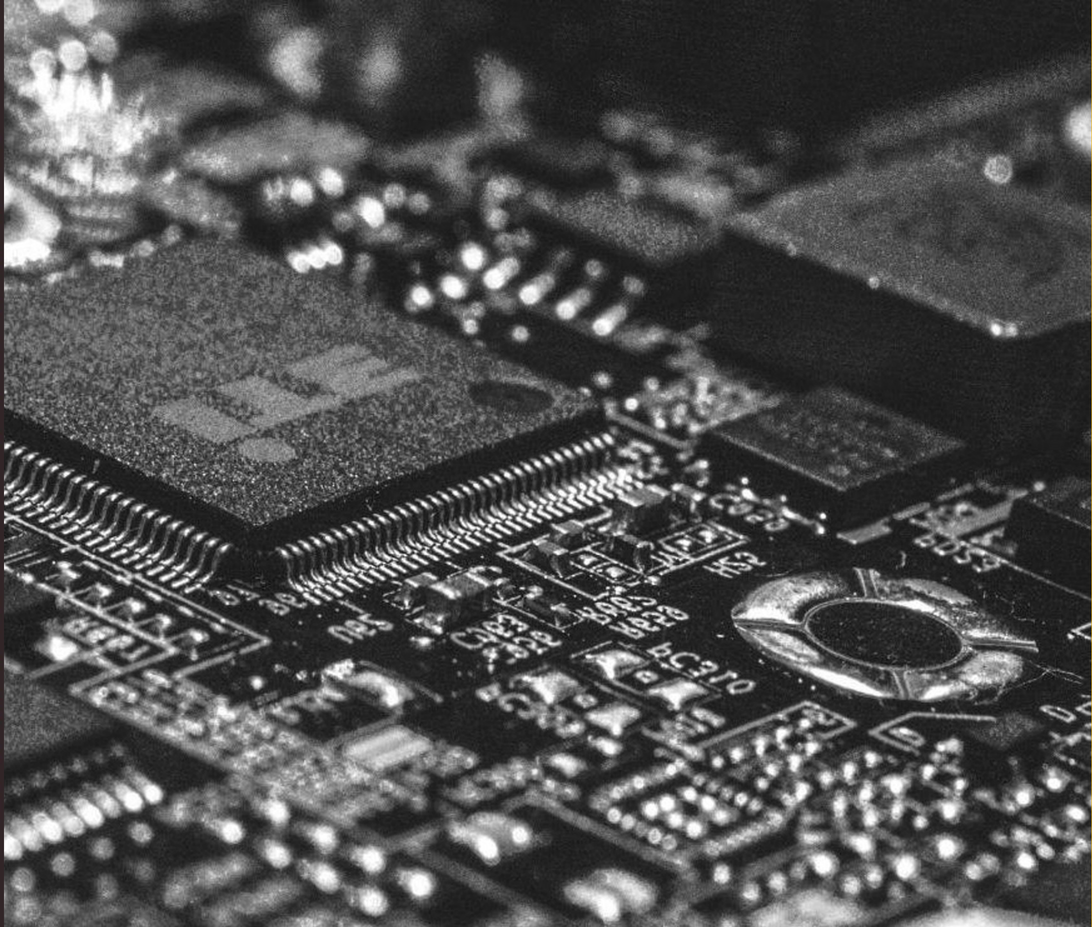
Development

Secure Development Practices
Attack Surface Reduction
Mandatory Access Control

Deployment

Identity and Asset Management
Secure Software Update
Lifecycle Security Management





OP4

SECURING IoT DEVICES
AND EMBEDDED SYSTEMS

SMART DESIGN PRINCIPLES™ FOR SECURE IOT

These are the ten most fundamental design principles you should employ to keep your IoT systems and devices secure. Find out what you're doing right – and what you may be missing.

Design Stage

The Design stage is the foundation of a product's security posture. Like architects drafting a blueprint, system design represents the most optimal time to introduce security controls, when pre-existing constraints are fewest and cost is lowest. The fundamental decisions made at this stage will dictate the effectiveness and effort required to implement (and maintain) security controls in subsequent stages – ensuring optimal cyber protection and minimizing future vulnerabilities. Fair warning: it becomes orders of magnitude more expensive to fix insecure design decisions in later stages of the product lifecycle.

DESIGN

- □ Data-at-Rest Protection
- □ Secure Boot
- □ Compartmentalization
- □ Secure Communications

1 **Data-at-Rest Protection**

Fulfillment Criteria: Software, data, and configuration files are protected against unauthorized access, modification, or deletion when stored in nonvolatile memory, usually through encryption, and sensitive cryptographic keys are stored in tamper-resistant security hardware.

2 **Secure Boot**

Fulfillment Criteria: Software, including firmware and configuration data, is digitally-signed, authenticated, and/or decrypted before use, and reset/rollback capabilities to earlier software and/or firmware revisions is prevented.

3 **Compartmentalization**

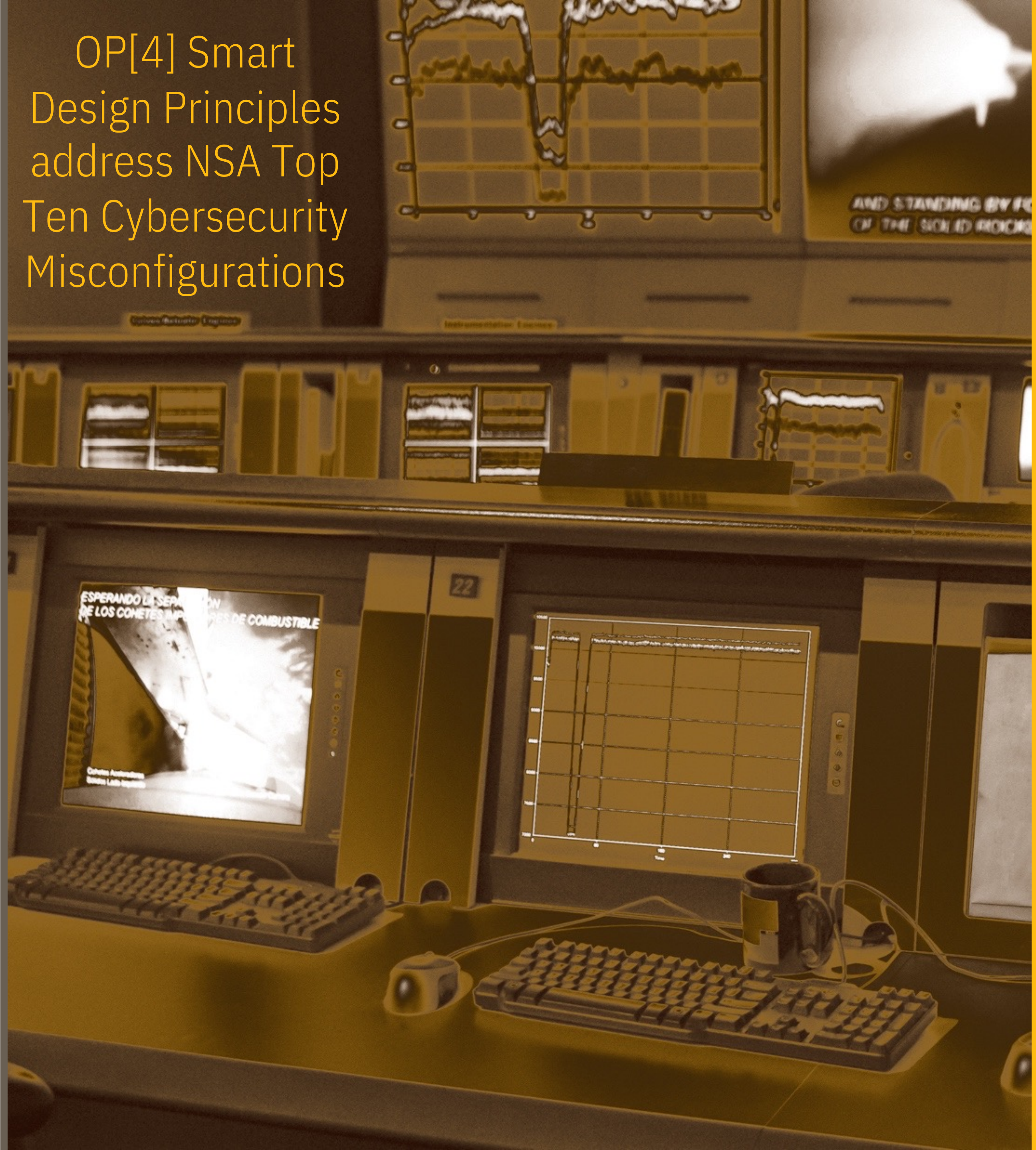
Fulfillment Criteria: Networks are segmented into distinct enclaves, dictated by system functionality and operations, while hardware compute resources are segregated to maximize independent functions. Software applications are well defined, self-contained, containerized, and logically isolated in memory and in access to devices and networks.

4 **Secure Communications**

Fulfillment Criteria: Communications with external sources are default-denied until remote sources are positively authenticated via cryptographically secure mechanisms, and data in transit is encrypted via cryptographically secure mechanisms. Encryption and decryption keys are secured at-rest, in-use, and intransit.

W op4.io E hello@op4.io P (703) 574.0280

Download the OP[4] Smart Design Principles Whitepaper



OP[4] Smart Design Principles address NSA Top Ten Cybersecurity Misconfigurations

NSA and CISA – Top Ten Cybersecurity Misconfigurations

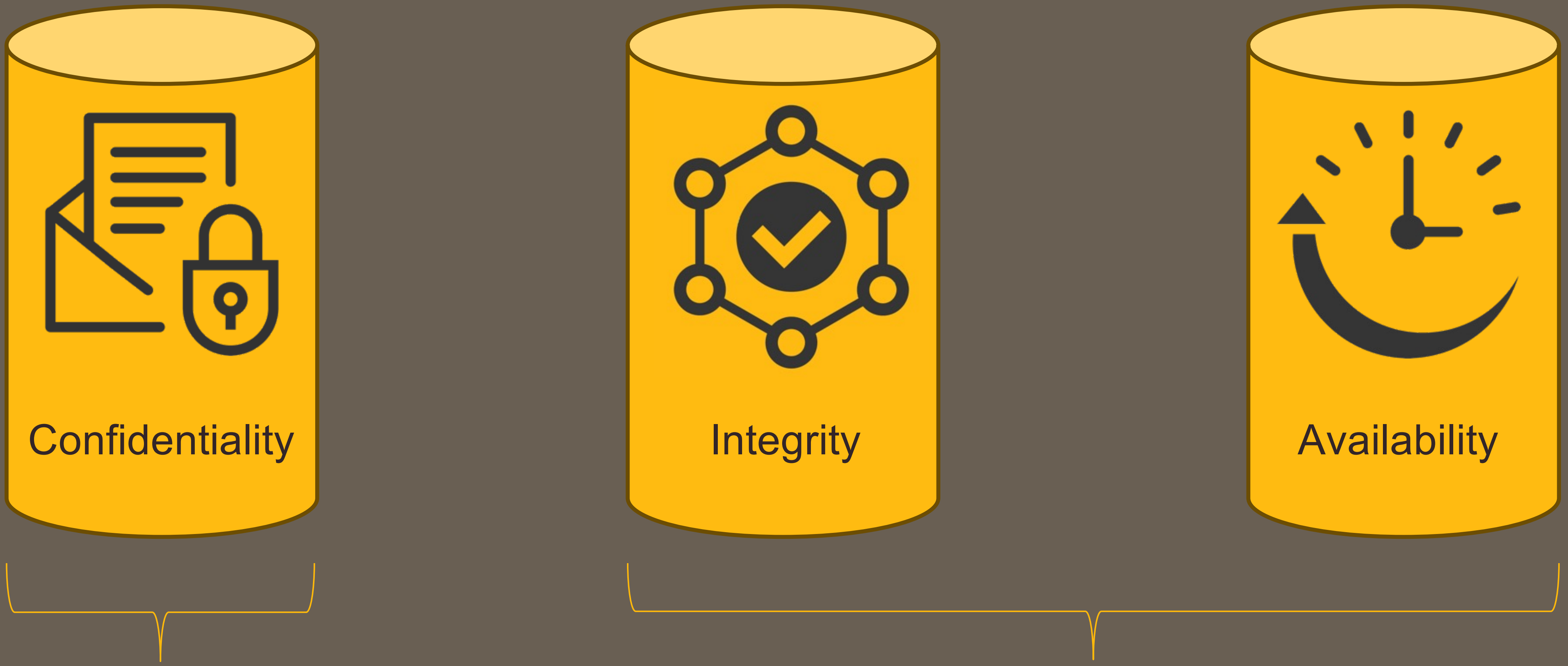
System Operations

- ✓ Default configurations of software & applications
- ✓ Improper separation of user/admin privileges
- ✓ Insufficient internal network monitoring
- ✓ Lack of network segmentation
- ✓ Poor patch management
- ✓ Bypass of system access controls
- ✓ Weak or misconfigured multifactor authentication
- ✓ Insufficient access control lists (ACLs) on network
- ✓ Poor credential hygiene
- ✓ Unrestricted code execution

Source: cisa.gov

The path towards cyber resilience

Start by assuming the attacker has root access to every subsystem



Confidentiality

Integrity

Availability

Solvable by inverting the privilege hierarchy

Make an attacker's access inconsequential

Solvable using cyber-fault-tolerant designs

Turn the attacker's access into a "don't care"

About the OP[4] Team

OP[4] was founded by established cybersecurity experts and industry leaders with a unique specialty performing offensive security assessments for embedded mission systems. The founder's groundbreaking research for DARPA has catalyzed *Automated Program Analysis* for commercial cybersecurity applications.

Don't Let the Enemy W[in]!
Take the next step
https://op4.io
hello@op4.io
[703] 574.0280

Supply Chain Risk Management Survey, Space ISAC SCRM COI

Megan Moloney, Associate Director, Defense and Security Segment, Guidehouse

2023

Supply Chain
Risk Management
Working Group

LIVE SURVEY SESSION

Megan Moloney

PURPOSE

INFORM SPACE ISAC SCRM WORKING GROUP

- **Vision:** *To promote a more secure space infrastructure through increased*
  community engagement,
  information sharing,
  supply chain visibility, and
  cyber survivability.

ILLUMINATE SPACE SCRM ENVIRONMENT

- **February 2023 Pilot Survey**
- **18 October 2023 Live Survey**

➢ **INTENDED OUTCOMES:**

- **Shared infographic and insights**
- **Starting point for collective understanding of SCRM environment**
- **SCRM Working Group priorities**

LEVEL SETTING

- You need a cell phone or laptop with connectivity
- One survey per person
- Answer based upon your experience
- Please answer all questions to allow for robust analysis
- Discussion around questions will not occur nor will there be livestreaming
- Survey will be open until end of day if extra time is needed
- Formal results will be shared
- Survey responses will be treated as anonymous, but it is requested that you provide your contact information on sign-in sheet, chat, and/or on survey if you'd like a copy of the results

LIVE COMMUNITY SCRM SURVEY

YOUR VOICE MATTERS

You can also vote at Slido.com with the code #1336294

Go to "Polls" tab on the top right

Question 1

Which best characterizes your organization?

Industry
Government
FFRDC
Academia
Other

Question 2

What is the size of your organization?

- 1-50 People
- 51-250 People
- 251-500 People
- 501-2,000 People
- 2,001-10,000 People
- 10,000+ People

Question 3

On which space segments does your organization concentrate? (Mark all that apply)

Ground Segment
Launch Segment
Link Segment
Space Segment

Question 4

Which part of the space lifecycle does your organization concentrate on? (Mark all that apply)

Research & Development
Manufacturing
Launch
On-Orbit Operations
End-of-Life/Recovery
Other

Question 5

Which of the following best describes the organization of SCRM efforts within your organization?

Centralized enterprise-wide program
Centralized oversight, decentralize execution
Siloed
Minimal/None
Other

Question 6

How would you describe your SCRM maturity?

Ad-hoc: *Not formalized; activities are ad-hoc, reactive*

Defined: *Policies, procedures, and strategies are formalized/documented but not consistently implemented*

Consistently Implemented: *Consistently implemented but no effectiveness measures are lacking*

Managed and Measurable: *Quantitative and qualitative measures of effectiveness collected across the organization and used to assess and make changes*

Optimized: *Fully institutionalized, repeatable, consistently implemented, and regularly updated based on changing needs*

Question 7

Which of the following are barriers to the successful implementation of SCRM within your organization? (Mark all that apply)

Lack of Resources
Lack of Senior Leadership Support
Lack of Capability/Technology
Unclear Roles & Responsibilities
Lack of Authority
Lack of Awareness
Lack of User Buy-In
Other

Questions 8-10: Lifecycle Ranking

Risk = Vulnerability x Threat x Severity of Impact

Question 8:

Rank each stage of the supply chain lifecycle from most vulnerable to least

Question 9:

Rank each stage of the supply chain lifecycle from most threatened to least

Question 10:

Rank each stage of the supply chain lifecycle from that likely to experience to most severe impacts to least

Question 11

Which of the following **disruptive actors** poses the most threat to your supply chain? (Mark all that apply)

State Actors – Intelligence
State Actors – Economic
Hybrid State/Non-state actors – Intelligence
Hybrid State/Non-state actors – Economic
Natural Disaster
Public Health Crisis
Other

Question 12

Which of the following disruptions poses a threat to your supply chain? (Mark all that apply)

Sourcing interruptions
Counterfeit materials
Limited supply
Limited supplier diversity
Malicious intrusion
Anti-tamper insufficiencies
Lack of Supplier Modularity
Geopolitical Instability (non-conflict)
War/Conflict
Other

Question 13

Which risk do you perceive as the greatest to your organization? (Mark all that apply)

Financial
Operational
Information and Security
Software
Reputational

Question 14

What does your organization need to strengthen supply chain risk management ?

Please provides 1-3 word response(s)

THANK YOU FOR PARTICIPATING!

YOUR VOICE MATTERS

Continue to vote at Slido.com with the code #1336294

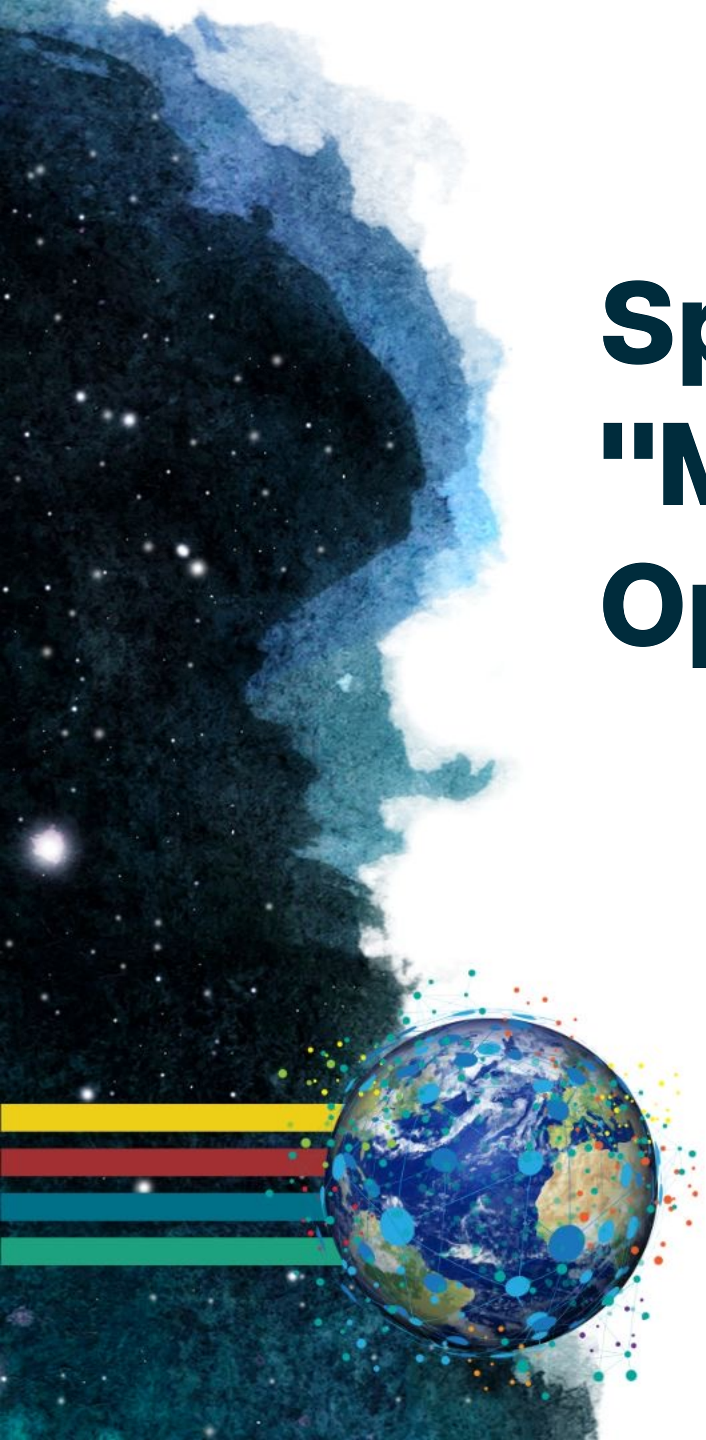
Megan M. Moloney
mmoloney@guidehouse.com
Linkedin.com/in/mmmoloney

Critical Challenges to Protecting Human Habitats On Orbit, On The Moon, And Beyond

Laura Winter, Editor & Host, Defense & Aerospace Report, The DownLink Podcast

Jason Aspiotis, Director, In-Space Infrastructure & Logistics, Axiom Space

Samuel Visner, Fellow, The Aerospace Corporation



Space ISAC AI/ML COI "Machine Learning Security Operations – MLSecOps"

Max Spolaor, Ph.D., Sr. Engineering Specialist – Advanced Autonomy, The Aerospace Corporation

Michelle Archuleta, Ph.D., Director of Data Science, RS21

Carnegie Mellon Sei Research on Securing Cyber-physical Systems in Space

Dionisio de Niz, Technical Director
Assuring Cyber Physical Systems
Directorate, Carnegie Mellon University

Cyber Threat Analysis as-a Service (CTAaaS)

William Belei, Aerospace Corporation, Cyber Operations and Resiliency Department (CORD)

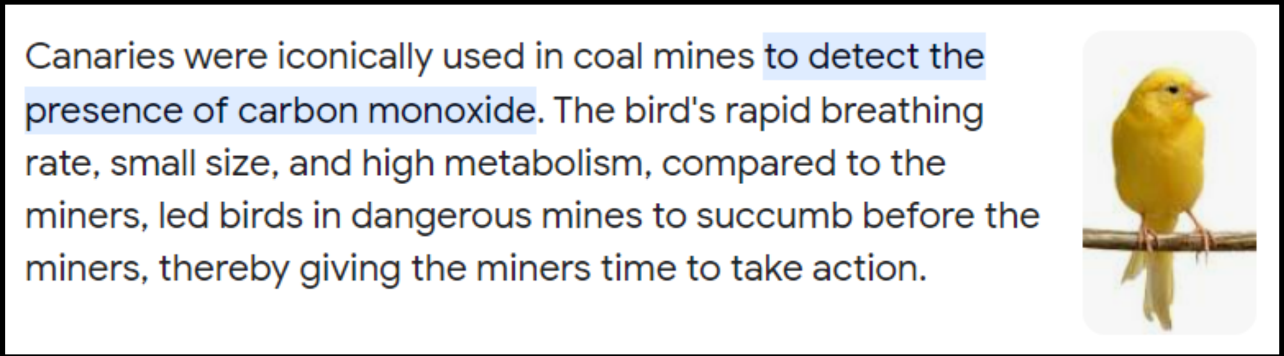
An Automated Supplemental Cyber Risk Assessment Tool that Leverages Open-Source Cyber Threat Intelligence (CTI)

William Belei,
Aerospace Corporation,
Cyber Operations and Resiliency Department (CORD)

2023-10-18

Types of Canaries

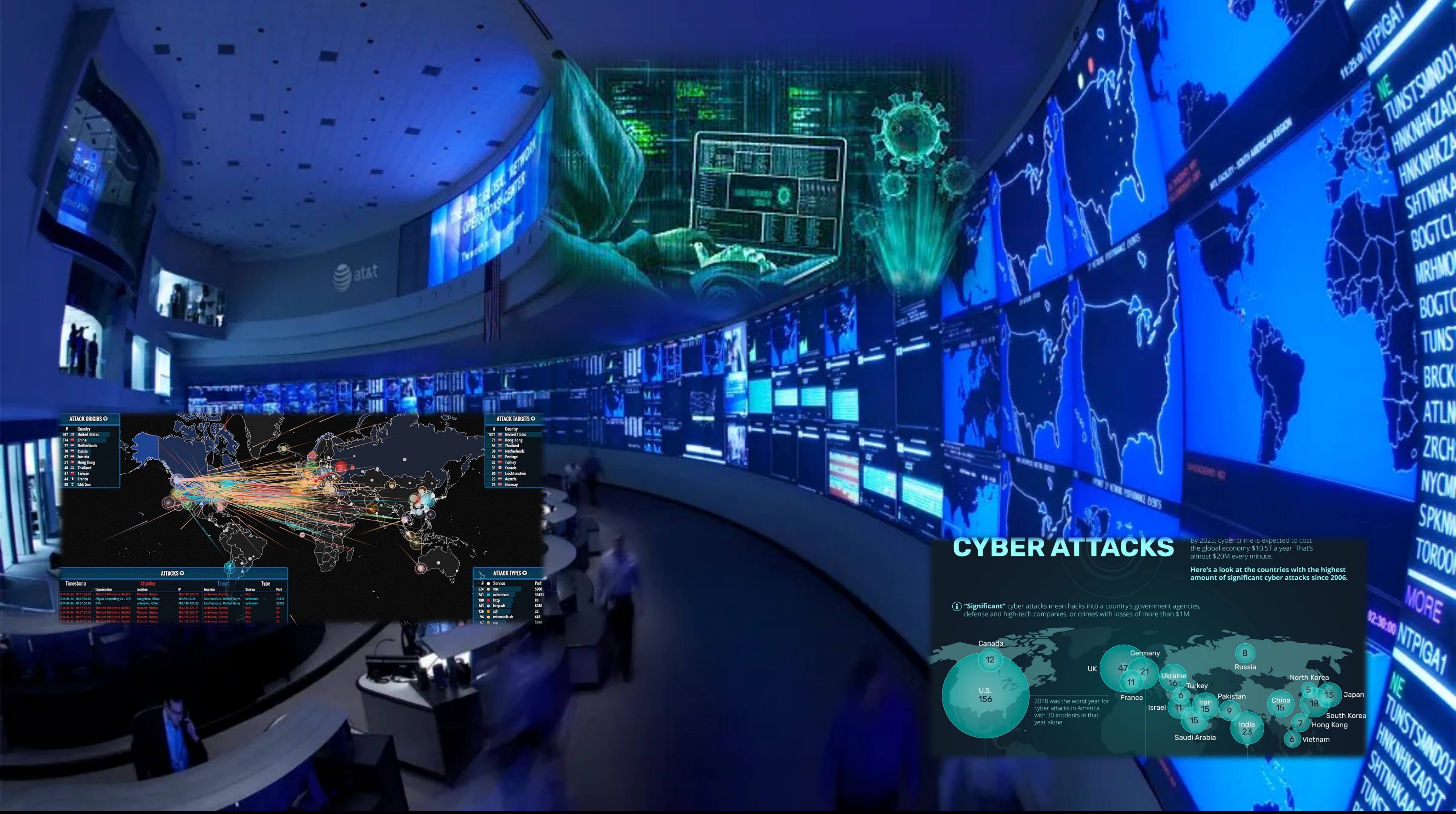
Canaries in Coal Mines



Canaries were iconically used in coal mines to detect the presence of carbon monoxide. The bird's rapid breathing rate, small size, and high metabolism, compared to the miners, led birds in dangerous mines to succumb before the miners, thereby giving the miners time to take action.

Border Fancy Canary

Photo credit: https://en.wikipedia.org/wiki/Canary



ATTACK ORIGINS

#	Country
907	United States
574	China
77	Netherlands
70	Russia
67	Austria
51	Hong Kong
48	Thailand
47	Taiwan
44	France
38	Mil/Gov

ATTACK TARGETS

#	Country
1871	United States
73	Hong Kong
55	Thailand
39	Netherlands
34	Portugal
32	Turkey
31	Canada
30	Liechtenstein
23	Austria
23	Norway

ATTACKS

Timestamp	Attacker			Target	Type	
	Organization	Location	IP	Location	Service	Port
2014-06-26 10:57:53.23	Thefirst-RU clients (WebDC	Moscow, Russia	188.120.225.71	unknown, Austria	http	80
2014-06-26 10:57:54.85	Aliyun Computing Co., LTD	Hangzhou, China	182.92.75.26	San Francisco, United States	unknown	33435
2014-06-26 10:57:54.86	N/A	unknown, Chile	190.110.121.93	San Francisco, United States	unknown	33435
2014-06-26 10:57:57.52	Thefirst-RU clients (WebDC	Moscow, Russia	188.120.225.71	unknown, Austria	http	80
2014-06-26 10:57:57.53	Thefirst-RU clients (WebDC	Moscow, Russia	188.120.225.71	unknown, Austria	http	80
2014-06-26 10:57:57.53	Thefirst-RU clients (WebDC	Moscow, Russia	188.120.225.71	unknown, Austria	http	80
2014-06-26 10:57:57.54	Thefirst-RU clients (WebDC	Moscow, Russia	188.120.225.71	unknown, Austria	http	80

ATTACK TYPES

#	Service	Port
524	vnc	5900
241	unknown	33435
180	http	80
143	http-alt	8080
126	ssh	22
94	microsoft-ds	445
67	sip	5060

CYBER ATTACKS

By 2025, cyber crime is expected to cost the global economy $10.5T a year. That's almost $20M every minute.

Here's a look at the countries with the highest amount of significant cyber attacks since 2006.

ⓘ **"Significant"** cyber attacks mean hacks into a country's government agencies, defense and high-tech companies, or crimes with losses of more than $1M.

2018 was the worst year for cyber attacks in America, with 30 incidents in that year alone.

Air Force Customer Turned to Aerospace For Help In Developing a Pragmatic Way of Leveraging Real-World Cyber Threat Intel (CTI)

- Customer: **Authorizing Official** (AO) office with significant resource limitations and looking to significantly increase the efficacy of their Cyber Risk Assessments. The approach had the following requirements/Imitations:
  - Must be mostly automated
  - Measure a given system's strategic level cyber risk posture
  - Use the system's non-compliant security controls to represent the system's vulnerabilities
  - Use existing open-source CTI to represent real-world Threat Sources and Threat Events (no-classified sources (at first))

Note: need to compress a pretty complex topic into 30 minutes. Happily available for follow on engagements to explain the methodology in more detail!

What Did Aerospace Learn and How Did We Apply That to a Solution?

A Virtual Global Network of Canaries in Cyber Coal Mines Exists!

Challenges Have Driven Organizations to Use Junk Science

Aerospace Developed a Methodology to Leverage ATT&CK, a CTID Mapping, and NIST SP 800-30

A Virtual Global Network of Canaries in Cyber Coal Mines Exists!

What Did Aerospace Learn and How Did We Apply That to a Solution?

A Virtual Global Network of Canaries in Cyber Coal Mines Exists!

Challenges Have Driven Organizations to Use Junk Science

Aerospace Developed a Methodology to Leverage ATT&CK, a CTID Mapping, and NIST SP 800-30

Challenges Have Driven Organizations to Use Junk Science

What Did Aerospace Learn and How Did We Apply That to a Solution?

A Virtual Global Network of Canaries in Cyber Coal Mines Exists!

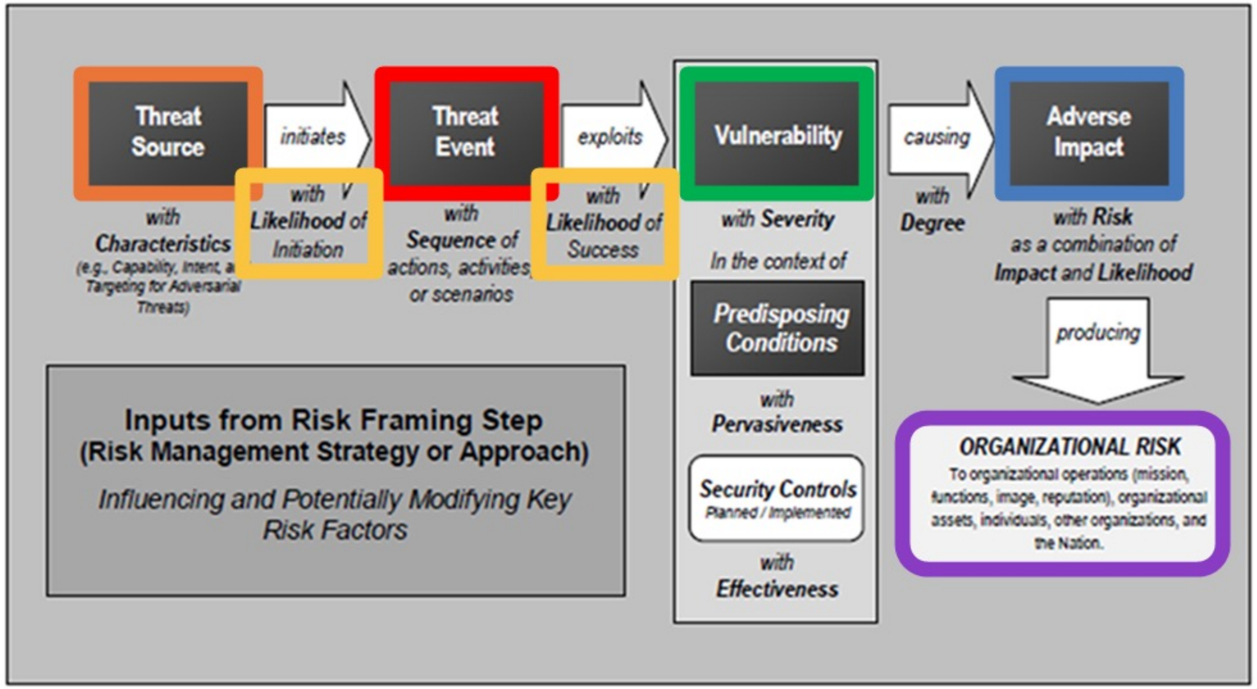
Challenges Have Driven Organizations to Use Junk Science

Aerospace Developed a Methodology to Leverage ATT&CK, a CTID Mapping, and NIST SP 800-30

Aerospace Developed a Methodology to Leverage ATT&CK, a CTID Mapping, and NIST SP 800-30

NIST says to employ a risk model to accomplish these 3 steps:

1) Document all relevant: VUs, TEs, and TSs.
2) Analyze every possible combination to determine LI, IM, and resulting risk of each
3) Aggregate and analyze results



Threat Source

initiates

with Likelihood of Initiation

with Characteristics (e.g., Capability, Intent, a Targeting for Adversarial Threats)

Threat Event

exploits

with Likelihood of Success

with Sequence of actions, activities, or scenarios

Vulnerability

with Severity

In the context of

Predisposing Conditions

with Pervasiveness

Security Controls Planned / Implemented

with Effectiveness

causing

with Degree

Adverse Impact

with Risk as a combination of Impact and Likelihood

producing

ORGANIZATIONAL RISK

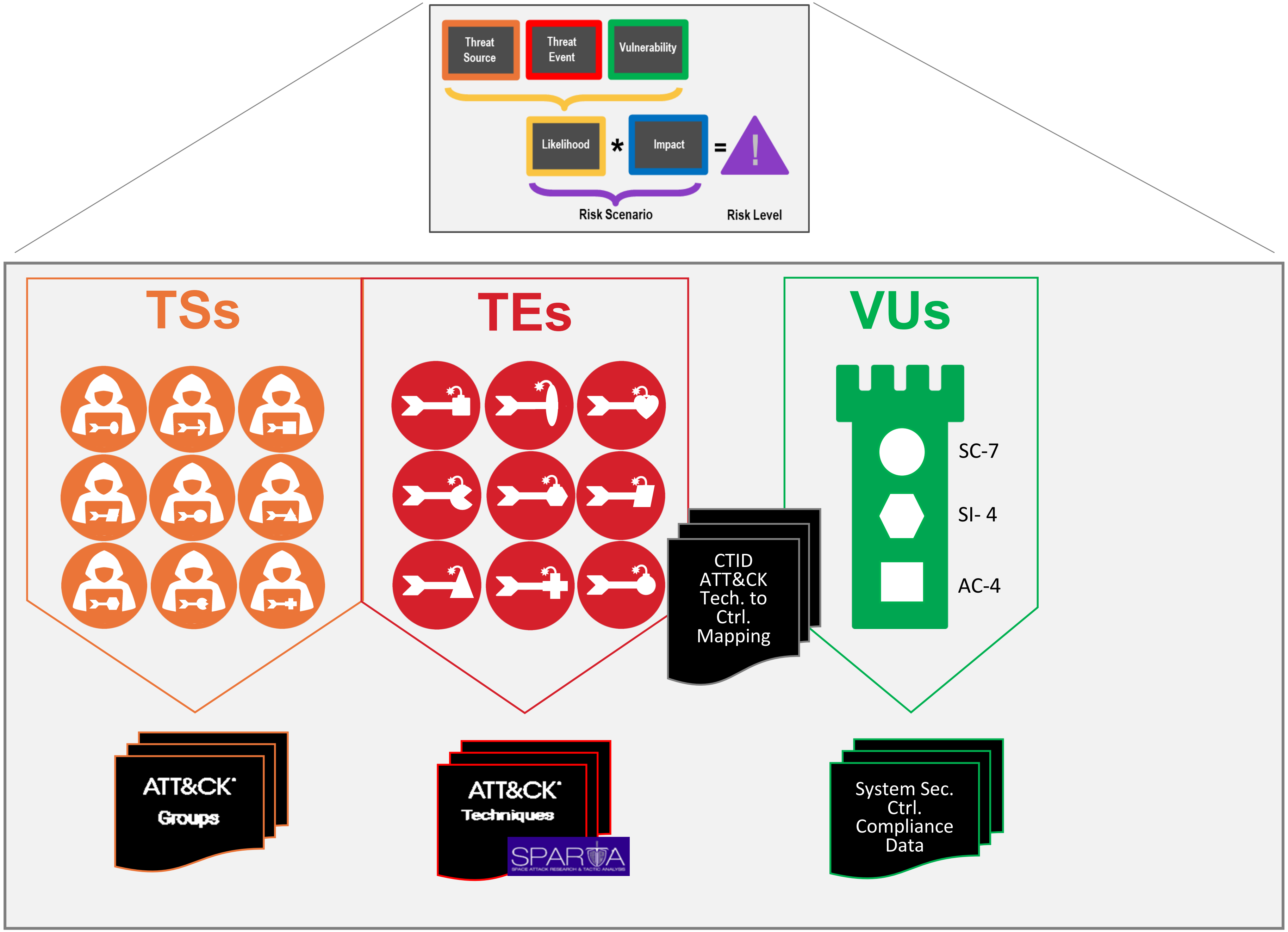
To organizational operations (mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation.

Inputs from Risk Framing Step (Risk Management Strategy or Approach)

Influencing and Potentially Modifying Key Risk Factors

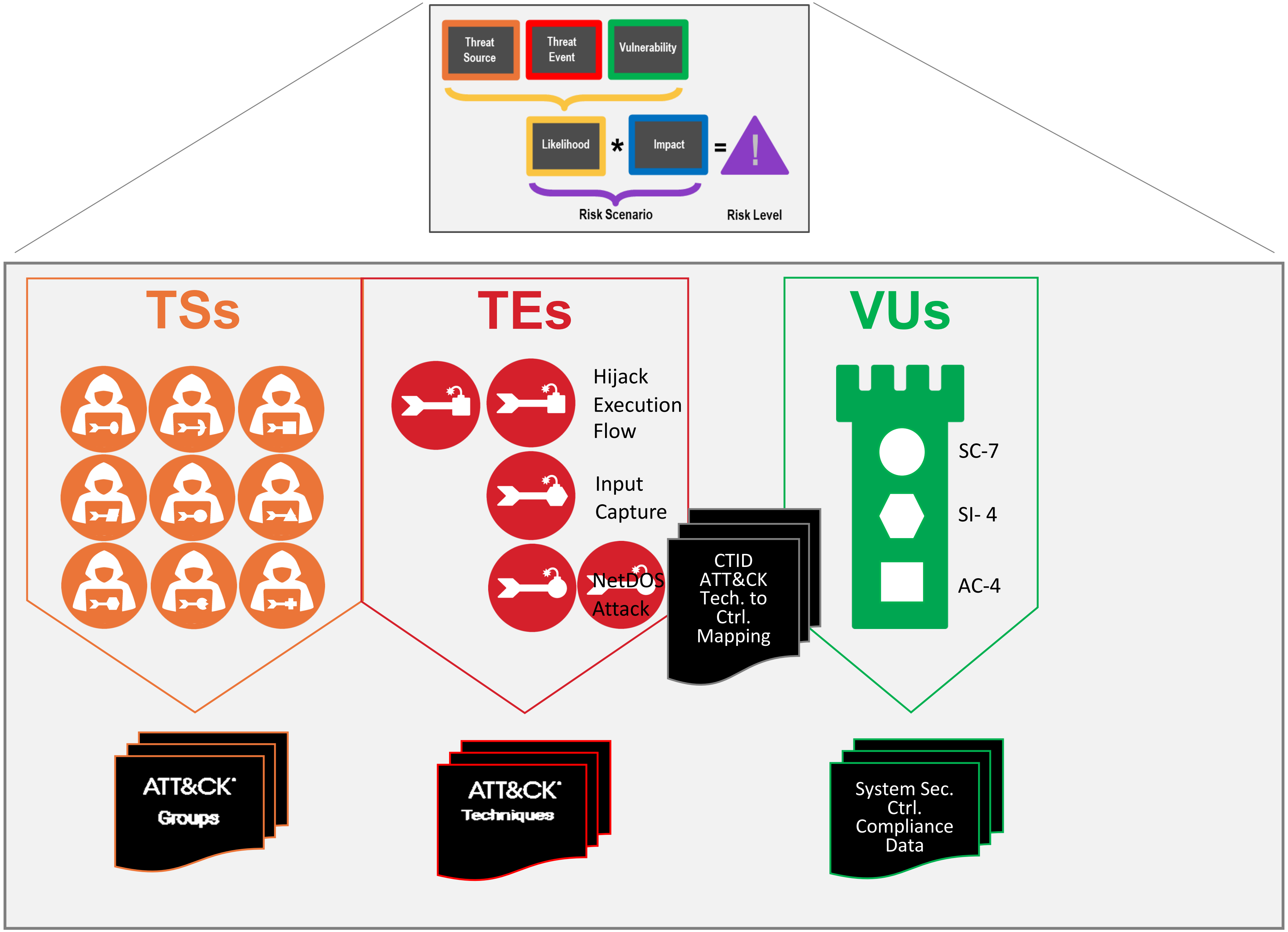
NIST says to employ a risk model to accomplish these 3 steps:

1) Document all relevant: VUs, TEs, and TSs.
2) Analyze every possible combination to determine LI, IM, and resulting risk of each
3) Aggregate and analyze results



NIST says to employ a risk model to accomplish these 3 steps:

1) Document all relevant: VUs, TEs, and TSs.
2) Analyze every possible combination to determine LI, IM, and resulting risk of each
3) Aggregate and analyze results

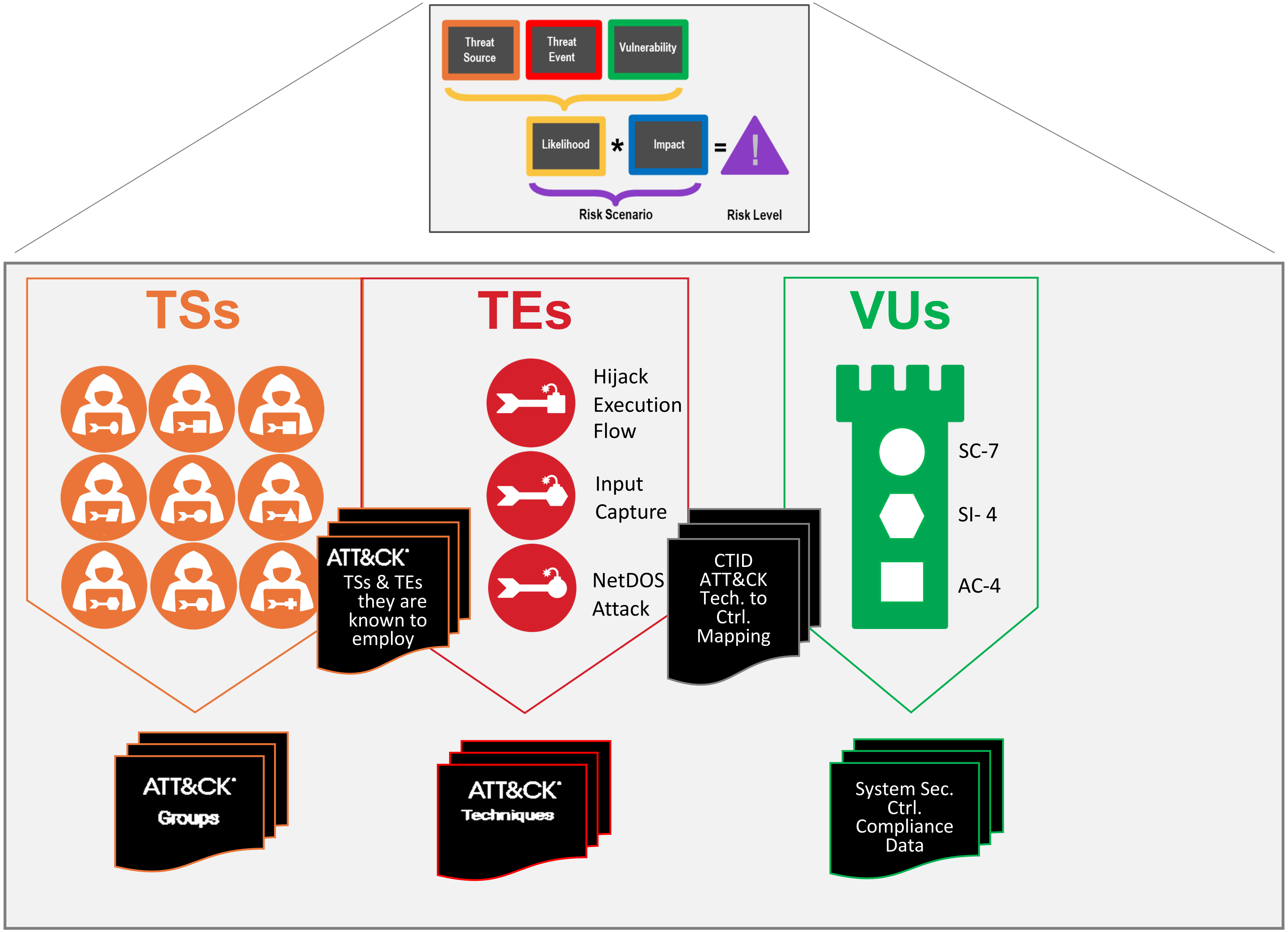


NIST says to employ a risk model to accomplish these 3 steps:

✓ Document all relevant: VUs, TEs, and TSs.

2) Analyze every possible combination to determine LI, IM, and resulting risk of each

3) Aggregate and analyze results



Threat Source

Threat Event

Vulnerability

Likelihood * Impact = !

Risk Scenario

Risk Level

TSs

TEs

VUs

Hijack Execution Flow

Input Capture

NetDOS Attack

SC-7

SI- 4

AC-4

ATT&CK® TSs & TEs they are known to employ

CTID ATT&CK Tech. to Ctrl. Mapping

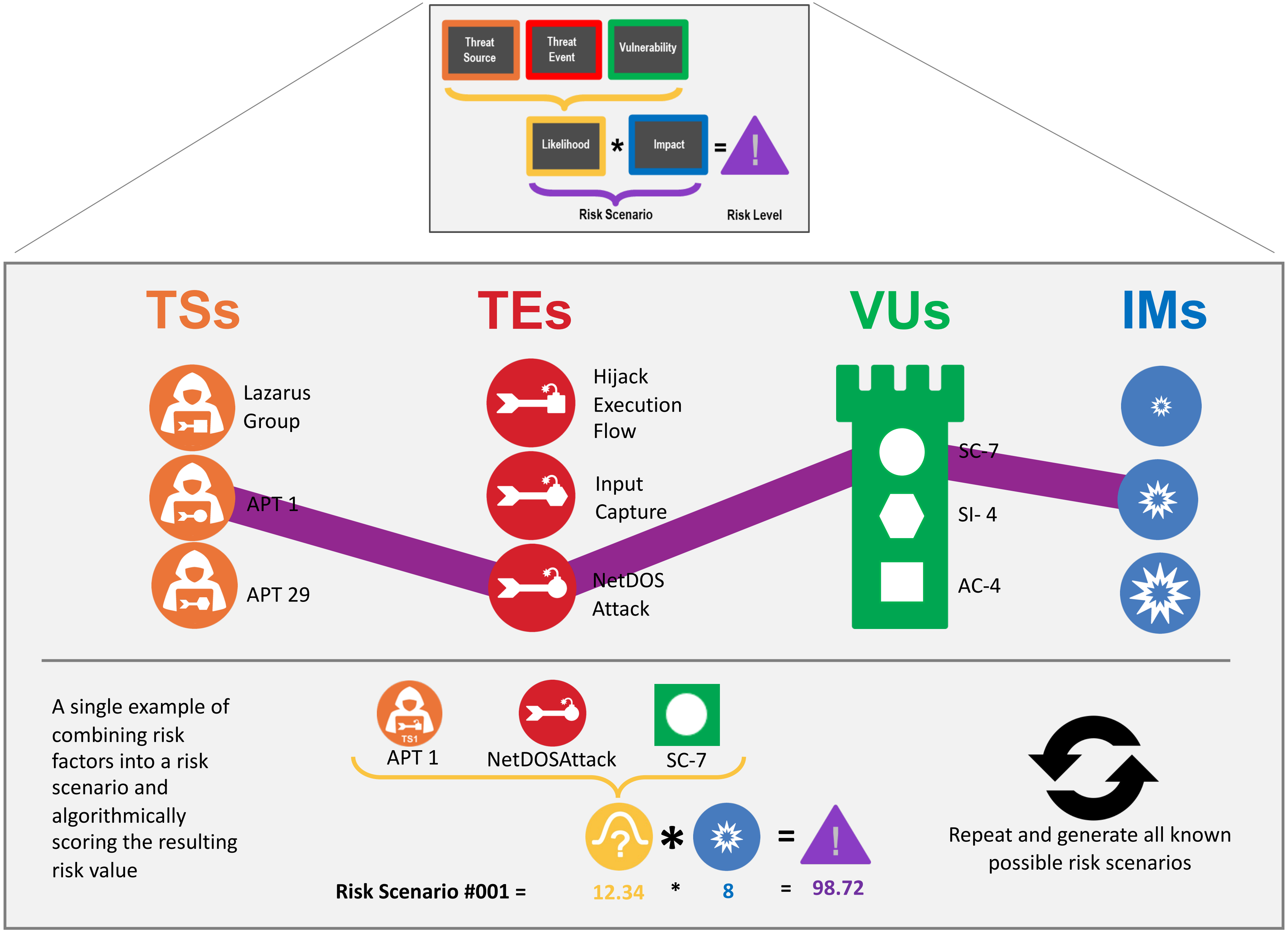
ATT&CK® Groups

ATT&CK® Techniques

System Sec. Ctrl. Compliance Data

NIST says to employ a risk model to accomplish these 3 steps:

- ✓ Document all relevant: VUs, TEs, and TSs.
- ✓ Analyze every possible combination to determine LI, IM, and resulting risk of each
- 3) Aggregate and analyze results



Threat Source

Threat Event

Vulnerability

Likelihood * Impact = !

Risk Scenario

Risk Level

TSs

Lazarus Group

APT 1

APT 29

TEs

Hijack Execution Flow

Input Capture

NetDOS Attack

VUs

SC-7

SI- 4

AC-4

IMs

A single example of combining risk factors into a risk scenario and algorithmically scoring the resulting risk value

APT 1

NetDOSAttack

SC-7

Risk Scenario #001 = 12.34 * 8 = 98.72

Repeat and generate all known possible risk scenarios

NIST says to employ a risk model to accomplish these 3 steps:

✓ Document all relevant: VUs, TEs, and TSs.

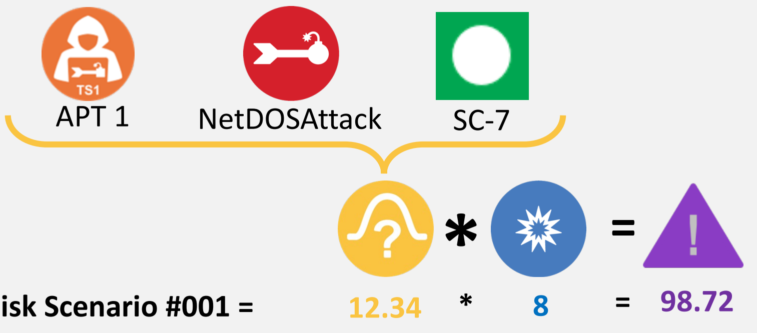
✓ Analyze every possible combination to determine LI, IM, and resulting risk of each

3) Aggregate and analyze results

CYBER RISK REGISTER (CRR)

Risk Scenario #001 APT 1|NetDOSAttack|NonComp SC-7|LI-12.34|IM-8 – 98.72

A single example of combining risk factors into a risk scenario and algorithmically scoring the resulting risk value



Risk Scenario #001 = 12.34 * 8 = 98.72

Repeat and generate all known possible risk scenarios

CYBER RISK REGISTER (CRR)

Risk Scenario #001 APT 1|NetDOSAttack|NonComp SC-7|LI-12.34|IM-8 – 98.72

How can we analyze this aggregated cyber risk information and thereby turn that CTI into actionable information?

CYBER RISK REGISTER (CRR)

Risk Scenario #001 APT 1|NetDOSAttack|NonComp SC-7|LI-12.34|IM-8 – 98.72

Risk Scenario #002 APT 3|Phishing|NonComp Ctrl 2,10|LI-2.12|IM-2 – 4.23

Risk Scenario #003 APT 29|UserExecution|NonComp Ctrl 1|LI-29.31|IM-10 – 293.06

Risk Scenario #004 AquaticPanda|ModifyExecution|NonComp Ctrl 83|LI-8.29|IM-4 – 33.17

Risk Scenario #005 Chimera|NetReconScan|NonComp Ctrl 49,91,139|LI-4.43|IM-8 – 35.46

Risk Scenario #006 APT 1|HijackExecutionFlow|NonComp Ctrl 82,77|LI-0.72|IM-2 – 1.44

Risk Scenario #007 APT 29|ImplantImage|NonComp Ctrl 4,9,37,111|LI-22.81|IM-4 – 91.27

Risk Scenario #008 DarkHotel|ModifyExecution|NonComp Ctrl 1,3,78,317|LI-11.41|IM-2 – 22.83

Risk Scenario #009 APT 41|HijackExecutionFlow|NonComp Ctrl 96,229|LI-3.86|IM-2 – 7.22

Risk Scenario #010 APT 29|ModifyExecution|NonComp Ctrl 1,10,29,119|IM-18.29|IM-10 – 182.89

Risk Scenario #011 Sandworm|Rootkit|NonComp Ctrl 1,72,73,88|LI-1.86|IM-6 – 11.18

Risk Scenario #012 APT 29|Rootkit|NonComp Ctrl 1,3,233|LI-12.38|LI-16.52|IM-6 – 99.09

Risk Scenario #013 Machete|HijackExecutionFlow|NonComp Ctrl 166,167|LI-5.13|IM-10 – 51.26

Risk Scenario #014 WizardSpider|ModifyExecution|NonComp Ctrl 201,229|LI-38.86|IM-2 – 77.72

Risk Scenario #015 APT 29|HijackExecutionFlow|NonComp Ctrl 1,89,121|LI-45.75|IM-4 – 183.82

We can we systematically, automatically, and consistently evaluate the risk of a given system with respect to the TS Groups and TE Techniques in MITRE ATT&CK to derive a risk posture score.

CYBER RISK REGISTER (CRR)

Risk Scenario #001 APT 1|NetDOSAttack|NonComp SC-7|LI-12.34|IM-8 – 98.72

Risk Scenario #002 APT 3|Phishing|NonComp Ctrl 2,10|LI-2.12|IM-2 – 4.23

Risk Scenario #003 APT 29|UserExecution|NonComp Ctrl 1|LI-29.31|IM-10 – 293.06

Risk Scenario #004 AquaticPanda|ModifyExecution|NonComp Ctrl 83|LI-8.29|IM-4 – 33.17

Risk Scenario #005 Chimera|NetReconScan|NonComp Ctrl 49,91,139|LI-4.43|IM-8 – 35.46

Risk Scenario #006 APT 1|HijackExecutionFlow|NonComp Ctrl 82,77|LI-0.72|IM-2 – 1.44

Risk Scenario #007 APT 29|ImplantImage|NonComp Ctrl 4,9,37,111|LI-22.81|IM-4 – 91.27

Risk Scenario #008 DarkHotel|ModifyExecution|NonComp Ctrl 1,3,78,317|LI-11.41|IM-2 – 22.83

Risk Scenario #009 APT 41|HijackExecutionFlow|NonComp Ctrl 96,229|LI-3.86|IM-2 – 7.22

Risk Scenario #010 APT 29|ModifyExecution|NonComp Ctrl 1,10,29,119|IM-18.29|IM-10 – 182.89

Risk Scenario #011 Sandworm|Rootkit|NonComp Ctrl 1,72,73,88|LI-1.86|IM-6 – 11.18

Risk Scenario #012 APT 29|Rootkit|NonComp Ctrl 1,3,233|LI-12.38|LI-16.52|IM-6 – 99.09

Risk Scenario #013 Machete|HijackExecutionFlow|NonComp Ctrl 166,167|LI-5.13|IM-10 – 51.26

Risk Scenario #014 WizardSpider|ModifyExecution|NonComp Ctrl 201,229|LI-38.86|IM-2 – 77.72

Risk Scenario #015 APT 29|HijackExecutionFlow|NonComp Ctrl 1,89,121|LI-45.75|IM-4 – 183.82

2,527 total risk

How about finding out which TE Techniques our system is the most risk exposed to (again, based on the data in ATT&CK) so we can prioritize mitigations?

CYBER RISK REGISTER (CRR)

Risk Scenario #001 APT 1|NetDOSAttack|NonComp SC-7|LI-12.34|IM-8 – 98.72

Risk Scenario #002 APT 3|Phishing|NonComp Ctrl 2,10|LI-2.12|IM-2 – 4.23

Risk Scenario #003 APT 29|UserExecution|NonComp Ctrl 1|LI-29.31|IM-10 – 293.06

Risk Scenario #004 AquaticPanda|ModifyExecution|NonComp Ctrl 83|LI-8.29|IM-4 – 33.17

Risk Scenario #005 Chimera|NetReconScan|NonComp Ctrl 49,91,139|LI-4.43|IM-8 – 35.46

Risk Scenario #006 APT 1|HijackExecutionFlow|NonComp Ctrl 82,77|LI-0.72|IM-2 – 1.44

Risk Scenario #007 APT 29|ImplantImage|NonComp Ctrl 4,9,37,111|LI-22.81|IM-4 – 91.27

Risk Scenario #008 DarkHotel|ModifyExecution|NonComp Ctrl 1,3,78,317|LI-11.41|IM-2 – 22.83

Risk Scenario #009 APT 41|HijackExecutionFlow|NonComp Ctrl 96,229|LI-3.86|IM-2 – 7.22

Risk Scenario #010 APT 29|ModifyExecution|NonComp Ctrl 1,10,29,119|IM-18.29|IM-10 – 182.89

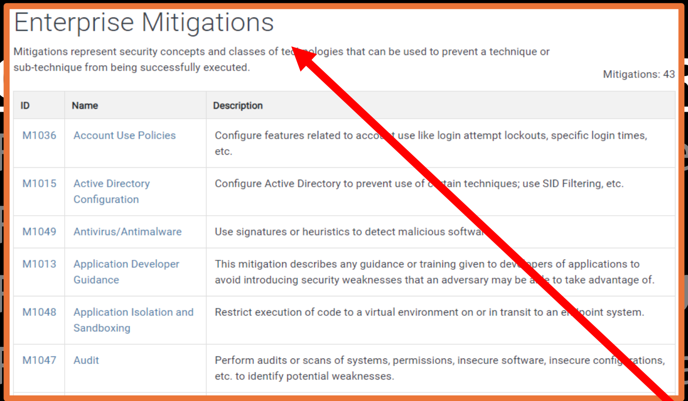
Risk Scenario #011 Sandworm|Rootkit|NonComp Ctrl 1,72,73,88|LI-1.86|IM-6 – 11.18

Risk Scenario #012 APT 29|Rootkit|NonComp Ctrl 1,3,233|LI-12.38|LI-16.52|IM-6 – 99.09

Risk Scenario #013 Machete|HijackExecutionFlow|NonComp Ctrl 166,167|LI-5.13|IM-10 – 51.26

Risk Scenario #014 WizardSpider|ModifyExecution|NonComp Ctrl 201,229|LI-38.86|IM-2 – 77.72

Risk Scenario #015 APT 29|HijackExecutionFlow|NonComp Ctrl 1,89,121|LI-45.75|IM-4 – 183.82

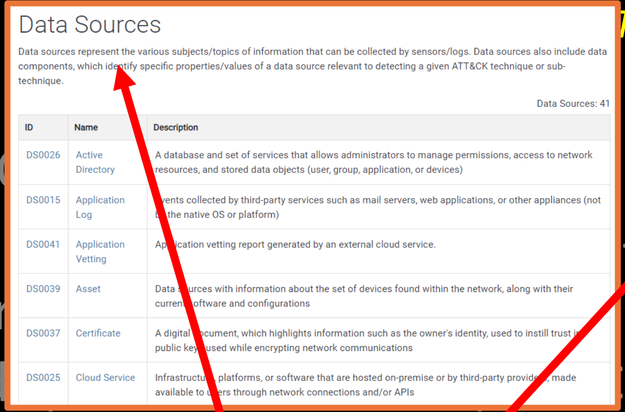


Enterprise Mitigations

Mitigations represent security concepts and classes of technologies that can be used to prevent a technique or sub-technique from being successfully executed.

Mitigations: 43

ID	Name	Description
M1036	Account Use Policies	Configure features related to account use like login attempt lockouts, specific login times, etc.
M1015	Active Directory Configuration	Configure Active Directory to prevent use of certain techniques; use SID Filtering, etc.
M1049	Antivirus/Antimalware	Use signatures or heuristics to detect malicious software.
M1013	Application Developer Guidance	This mitigation describes any guidance or training given to developers of applications to avoid introducing security weaknesses that an adversary may be able to take advantage of.
M1048	Application Isolation and Sandboxing	Restrict execution of code to a virtual environment on or in transit to an endpoint system.
M1047	Audit	Perform audits or scans of systems, permissions, insecure software, insecure configurations, etc. to identify potential weaknesses.



Data Sources

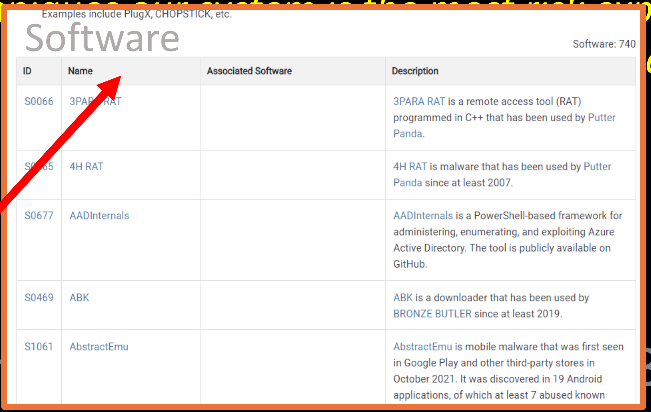
Data sources represent the various subjects/topics of information that can be collected by sensors/logs. Data sources also include data components, which identify specific properties/values of a data source relevant to detecting a given ATT&CK technique or sub-technique.

Data Sources: 41

ID	Name	Description
DS0026	Active Directory	A database and set of services that allows administrators to manage permissions, access to network resources, and stored data objects (user, group, application, or devices)
DS0015	Application Log	Events collected by third-party services such as mail servers, web applications, or other appliances (not by the native OS or platform)
DS0041	Application Vetting	Application vetting report generated by an external cloud service.
DS0039	Asset	Data sources with information about the set of devices found within the network, along with their current software and configurations
DS0037	Certificate	A digital document, which highlights information such as the owner's identity, used to instill trust in public keys used while encrypting network communications
DS0025	Cloud Service	Infrastructure, platforms, or software that are hosted on-premise or by third-party providers, made available to users through network connections and/or APIs

Techniques our system is the most risk exposed to (again, based on

an prioritize mitigations?



Examples include PlugX, CHOPSTICK, etc.

Software

Software: 740

ID	Name	Associated Software	Description
S0066	3PARA RAT		3PARA RAT is a remote access tool (RAT) programmed in C++ that has been used by Putter Panda.
S0065	4H RAT		4H RAT is malware that has been used by Putter Panda since at least 2007.
S0677	AADInternals		AADInternals is a PowerShell-based framework for administering, enumerating, and exploiting Azure Active Directory. The tool is publicly available on GitHub.
S0469	ABK		ABK is a downloader that has been used by BRONZE BUTLER since at least 2019.
S1061	AbstractEmu		AbstractEmu is mobile malware that was first seen in Google Play and other third-party stores in October 2021. It was discovered in 19 Android applications, of which at least 7 abused known

And, what kind of help can ATT&CK provide towards the pragmatic steps to address these techniques?

Risk Scenario #005 Chimera|NetReconScan|NonComp Ctrl 49,91,139|LI-4.43|IM-8 – 35.46

Risk Scenario #006 APT 1|HijackExecutionFlow|NonComp Ctrl 82,77|LI-0.72|IM-2 – 1.44

Risk Scenario #007 APT 29|ImplantImage|NonComp Ctrl 4,9,37,111|LI-22.81|IM-4 – 91.27

Risk Scenario #008 DarkHotel|ModifyExecution|NonComp Ctrl 1,3,78,317|LI-11.41|IM-2 – 22.83

Risk Scenario #009 APT 41|HijackExecutionFlow|NonComp Ctrl 96,229|LI-3.86|IM-2 – 7.22

Risk Scenario #010 APT 29|ModifyExecution|NonComp Ctrl 1,10,29,119|IM-18.29|IM-10 – 182.89

Risk Scenario #011 Sandworm|Rootkit|NonComp Ctrl 1,72,73,88|LI-1.86|IM-6 – 11.18

Risk Scenario #012 APT 29|Rootkit|NonComp Ctrl 1,3,233|LI-12.38|LI-16.52|IM-6 – 99.09

Risk Scenario #013 Machete|HijackExecutionFlow|NonComp Ctrl 166,167|LI-5.13|IM-10 – 51.26

Risk Scenario #014 WizardSpider|ModifyExecution|NonComp Ctrl 201,229|LI-38.86|IM-2 – 77.72

Risk Scenario #015 APT 29|HijackExecutionFlow|NonComp Ctrl 1,89,121|LI-45.75|IM-4 – 183.82

And how about using the above to inform our Red and Blue Teams as to which TTPs to prioritize for cyber training and exercises?

How about objectively prioritizing cyber mitigations investments. Ex. Should we focus resources on mitigating risks by implementing security Ctrl 1 or Ctrl 2? Which is the higher priority?

CYBER RISK REGISTER (CRR)

Risk Scenario #001 APT 1|NetDOSAttack|NonComp SC-7|LI-12.34|IM-8 – 98.72

Risk Scenario #002 APT 3|Phishing|NonComp Ctrl 2,10|LI-2.12|IM-2 – 4.23

Risk Scenario #003 APT 29|UserExecution|NonComp Ctrl 1 LI-29.31|IM-10 – 293.06

Risk Scenario #004 AquaticPanda|ModifyExecution|NonComp Ctrl 83|LI-8.29|IM-4 – 33.17

Risk Scenario #005 Chimera|NetReconScan|NonComp Ctrl 49,91,139|LI-4.43|IM-8 – 35.46

Risk Scenario #006 APT 1|HijackExecutionFlow|NonComp Ctrl 82,77|LI-0.72|IM-2 – 1.44

Risk Scenario #007 APT 29|ImplantImage|NonComp Ctrl 4,9,37,111|LI-22.81|IM-4 – 91.27

Risk Scenario #008 DarkHotel|ModifyExecution|NonComp Ctrl 1,3,78,317|LI-11.41|IM-2 – 22.83

Risk Scenario #009 APT 41|HijackExecutionFlow|NonComp Ctrl 96,229|LI-3.86|IM-2 – 7.22

Risk Scenario #010 APT 29|ModifyExecution|NonComp Ctrl 1,10,29,119|IM-18.29|IM-10 – 182.89

Risk Scenario #011 Sandworm|Rootkit|NonComp Ctrl 1,72,73,88|LI-1.86|IM-6 – 11.18

Risk Scenario #012 APT 29|Rootkit|NonComp Ctrl 1,3,233|LI-12.38|LI-16.52|IM-6 – 99.09

Risk Scenario #013 Machete|HijackExecutionFlow|NonComp Ctrl 166,167|LI-5.13|IM-10 – 51.26

Risk Scenario #014 WizardSpider|ModifyExecution|NonComp Ctrl 201,229|LI-38.86|IM-2 – 77.72

Risk Scenario #015 APT 29|HijackExecutionFlow|NonComp Ctrl 1,89,121|LI-45.75|IM-4 – 183.82

Objectively prioritizing cyber intelligence Requests For Information (RFIs).

CYBER RISK REGISTER (CRR)

Risk Scenario #001 APT 1|NetDOSAttack|NonComp SC-7|LI-12.34|IM-8 – 98.72

Risk Scenario #002 APT 3|Phishing|NonComp Ctrl 2,10|LI-2.12|IM-2 – 4.23

Risk Scenario #003 APT 29|UserExecution|NonComp Ctrl 1|LI-29.31|IM-10 – 293.06

Risk Scenario #004 AquaticPanda|ModifyExecution|NonComp Ctrl 83|LI-8.29|IM-4 – 33.17

Risk Scenario #005 Chimera|NetReconScan|NonComp Ctrl 49,91,139|LI-4.43|IM-8 – 35.46

Risk Scenario #006 APT 1|HijackExecutionFlow|NonComp Ctrl 82,77|LI-0.72|IM-2 – 1.44

Risk Scenario #007 APT 29|ImplantImage|NonComp Ctrl 4,9,37,111|LI-22.81|IM-4 – 91.27

Risk Scenario #008 DarkHotel|ModifyExecution|NonComp Ctrl 1,3,78,317|LI-11.41|IM-2 – 22.83

Risk Scenario #009 APT 41|HijackExecutionFlow|NonComp Ctrl 96,229|LI-3.86|IM-2 – 7.22

Risk Scenario #010 APT 29|ModifyExecution|NonComp Ctrl 1,10,29,119|IM-18.29|IM-10 – 182.89

Risk Scenario #011 Sandworm|Rootkit|NonComp Ctrl 1,72,73,88|LI-1.86|IM-6 – 11.18

Risk Scenario #012 APT 29|Rootkit|NonComp Ctrl 1,3,233|LI-12.38|LI-16.52|IM-6 – 99.09

Risk Scenario #013 Machete|HijackExecutionFlow|NonComp Ctrl 166,167|LI-5.13|IM-10 – 51.26

Risk Scenario #014 WizardSpider|ModifyExecution|NonComp Ctrl 201,229|LI-38.86|IM-2 – 77.72

Risk Scenario #015 APT 29|HijackExecutionFlow|NonComp Ctrl 1,89,121|LI-45.75|IM-4 – 183.82

Dashboard

Topline Summary

Based on the 3 non-compliant controls entered (explicit and known Vulnerabilities (VU)), CTAaaS analysis has determined the following:

- Your system is exposed to 8 MITRE ATT&CK Threat Event Techniques (TE Techniques) and are subsequently referred to in this report as “Menacing TE Techniques.”

- Of those 8 Menacing TE Techniques, there are currently 11 MITRE ATT&CK Threat Source Groups (TS Groups) that are known by MITRE to employ those specific Menacing TE Techniques and are subsequently referred to in this report as “Menacing TS Techniques.”

- CTAaaS has assembled all the possible combinations of those Menacing TE Techniques and Menacing TS Techniques into 15 of known-possible Risk Scenarios.

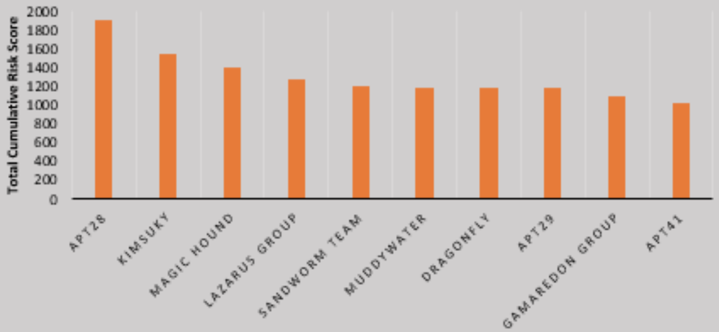
- Each of these 15 Risk Scenarios have been quantified by CTAaaS employing NIST SP 800-30R1 guidance on semi-quantitative assessments and have been documented in the Cyber Risk Register (CRR) contained within the CRR tab of this CTAaaS report.

- And finally, the overall cyber risk posture of this system is considered to be the total score of all the risk scenarios in the CRR which for this system is: 2,527.

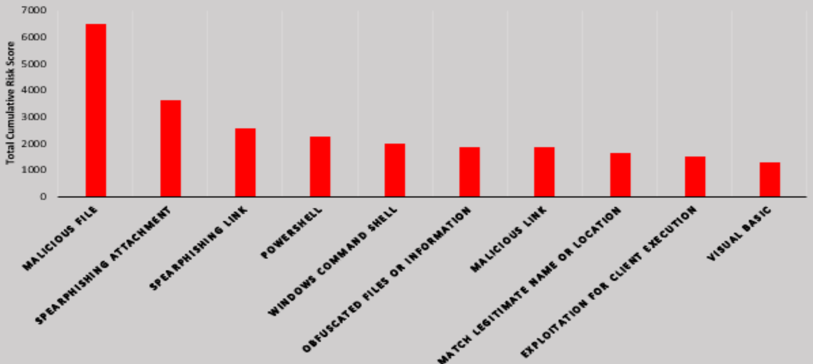
Results

Menacing TS Groups	Menacing TE Techniques	Total Number of VUs	Total Risk Scenarios	Total Risk Score
11	8	10	15	2,527

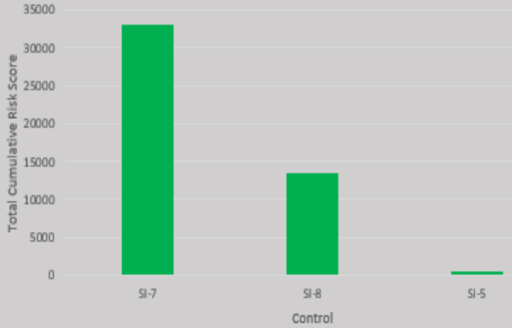
Top 10 Menacing TS Groups



Top 8 Menacing TE Techniques



Top 3 Menacing VUs (Non-Compliant Ctrls)



CTAaaS For the Space ISAC Community

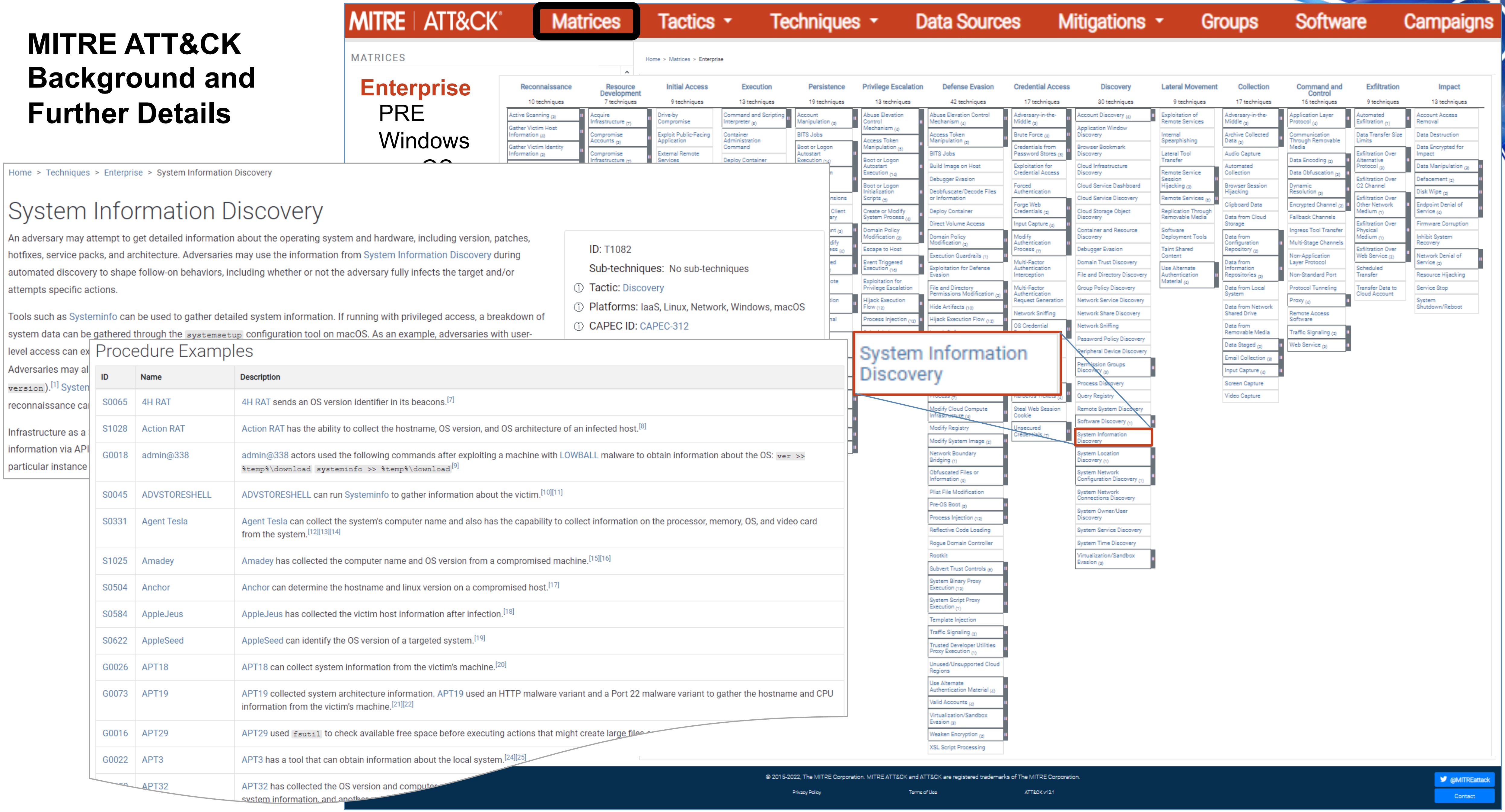
- How is CTAaaS is a service (vice software tool to be distributed)?:
  - Aerospace to keep spreadsheet tool up to date with continually updated MITRE ATT&CK data/structure
  - Will provide refreshed spreadsheets to CTAaaS users
- Why was CTAaaS functionality made available to users as a spreadsheet vice website?
  - Avoids having to deploy software to countless user environments
  - Many users were unwilling to enter their sensitive security control status information into a CTAaaS website
  - Avoids need for ATO by relying on a standard MS Office product (note: MS Excel Spreadsheet uses no-macros)
- Status of Availability to Space ISAC and Members/Partners
  - Going through Aerospace legal to obtain terms of use language and permission to distribute CTAaaS functionality
  - Adding SPARTA techniques into methodology
  - Plan to imbed CTAaaS reports/analysis into Space Watch Center reports
  - Will host subsequent Q&A sessions with interested users

For more information, contact William.d.belei@Aero.org

Backup Content Past This Point

MITRE | ATT&CK®
Matrices
Tactics
Techniques
Data Sources
Mitigations
Groups
Software
Campaigns
Resources
Blog
Contribute
Search

MITRE ATT&CK Background and Further Details



Home > Matrices > Enterprise

Reconnaissance (10 techniques): Active Scanning (3), Gather Victim Host Information (4), Gather Victim Identity Information (3)

Resource Development (7 techniques): Acquire Infrastructure (7), Compromise Accounts (3), Compromise Infrastructure (7)

Initial Access (9 techniques): Drive-by Compromise, Exploit Public-Facing Application, External Remote Services

Execution (13 techniques): Command and Scripting Interpreter (8), Container Administration Command, Deploy Container

Persistence (19 techniques): Account Manipulation (5), BITS Jobs, Boot or Logon Autostart Execution (14)

Privilege Escalation (13 techniques): Abuse Elevation Control Mechanism (4), Access Token Manipulation (5), Boot or Logon Autostart Execution (14), Boot or Logon Initialization Scripts (5), Create or Modify System Process (4), Domain Policy Modification (2), Escape to Host, Event Triggered Execution (16), Exploitation for Privilege Escalation, Hijack Execution Flow (12), Process Injection (12)

Defense Evasion (42 techniques): Abuse Elevation Control Mechanism (4), Access Token Manipulation (5), BITS Jobs, Build Image on Host, Debugger Evasion, Deobfuscate/Decode Files or Information, Deploy Container, Direct Volume Access, Domain Policy Modification (2), Execution Guardrails (1), Exploitation for Defense Evasion, File and Directory Permissions Modification (2), Hide Artifacts (10), Hijack Execution Flow (12), Modify Cloud Compute Infrastructure (4), Modify Registry, Modify System Image (2), Network Boundary Bridging (1), Obfuscated Files or Information (9), Plist File Modification, Pre-OS Boot (5), Process Injection (12), Reflective Code Loading, Rogue Domain Controller, Rootkit, Subvert Trust Controls (6), System Binary Proxy Execution (13), System Script Proxy Execution (1), Template Injection, Traffic Signaling (2), Trusted Developer Utilities Proxy Execution (1), Unused/Unsupported Cloud Regions, Use Alternate Authentication Material (4), Valid Accounts (4), Virtualization/Sandbox Evasion (3), Weaken Encryption (2), XSL Script Processing

Credential Access (17 techniques): Adversary-in-the-Middle (3), Brute Force (4), Credentials from Password Stores (5), Exploitation for Credential Access, Forced Authentication, Forge Web Credentials (2), Input Capture (4), Modify Authentication Process (7), Multi-Factor Authentication Interception, Multi-Factor Authentication Request Generation, Network Sniffing, OS Credential Dumping, Steal Web Session Cookie, Unsecured Credentials (7)

Discovery (30 techniques): Account Discovery (4), Application Window Discovery, Browser Bookmark Discovery, Cloud Infrastructure Discovery, Cloud Service Dashboard, Cloud Service Discovery, Cloud Storage Object Discovery, Container and Resource Discovery, Debugger Evasion, Domain Trust Discovery, File and Directory Discovery, Group Policy Discovery, Network Service Discovery, Network Share Discovery, Network Sniffing, Password Policy Discovery, Peripheral Device Discovery, Permission Groups Discovery (3), Process Discovery, Query Registry, Remote System Discovery, Software Discovery (1), System Information Discovery, System Location Discovery (1), System Network Configuration Discovery (1), System Network Connections Discovery, System Owner/User Discovery, System Service Discovery, System Time Discovery, Virtualization/Sandbox Evasion (3)

Lateral Movement (9 techniques): Exploitation of Remote Services, Internal Spearphishing, Lateral Tool Transfer, Remote Service Session Hijacking (2), Remote Services (8), Replication Through Removable Media, Software Deployment Tools, Taint Shared Content, Use Alternate Authentication Material (4)

Collection (17 techniques): Adversary-in-the-Middle (3), Archive Collected Data (3), Audio Capture, Automated Collection, Browser Session Hijacking, Clipboard Data, Data from Cloud Storage, Data from Configuration Repository (2), Data from Information Repositories (3), Data from Local System, Data from Network Shared Drive, Data from Removable Media, Data Staged (2), Email Collection (3), Input Capture (4), Screen Capture, Video Capture

Command and Control (16 techniques): Application Layer Protocol (4), Communication Through Removable Media, Data Encoding (2), Data Obfuscation (3), Dynamic Resolution (3), Encrypted Channel (2), Fallback Channels, Ingress Tool Transfer, Multi-Stage Channels, Non-Application Layer Protocol, Non-Standard Port, Protocol Tunneling, Proxy (4), Remote Access Software, Traffic Signaling (2), Web Service (3)

Exfiltration (9 techniques): Automated Exfiltration (1), Data Transfer Size Limits, Exfiltration Over Alternative Protocol (3), Exfiltration Over C2 Channel, Exfiltration Over Other Network Medium (1), Exfiltration Over Physical Medium (1), Exfiltration Over Web Service (2), Scheduled Transfer, Transfer Data to Cloud Account

Impact (13 techniques): Account Access Removal, Data Destruction, Data Encrypted for Impact, Data Manipulation (3), Defacement (2), Disk Wipe (2), Endpoint Denial of Service (4), Firmware Corruption, Inhibit System Recovery, Network Denial of Service (2), Resource Hijacking, Service Stop, System Shutdown/Reboot

System Information Discovery

© 2015-2022, The MITRE Corporation. MITRE ATT&CK and ATT&CK are registered trademarks of The MITRE Corporation.

Privacy Policy Terms of Use ATT&CK v12.1

@MITREattack
Contact

Home > Techniques > Enterprise > System Information Discovery

System Information Discovery

An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Adversaries may use the information from System Information Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

Tools such as Systeminfo can be used to gather detailed system information. If running with privileged access, a breakdown of system data can be gathered through the `systemsetup` configuration tool on macOS. As an example, adversaries with user-level access can ex

Adversaries may al

`version`).[1] Systen

reconnaissance ca

Infrastructure as a

information via API

particular instance

ID: T1082

Sub-techniques: No sub-techniques

ⓘ Tactic: Discovery

ⓘ Platforms: IaaS, Linux, Network, Windows, macOS

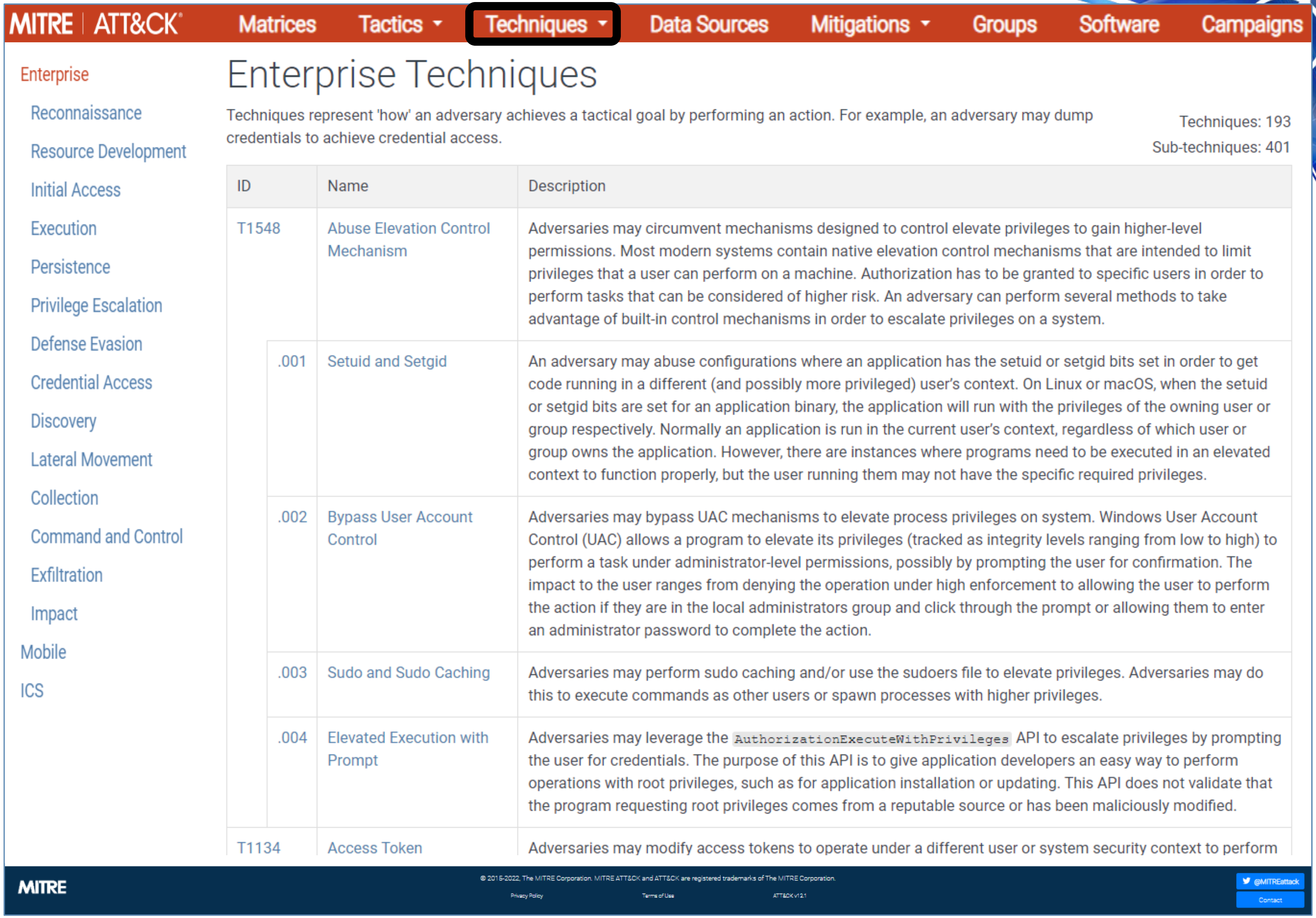
ⓘ CAPEC ID: CAPEC-312

Procedure Examples

ID	Name	Description
S0065	4H RAT	4H RAT sends an OS version identifier in its beacons.[7]
S1028	Action RAT	Action RAT has the ability to collect the hostname, OS version, and OS architecture of an infected host.[8]
G0018	admin@338	admin@338 actors used the following commands after exploiting a machine with LOWBALL malware to obtain information about the OS: `ver >> %temp%\download systeminfo >> %temp%\download`[9]
S0045	ADVSTORESHELL	ADVSTORESHELL can run Systeminfo to gather information about the victim.[10][11]
S0331	Agent Tesla	Agent Tesla can collect the system's computer name and also has the capability to collect information on the processor, memory, OS, and video card from the system.[12][13][14]
S1025	Amadey	Amadey has collected the computer name and OS version from a compromised machine.[15][16]
S0504	Anchor	Anchor can determine the hostname and linux version on a compromised host.[17]
S0584	AppleJeus	AppleJeus has collected the victim host information after infection.[18]
S0622	AppleSeed	AppleSeed can identify the OS version of a targeted system.[19]
G0026	APT18	APT18 can collect system information from the victim's machine.[20]
G0073	APT19	APT19 collected system architecture information. APT19 used an HTTP malware variant and a Port 22 malware variant to gather the hostname and CPU information from the victim's machine.[21][22]
G0016	APT29	APT29 used `fsutil` to check available free space before executing actions that might create large files
G0022	APT3	APT3 has a tool that can obtain information about the local system.[24][25]
	APT32	APT32 has collected the OS version and computer system information, and anothe

[Return to background/details]

MITRE ATT&CK Background and Further Details



Enterprise Techniques

Techniques represent 'how' an adversary achieves a tactical goal by performing an action. For example, an adversary may dump credentials to achieve credential access.

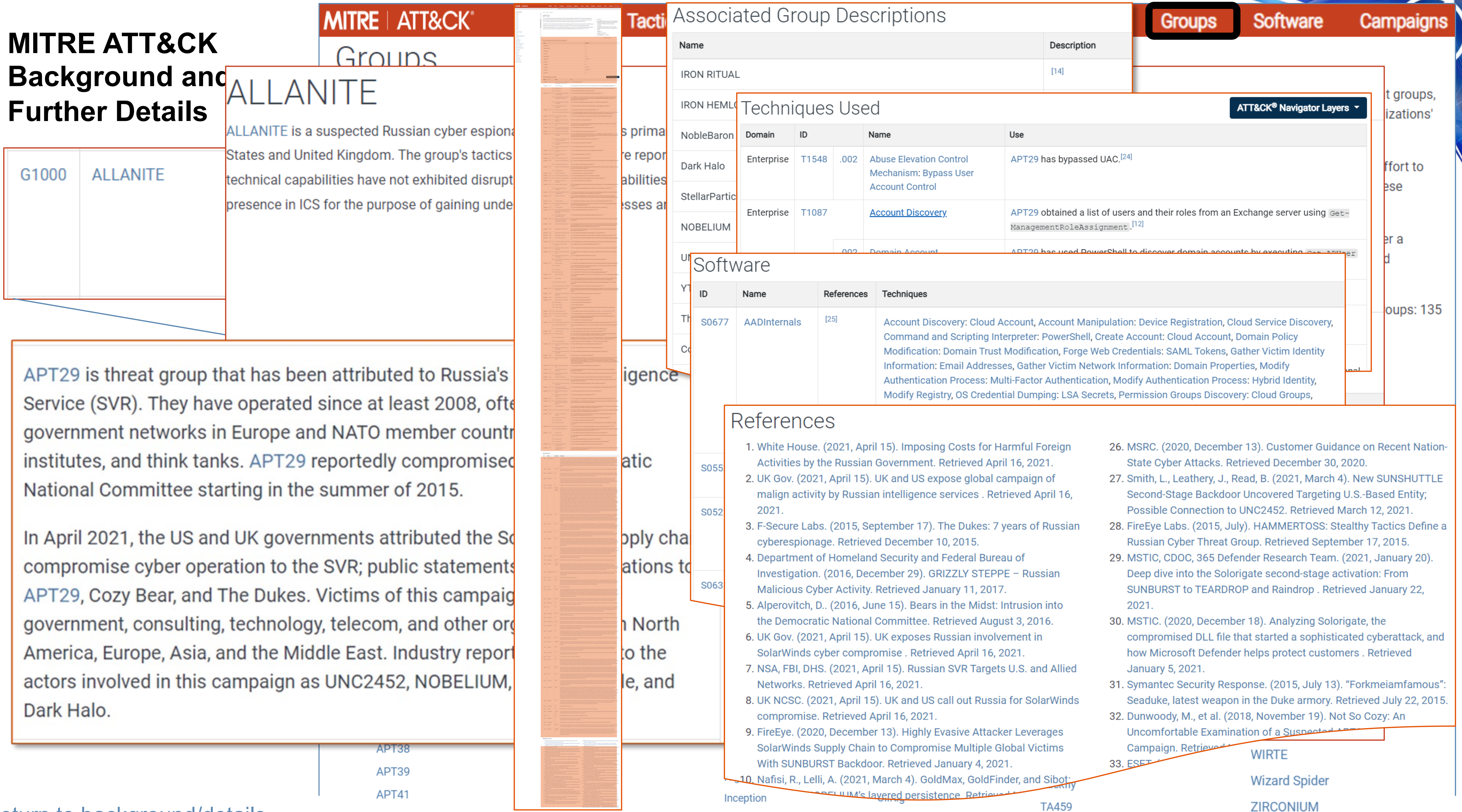
Techniques: 193
Sub-techniques: 401

ID		Name	Description
T1548		Abuse Elevation Control Mechanism	Adversaries may circumvent mechanisms designed to control elevate privileges to gain higher-level permissions. Most modern systems contain native elevation control mechanisms that are intended to limit privileges that a user can perform on a machine. Authorization has to be granted to specific users in order to perform tasks that can be considered of higher risk. An adversary can perform several methods to take advantage of built-in control mechanisms in order to escalate privileges on a system.
	.001	Setuid and Setgid	An adversary may abuse configurations where an application has the setuid or setgid bits set in order to get code running in a different (and possibly more privileged) user's context. On Linux or macOS, when the setuid or setgid bits are set for an application binary, the application will run with the privileges of the owning user or group respectively. Normally an application is run in the current user's context, regardless of which user or group owns the application. However, there are instances where programs need to be executed in an elevated context to function properly, but the user running them may not have the specific required privileges.
	.002	Bypass User Account Control	Adversaries may bypass UAC mechanisms to elevate process privileges on system. Windows User Account Control (UAC) allows a program to elevate its privileges (tracked as integrity levels ranging from low to high) to perform a task under administrator-level permissions, possibly by prompting the user for confirmation. The impact to the user ranges from denying the operation under high enforcement to allowing the user to perform the action if they are in the local administrators group and click through the prompt or allowing them to enter an administrator password to complete the action.
	.003	Sudo and Sudo Caching	Adversaries may perform sudo caching and/or use the sudoers file to elevate privileges. Adversaries may do this to execute commands as other users or spawn processes with higher privileges.
	.004	Elevated Execution with Prompt	Adversaries may leverage the `AuthorizationExecuteWithPrivileges` API to escalate privileges by prompting the user for credentials. The purpose of this API is to give application developers an easy way to perform operations with root privileges, such as for application installation or updating. This API does not validate that the program requesting root privileges comes from a reputable source or has been maliciously modified.
T1134		Access Token	Adversaries may modify access tokens to operate under a different user or system security context to perform

MITRE
© 2015-2022, The MITRE Corporation. MITRE ATT&CK and ATT&CK are registered trademarks of The MITRE Corporation.
Privacy Policy
Terms of Use
ATT&CK v12.1
@MITREattack
Contact

Return to background/details

MITRE ATT&CK Background and Further Details



Groups

ALLANITE

ALLANITE is a suspected Russian cyber espiona… s prima…
States and United Kingdom. The group's tactics … re repor…
technical capabilities have not exhibited disrupt… abilities
presence in ICS for the purpose of gaining unde… sses ar…

G1000	ALLANITE

APT29 is threat group that has been attributed to Russia's … igence Service (SVR). They have operated since at least 2008, ofte… government networks in Europe and NATO member countr… institutes, and think tanks. APT29 reportedly compromised … atic National Committee starting in the summer of 2015.

In April 2021, the US and UK governments attributed the Sc… pply cha… compromise cyber operation to the SVR; public statements … ations to APT29, Cozy Bear, and The Dukes. Victims of this campaig… government, consulting, technology, telecom, and other org… n North America, Europe, Asia, and the Middle East. Industry report… to the actors involved in this campaign as UNC2452, NOBELIUM, … le, and Dark Halo.

APT38
APT39
APT41

Associated Group Descriptions

Name	Description
IRON RITUAL	[14]
IRON HEML…	
NobleBaron	
Dark Halo	
StellarPartic…	
NOBELIUM	
U…	
YT…	
Th…	
Co…	

… t groups,
… izations'
… ffort to
… ese
… er a
… d
… oups: 135

Techniques Used

Domain	ID		Name	Use
Enterprise	T1548	.002	Abuse Elevation Control Mechanism: Bypass User Account Control	APT29 has bypassed UAC.[24]
Enterprise	T1087		Account Discovery	APT29 obtained a list of users and their roles from an Exchange server using Get-ManagementRoleAssignment.[12]
		.002	Domain Account	APT29 has used PowerShell to discover domain accounts by executing Get-ADUser

Software

ID	Name	References	Techniques
S0677	AADInternals	[25]	Account Discovery: Cloud Account, Account Manipulation: Device Registration, Cloud Service Discovery, Command and Scripting Interpreter: PowerShell, Create Account: Cloud Account, Domain Policy Modification: Domain Trust Modification, Forge Web Credentials: SAML Tokens, Gather Victim Identity Information: Email Addresses, Gather Victim Network Information: Domain Properties, Modify Authentication Process: Multi-Factor Authentication, Modify Authentication Process: Hybrid Identity, Modify Registry, OS Credential Dumping: LSA Secrets, Permission Groups Discovery: Cloud Groups,
S055…			
S052…			
S063…			

References

1. White House. (2021, April 15). Imposing Costs for Harmful Foreign Activities by the Russian Government. Retrieved April 16, 2021.
2. UK Gov. (2021, April 15). UK and US expose global campaign of malign activity by Russian intelligence services . Retrieved April 16, 2021.
3. F-Secure Labs. (2015, September 17). The Dukes: 7 years of Russian cyberespionage. Retrieved December 10, 2015.
4. Department of Homeland Security and Federal Bureau of Investigation. (2016, December 29). GRIZZLY STEPPE – Russian Malicious Cyber Activity. Retrieved January 11, 2017.
5. Alperovitch, D.. (2016, June 15). Bears in the Midst: Intrusion into the Democratic National Committee. Retrieved August 3, 2016.
6. UK Gov. (2021, April 15). UK exposes Russian involvement in SolarWinds cyber compromise . Retrieved April 16, 2021.
7. NSA, FBI, DHS. (2021, April 15). Russian SVR Targets U.S. and Allied Networks. Retrieved April 16, 2021.
8. UK NCSC. (2021, April 15). UK and US call out Russia for SolarWinds compromise. Retrieved April 16, 2021.
9. FireEye. (2020, December 13). Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor. Retrieved January 4, 2021.
10. Nafisi, R., Lelli, A. (2021, March 4). GoldMax, GoldFinder, and Sibot: … NOBELIUM's layered persistence. Retrieved …

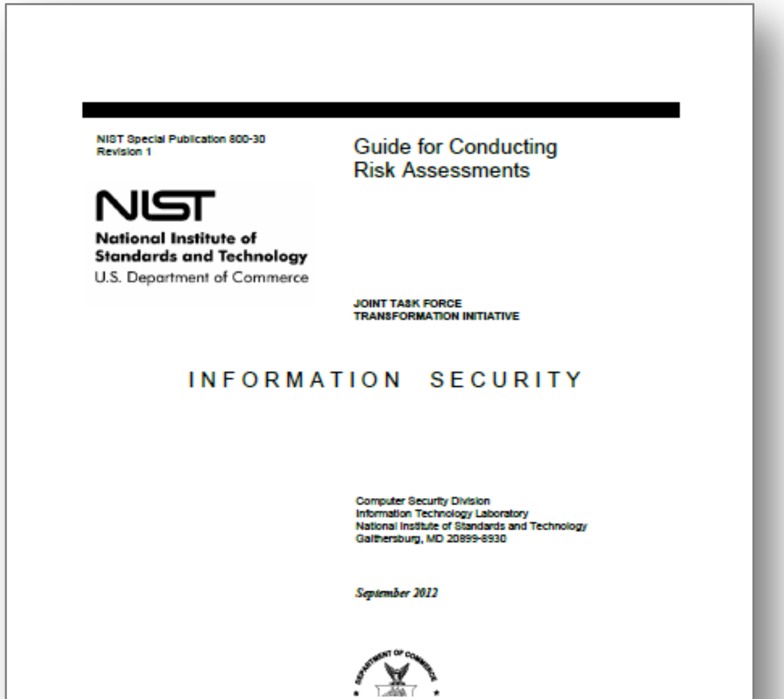
26. MSRC. (2020, December 13). Customer Guidance on Recent Nation-State Cyber Attacks. Retrieved December 30, 2020.
27. Smith, L., Leathery, J., Read, B. (2021, March 4). New SUNSHUTTLE Second-Stage Backdoor Uncovered Targeting U.S.-Based Entity; Possible Connection to UNC2452. Retrieved March 12, 2021.
28. FireEye Labs. (2015, July). HAMMERTOSS: Stealthy Tactics Define a Russian Cyber Threat Group. Retrieved September 17, 2015.
29. MSTIC, CDOC, 365 Defender Research Team. (2021, January 20). Deep dive into the Solorigate second-stage activation: From SUNBURST to TEARDROP and Raindrop . Retrieved January 22, 2021.
30. MSTIC. (2020, December 18). Analyzing Solorigate, the compromised DLL file that started a sophisticated cyberattack, and how Microsoft Defender helps protect customers . Retrieved January 5, 2021.
31. Symantec Security Response. (2015, July 13). "Forkmeiamfamous": Seaduke, latest weapon in the Duke armory. Retrieved July 22, 2015.
32. Dunwoody, M., et al. (2018, November 19). Not So Cozy: An Uncomfortable Examination of a Suspected APT… Campaign. Retrieve…
33. ESET …

Inception
TA459
WIRTE
Wizard Spider
ZIRCONIUM

Return to background/details

Highlights of Key DoD/NIST Risk Assessment Guidance (continued)

- CRAs should be based on risk models, include explicit formulas and algorithms for combining risk factors, and result in scores/values.
  - Page 16: "The expectation set forth in Special Publications 800-39 and 800-30 is that each organization or community will define a risk model appropriate to its view of risk (i.e., formulas that reflect organizational or community views of which risk factors must be considered, which factors can be combined, which factors must be further decomposed, and how assessed values should be combined algorithmically)."
  - Page 28: "Organization-specific risk models include algorithms (e.g., formulas, tables, rules) for combining risk factors" (page 28)
  - "Combinations of factors such as targeting, intent, and capability thus can be used to produce a score representing the likelihood of threat initiation; combinations of factors such as capability and vulnerability severity can be used to produce a score representing the likelihood of adverse impacts; and combinations of these scores can be used to produce an overall likelihood score." (page G-1)
- Guide for Conducting Risk Assessments appendices provide extensive tools
  - 36 taxonomy guides, semi-quantitative assessment tables, assessment process exemplars, etc that are routinely ignored by organization risk assessment approaches



NIST Special Publication 800-30
Revision 1

Guide for Conducting
Risk Assessments

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

September 2012

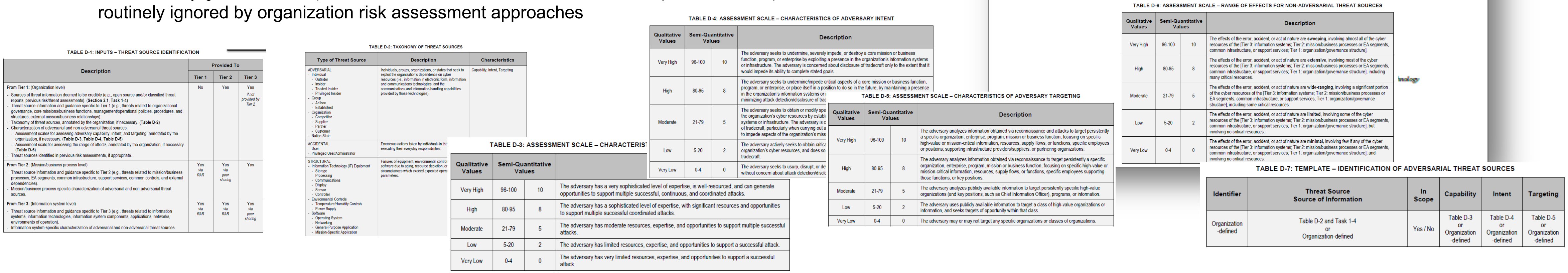


TABLE D-1: INPUTS – THREAT SOURCE IDENTIFICATION

Description	Provided To		
	Tier 1	Tier 2	Tier 3
From Tier 1: (Organization level) - Sources of threat information deemed to be credible (e.g., open source and/or classified threat reports, previous risk/threat assessments). (**Section 3.1**, **Task 1-4**) - Threat source information and guidance specific to Tier 1 (e.g., threats related to organizational governance, core missions/business functions, management/operational policies, procedures, and structures, external mission/business relationships). - Taxonomy of threat sources, annotated by the organization, if necessary. (**Table D-2**) - Characterization of adversarial and non-adversarial threat sources. - Assessment scales for assessing adversary capability, intent, and targeting, annotated by the organization, if necessary. (**Table D-3, Table D-4, Table D-5**) - Assessment scale for assessing the range of effects, annotated by the organization, if necessary. (**Table D-6**) - Threat sources identified in previous risk assessments, if appropriate.	No	Yes	Yes *if not provided by Tier 2*
From Tier 2: (Mission/business process level) - Threat source information and guidance specific to Tier 2 (e.g., threats related to mission/business processes, EA segments, common infrastructure, support services, common controls, and external dependencies). - Mission/business process-specific characterization of adversarial and non-adversarial threat sources.	Yes *via RAR*	Yes *via peer sharing*	Yes
From Tier 3: (Information system level) - Threat source information and guidance specific to Tier 3 (e.g., threats related to information systems, information technologies, information system components, applications, networks, environments of operation). - Information system-specific characterization of adversarial and non-adversarial threat sources.	Yes *via RAR*	Yes *via RAR*	Yes *via peer sharing*

TABLE D-2: TAXONOMY OF THREAT SOURCES

Type of Threat Source	Description	Characteristics
ADVERSARIAL - Individual - Outsider - Insider - Trusted Insider - Privileged Insider - Group - Ad hoc - Established - Organization - Competitor - Supplier - Partner - Customer - Nation-State	Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources (i.e., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies).	Capability, Intent, Targeting
ACCIDENTAL - User - Privileged User/Administrator	Erroneous actions taken by individuals in the executing their everyday responsibilities.	
STRUCTURAL - Information Technology (IT) Equipment - Storage - Processing - Communications - Display - Sensor - Controller - Environmental Controls - Temperature/Humidity Controls - Power Supply - Software - Operating System - Networking - General-Purpose Application - Mission-Specific Application	Failures of equipment, environmental control software due to aging, resource depletion, or circumstances which exceed expected opera parameters.	

TABLE D-3: ASSESSMENT SCALE – CHARACTERIST

Qualitative Values	Semi-Quantitative Values		
Very High	96-100	10	The adversary has a very sophisticated level of expertise, is well-resourced, and can generate opportunities to support multiple successful, continuous, and coordinated attacks.
High	80-95	8	The adversary has a sophisticated level of expertise, with significant resources and opportunities to support multiple successful coordinated attacks.
Moderate	21-79	5	The adversary has moderate resources, expertise, and opportunities to support multiple successful attacks.
Low	5-20	2	The adversary has limited resources, expertise, and opportunities to support a successful attack.
Very Low	0-4	0	The adversary has very limited resources, expertise, and opportunities to support a successful attack.

TABLE D-4: ASSESSMENT SCALE – CHARACTERISTICS OF ADVERSARY INTENT

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The adversary seeks to undermine, severely impede, or destroy a core mission or business function, program, or enterprise by exploiting a presence in the organization's information systems or infrastructure. The adversary is concerned about disclosure of tradecraft only to the extent that it would impede its ability to complete stated goals.
High	80-95	8	The adversary seeks to undermine/impede critical aspects of a core mission or business function, program, or enterprise, or place itself in a position to do so in the future, by maintaining a presence in the organization's information systems or i minimizing attack detection/disclosure of trac
Moderate	21-79	5	The adversary seeks to obtain or modify spe the organization's cyber resources by establi systems or infrastructure. The adversary is c of tradecraft, particularly when carrying out a to impede aspects of the organization's missi
Low	5-20	2	The adversary actively seeks to obtain critica organization's cyber resources, and does so tradecraft.
Very Low	0-4	0	The adversary seeks to usurp, disrupt, or de without concern about attack detection/disclo

TABLE D-5: ASSESSMENT SCALE – CHARACTERISTICS OF ADVERSARY TARGETING

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The adversary analyzes information obtained via reconnaissance and attacks to target persistently a specific organization, enterprise, program, mission or business function, focusing on specific high-value or mission-critical information, resources, supply flows, or functions; specific employees or positions; supporting infrastructure providers/suppliers; or partnering organizations.
High	80-95	8	The adversary analyzes information obtained via reconnaissance to target persistently a specific organization, enterprise, program, mission or business function, focusing on specific high-value or mission-critical information, resources, supply flows, or functions, specific employees supporting those functions, or key positions.
Moderate	21-79	5	The adversary analyzes publicly available information to target persistently specific high-value organizations (and key positions, such as Chief Information Officer), programs, or information.
Low	5-20	2	The adversary uses publicly available information to target a class of high-value organizations or information, and seeks targets of opportunity within that class.
Very Low	0-4	0	The adversary may or may not target any specific organizations or classes of organizations.

TABLE D-6: ASSESSMENT SCALE – RANGE OF EFFECTS FOR NON-ADVERSARIAL THREAT SOURCES

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The effects of the error, accident, or act of nature are **sweeping**, involving almost all of the cyber resources of the [Tier 3: information systems; Tier 2: mission/business processes or EA segments, common infrastructure, or support services; Tier 1: organization/governance structure].
High	80-95	8	The effects of the error, accident, or act of nature are **extensive**, involving most of the cyber resources of the [Tier 3: information systems; Tier 2: mission/business processes or EA segments, common infrastructure, or support services; Tier 1: organization/governance structure], including many critical resources.
Moderate	21-79	5	The effects of the error, accident, or act of nature are **wide-ranging**, involving a significant portion of the cyber resources of the [Tier 3: information systems; Tier 2: mission/business processes or EA segments, common infrastructure, or support services; Tier 1: organization/governance structure], including some critical resources.
Low	5-20	2	The effects of the error, accident, or act of nature are **limited**, involving some of the cyber resources of the [Tier 3: information systems; Tier 2: mission/business processes or EA segments, common infrastructure, or support services; Tier 1: organization/governance structure], but involving no critical resources.
Very Low	0-4	0	The effects of the error, accident, or act of nature are **minimal**, involving few if any of the cyber resources of the [Tier 3: information systems; Tier 2: mission/business processes or EA segments, common infrastructure, or support services; Tier 1: organization/governance structure], and involving no critical resources.

TABLE D-7: TEMPLATE – IDENTIFICATION OF ADVERSARIAL THREAT SOURCES

Identifier	Threat Source Source of Information	In Scope	Capability	Intent	Targeting
Organization-defined	Table D-2 and Task 1-4 or Organization-defined	Yes / No	Table D-3 or Organization-defined	Table D-4 or Organization-defined	Table D-5 or Organization-defined

Now let's look at some animations to explain how CTAaaS operationalizes 800-30 guidance to meet this CRA use case

Challenge 3: Profound Complexity in Deciphering Relevancy of CTI

Let's look at how many organizations attempt to manually analyze CTI

Ex. Commodity CTI sources:

- MITRE CVEs
- MITRE CWEs
- CISA KEV
- Comm. Reports
- CTI Feeds
- ISAC Reports

Etc…………………

Example CTI finding "*Threat Source (cyber group)* ***A*** employed *Threat Event (technique)* ***B*** on *[org, system, asset]* ***C***"

Is Threat Source A a cyber attacker who would be likely to attack any of my systems?

AKA – is Threat Source X contextually relevant? There are 138 Threat Sources, how do you know which are relevant and which are not?

Is Threat Event B an attack technique that my systems' are even vulnerable to?

AKA – is Threat Source X contextually relevant? There are 607 attack techniques, they map to ~7,000 different vulnerabilities. Can you determine if relevant and how relevant?

Is [org, sys, asset] Z a similar target as the systems I'm concerned with protecting?

You need to know if Threat Source X is targeting same or similar targets so you can determine if relevant.

I've already got a 100 other cyber concerns, should this become my #1 or #101 concern?

In a sense every potential cyber attack is a concern but you can't defend against everything so understanding your priorities is KEY! So how do you measure and adjust your priorities every time CTI like this floats in?

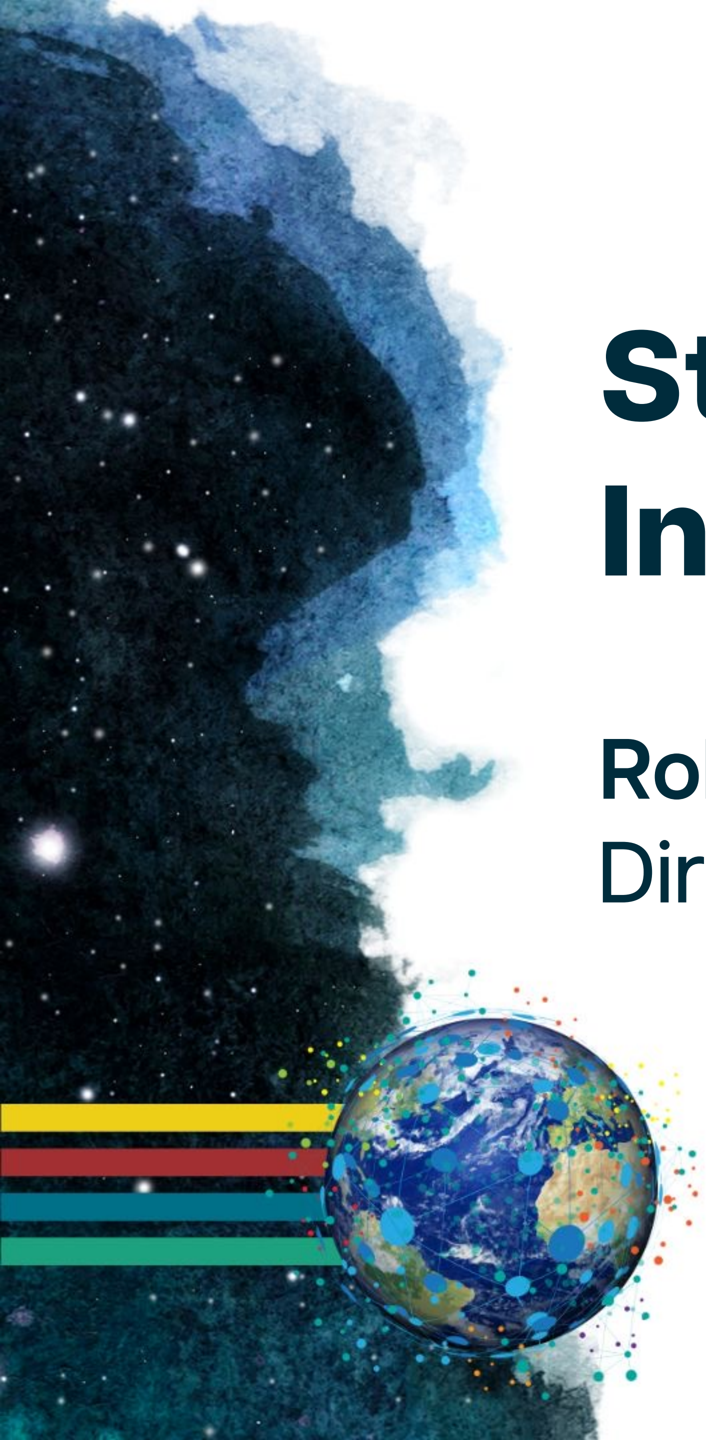
If this data drives me to generate a new cyber priority, how do I find the time to mitigate this new one?

Rarely do cyber problems have a nice and neat single solution to eliminate the risk. They typically have many different ways to mitigate (aka reduce) the risk. How can you determine the right mitigation or combination of mitigations?

So much to think about … yet so little time to do so …

Space ISAC Cislunar Affinity Group Discussion

Gabrielle Hedrick, Ph.D, Aerospace Engineer, The MITRE Corporation



Strategic Earthshot Initiative

Robert Katz, Founder, CEO & Executive Director, World Innovation Network

World

Innovation

Network

NASA INTERNATIONAL SPACE APPS CHALLENGE

57,900+
INTERNATIONAL
PARTICIPANTS

8,400+
SOLUTION
TEAMS

402
EVENT
VENUES

PPPs

NASA SPACE APPS Kennedy Space Center

CareerSource BREVARD

Delaware North

presented by CommHIT at Kennedy Space Center CommHIT.org

WOMEN IN AVIATION CENTRAL FLORIDA CHAPTER

UES Universal Engineering Sciences

CYNCROCITY

SPACE FOUNDATION

ASTRONAUT SCHOLARSHIP FOUNDATION

SPACE TREK

THE GREATER PALM BAY CHAMBER OF COMMERCE

Canaveral Council of Technical Societies CCTS

World Innovation Network

inetUSA

MASC MANUFACTURERS ASSOCIATION FLORIDA'S SPACE COAST

Society of SAME American Military Engineers

IEEE Melbourne Section

IEEE Canaveral Section

FIRST ROBOTICS COMPETITION

ASME

Space and Rocket PIONEERS

NASA Alumni League

frea

AIChE

PMI Project Management Institute. Space Coast, Florida

AIAA SHAPING THE FUTURE OF AEROSPACE

INCOSE

AMERICAN SOCIETY OF SAFETY PROFESSIONALS

AACE NORTH FLORIDA SECTION

ASHRAE SPACE COAST COMMUNITY

IBM

meteomatics

Google

Xd Adobe XD

tableau

planet.

GoDaddy Registry

miro

ANITA B.ORG

AMERICAN FAMILY INSURANCE INSTITUTE FOR CORPORATE AND SOCIAL IMPACT

Microsoft Azure

Microsoft Teams

Genspace

UA LITTLE ROCK

gener8tor

coding temple

BLACK GIRLS CODE

national center for women & INFORMATION TECHNOLOGY

Penn GSE GRADUATE SCHOOL OF EDUCATION UNIVERSITY of PENNSYLVANIA

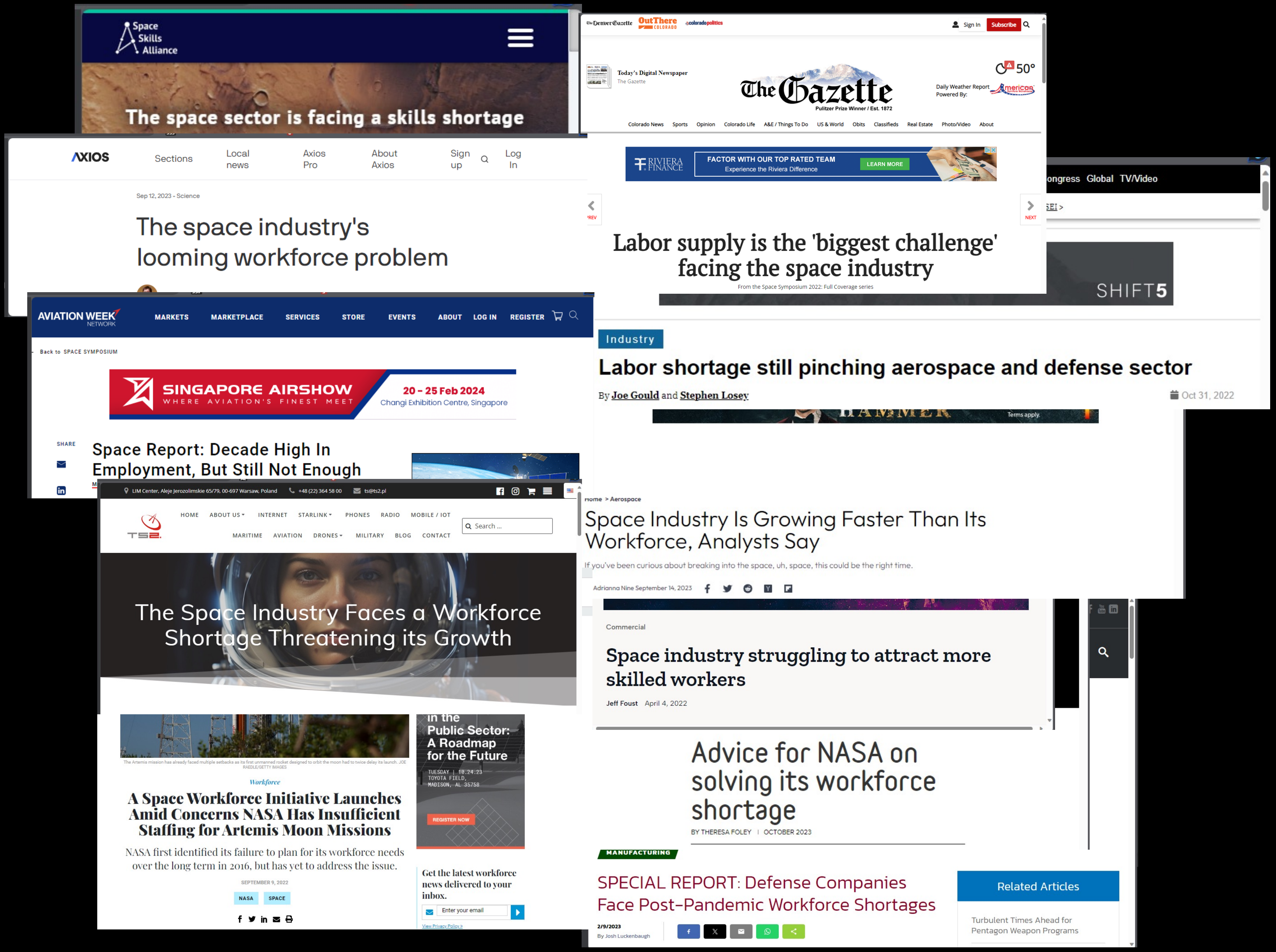
WOMEN OF MENA IN TECH

Solution

People

Public	Private	Pupil	Press	Promises	Pride	Propagation	Proclaimation	Proliferation
Promulgation	Prosperity	Projects	Processes	Planet	Programs	Partnerships	Partners	Presentations
Productivity	Platforms	Pledges	Plans	Pronouncement	Procurement	Prolongation	Practices	Proposals
People	Patents	Planning	Providers	PIpelines	Packaging	Promotion	Publications	Prospectuses
Productization	Perseverance	Power	Patience	Perspective	Protection	Perspiration	Prediction	Persepolis
Preparation	Politics	Profits	Persistence	Personality	Policies	Performance	Purpose	Passion

Problem



The space sector is facing a skills shortage

Sep 12, 2023 - Science

The space industry's looming workforce problem

Back to SPACE SYMPOSIUM

SINGAPORE AIRSHOW
WHERE AVIATION'S FINEST MEET
20 – 25 Feb 2024
Changi Exhibition Centre, Singapore

Space Report: Decade High In Employment, But Still Not Enough

FACTOR WITH OUR TOP RATED TEAM
Experience the Riviera Difference
LEARN MORE

Labor supply is the 'biggest challenge' facing the space industry

From the Space Symposium 2022: Full Coverage series

Industry

Labor shortage still pinching aerospace and defense sector

By Joe Gould and Stephen Losey

Oct 31, 2022

LIM Center, Aleje Jerozolimskie 65/79, 00-697 Warsaw, Poland   +48 (22) 364 58 00   ts@ts2.pl

The Space Industry Faces a Workforce Shortage Threatening its Growth

Home > Aerospace

Space Industry Is Growing Faster Than Its Workforce, Analysts Say

If you've been curious about breaking into the space, uh, space, this could be the right time.

Adrianna Nine September 14, 2023

Commercial

Space industry struggling to attract more skilled workers

Jeff Foust   April 4, 2022

The Artemis mission has already faced multiple setbacks as its first unmanned rocket designed to orbit the moon had to twice delay its launch. JOE RAEDLE/GETTY IMAGES

Workforce

A Space Workforce Initiative Launches Amid Concerns NASA Has Insufficient Staffing for Artemis Moon Missions

NASA first identified its failure to plan for its workforce needs over the long term in 2016, but has yet to address the issue.

SEPTEMBER 9, 2022

NASA   SPACE

in the Public Sector: A Roadmap for the Future

TUESDAY | 10.24.23
TOYOTA FIELD,
MADISON, AL 35758

Get the latest workforce news delivered to your inbox.

View Privacy Policy »

Advice for NASA on solving its workforce shortage

BY THERESA FOLEY | OCTOBER 2023

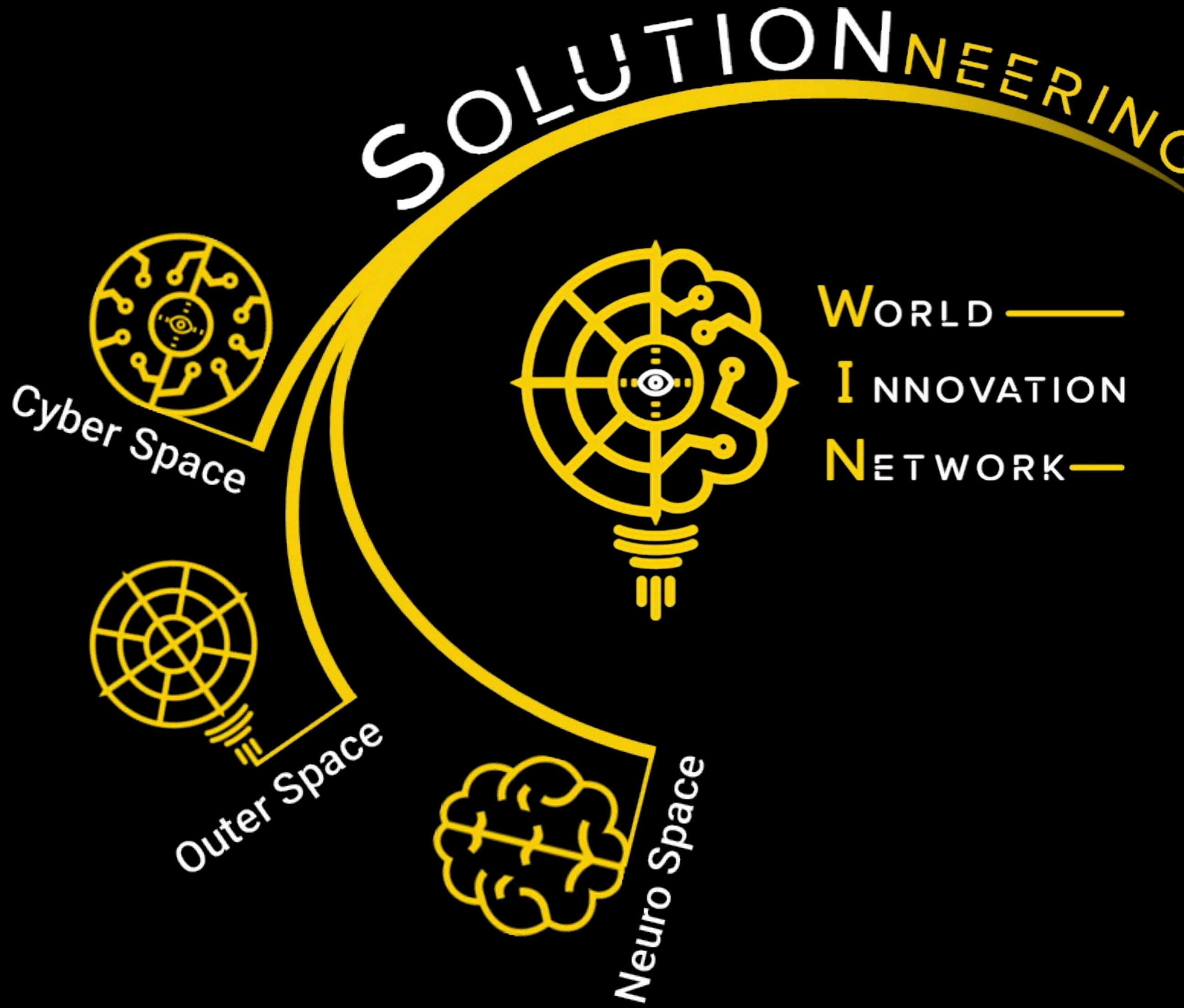
MANUFACTURING

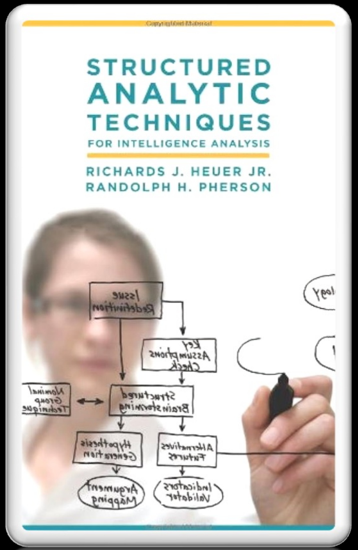
SPECIAL REPORT: Defense Companies Face Post-Pandemic Workforce Shortages

2/9/2023
By Josh Luckenbaugh

Turbulent Times Ahead for Pentagon Weapon Programs

Solution




Copyrighted Material

STRUCTURED ANALYTIC TECHNIQUES

FOR INTELLIGENCE ANALYSIS

RICHARDS J. HEUER JR.
RANDOLPH H. PHERSON

RIGHTLINX.COM

STRATEGIC DEFENSE INITIATIVE
DEPARTMENT OF DEFENSE

Strategic Earthshot Initiative

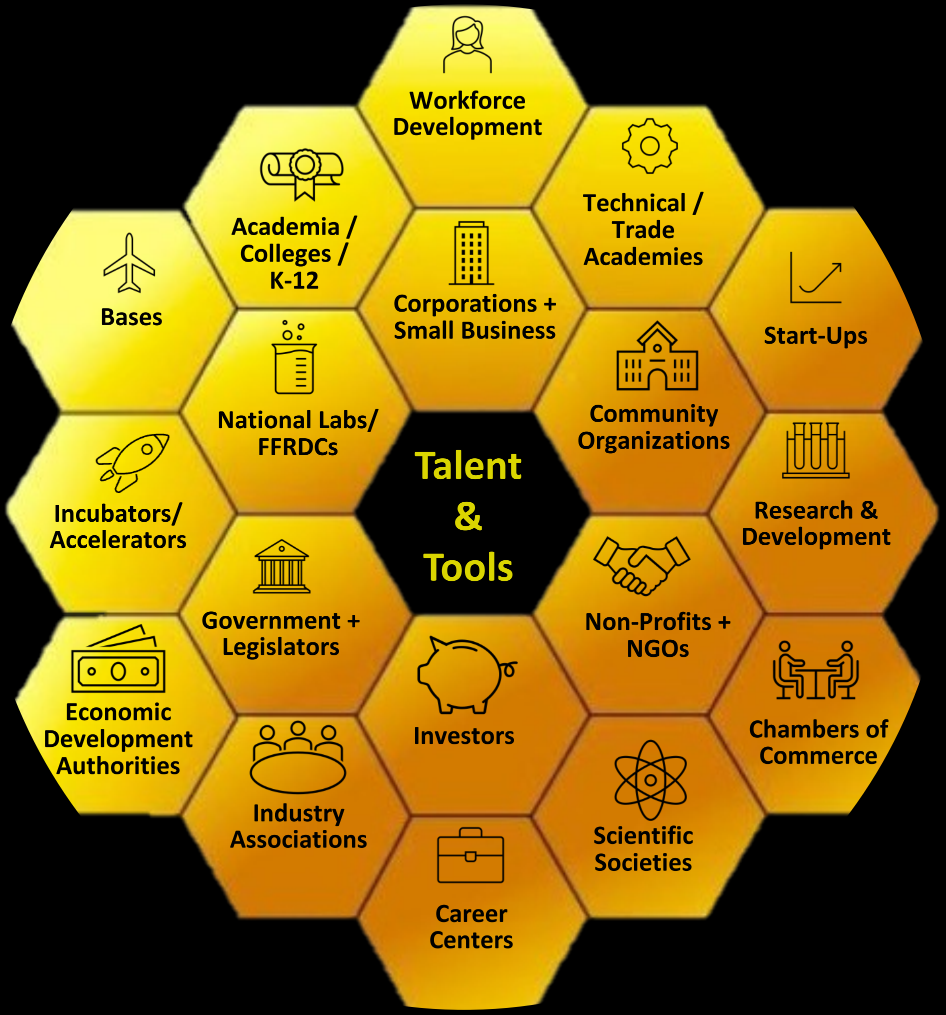
★ Educate ★ Employ ★ Energize ★ Engage ★ Enable ★

Strategic Earthshot Initiative

* Educate * Employ * Energize * Employ * Enable *

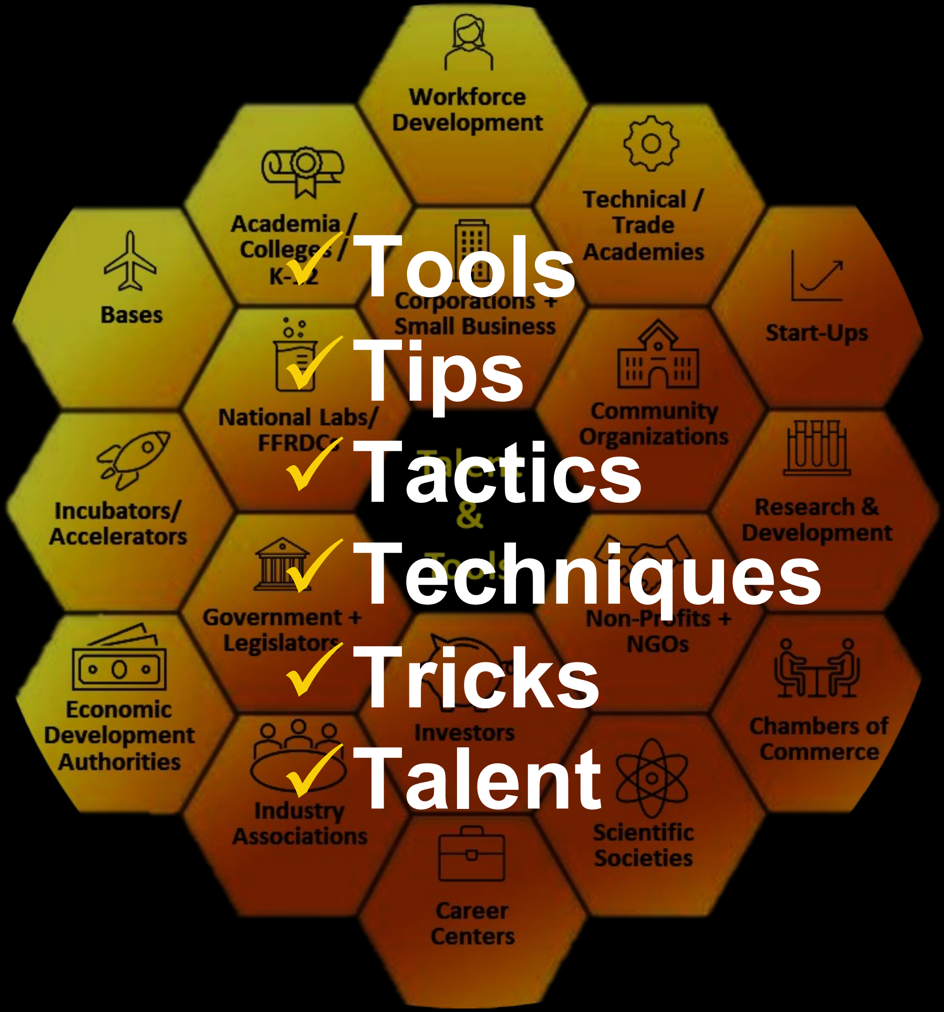
Educate	Community Colleges	4-Year Institutions	Technical Training	K-12 Programs
Employ	Companies	Associations	Chambers	Centers
Energize	Defense Installations	Defense Innovation	National Laboratories	Resources
Engage	Community	Social	Military	Non-Traditional
Enable	Foundations	Providers	Professionals	Media

Initiative 1 - Interconnection: Holistic Hyper-Connectivity



Takes a Village

Initiative 2 - Identification: Hunt & Gather Resources



- ✓ Tools
- ✓ Tips
- ✓ Tactics
- ✓ Techniques
- ✓ Tricks
- ✓ Talent

Initiative 3 - Information: National Space Month

January

su	mo	tu	we	th	fr	sa
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

February

su	mo	tu	we	th	fr	sa
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29

March

su	mo	tu	we	th	fr	sa
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

April

su	mo	tu	we	th	fr	sa
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

May

June

su	mo	tu	we	th	fr	sa
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

July

su	mo	tu	we	th	fr	sa
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

August

su	mo	tu	we	th	fr	sa
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

September

su	mo	tu	we	th	fr	sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

October

su	mo	tu	we	th	fr	sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

November

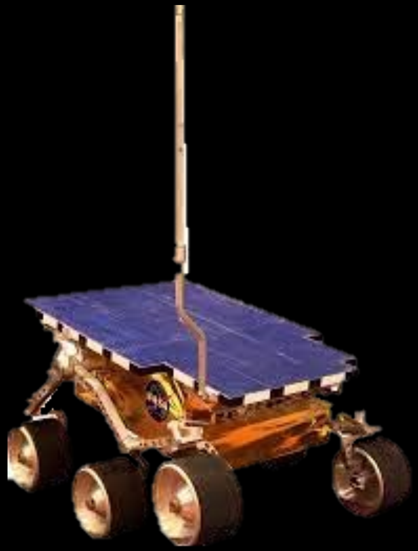
su	mo	tu	we	th	fr	sa
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

December

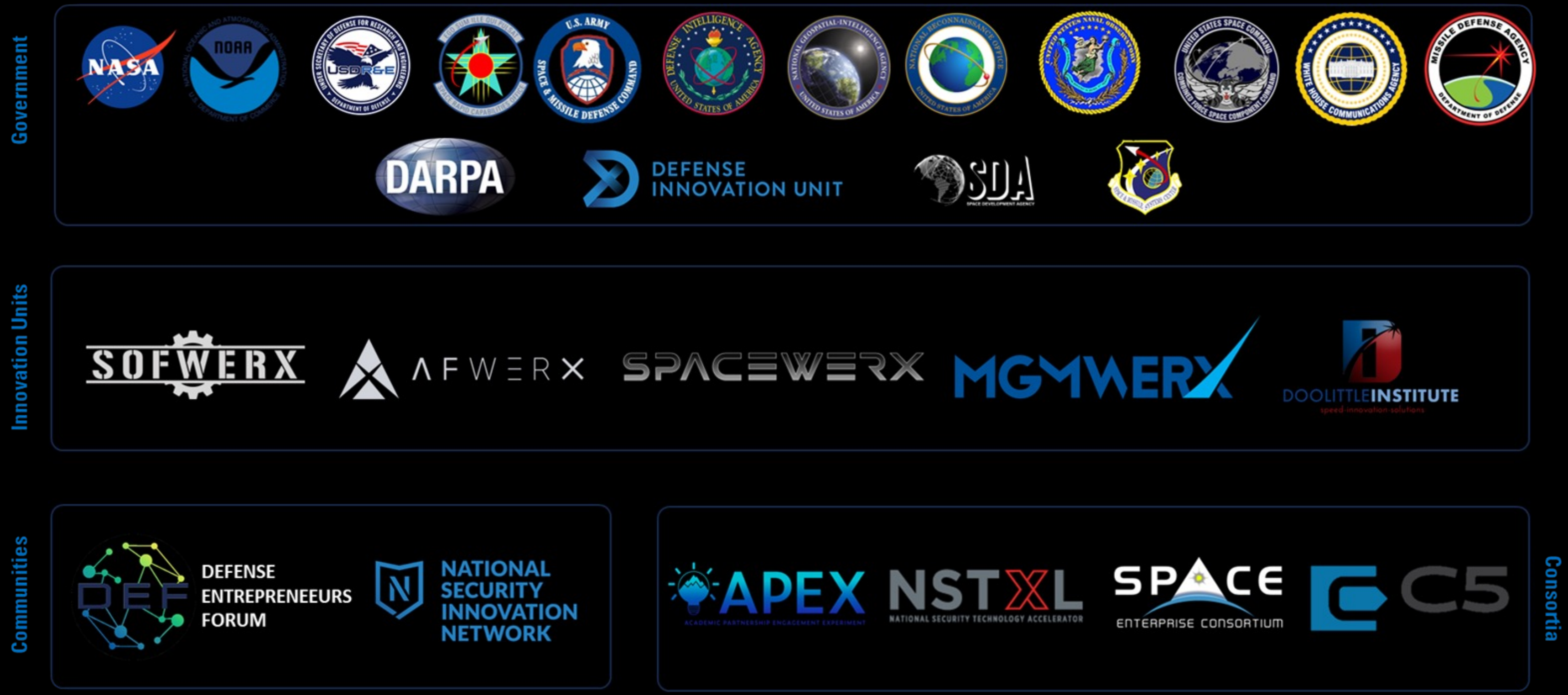
su	mo	tu	we	th	fr	sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

Initiative 4

First Autonomous Vehicle?



Initiative 4 - Incubation: ASTROpreneurship



Government

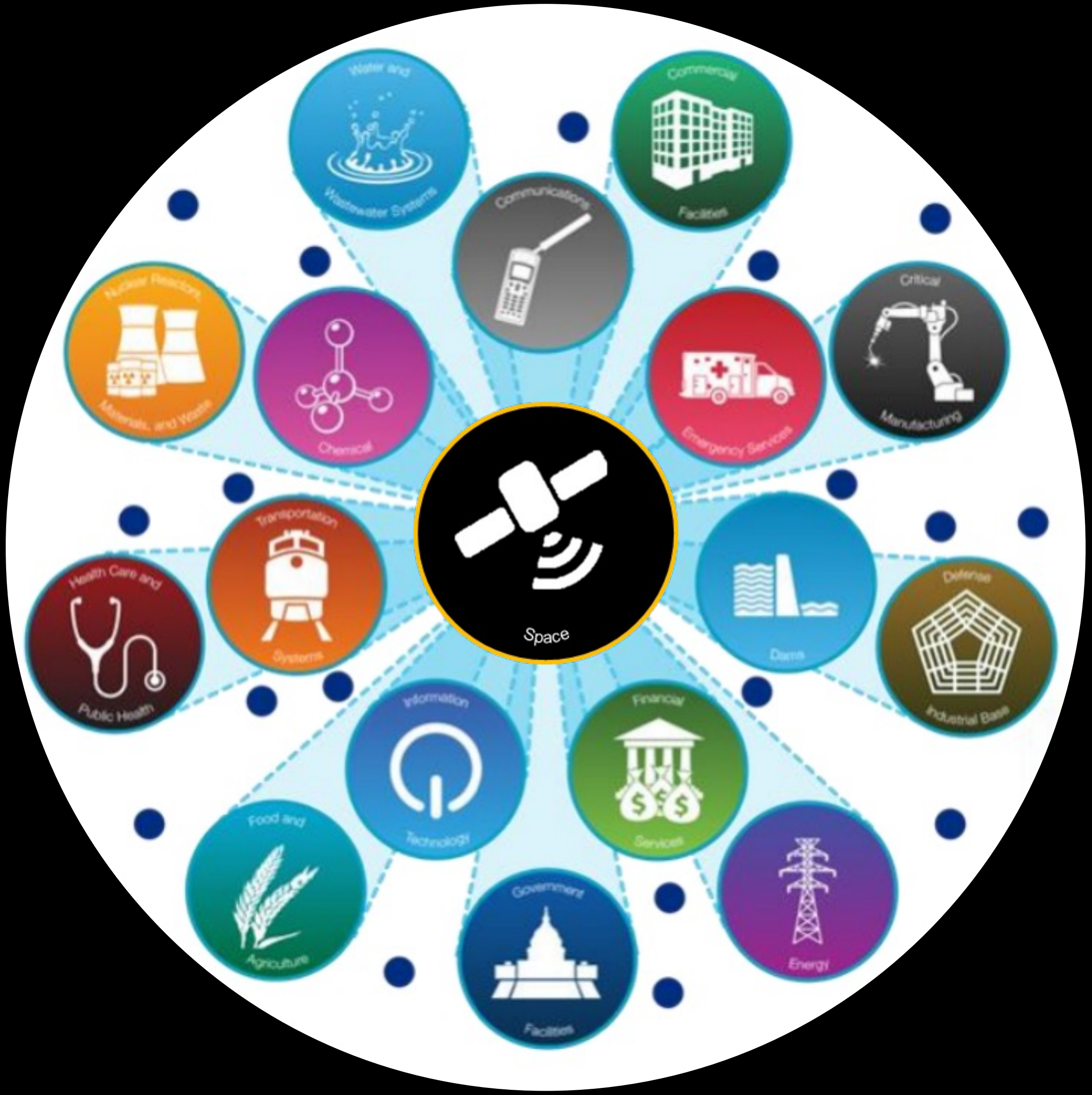
Innovation Units

Communities

Consortia

NASA
NOAA
USD(R&E)
U.S. ARMY SPACE & MISSILE DEFENSE COMMAND
DEFENSE INTELLIGENCE AGENCY
NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY
NATIONAL RECONNAISSANCE OFFICE
UNITED STATES SPACE COMMAND
WHITE HOUSE COMMUNICATIONS AGENCY
MISSILE DEFENSE AGENCY
DARPA
DEFENSE INNOVATION UNIT
SDA
SOFWERX
AFWERX
SPACEWERX
MGMWERX
DOOLITTLEINSTITUTE
DEFENSE ENTREPRENEURS FORUM
NATIONAL SECURITY INNOVATION NETWORK
APEX
NSTXL
NATIONAL SECURITY TECHNOLOGY ACCELERATOR
SPACE ENTERPRISE CONSORTIUM
C5

Initiative 5 - Invigoration: Designated Critical Infrastructure



Initiative 6

SUSTAINABLE DEVELOPMENT GOALS
17 GOALS TO TRANSFORM OUR WORLD
1 NO POVERTY
2 ZERO HUNGER
3 GOOD HEALTH AND WELL-BEING
4 QUALITY EDUCATION
5 GENDER EQUALITY
6 CLEAN WATER AND SANITATION
7 AFFORDABLE AND CLEAN ENERGY
8 DECENT WORK AND ECONOMIC GROWTH
9 INDUSTRY, INNOVATION AND INFRASTRUCTURE
10 REDUCED INEQUALITIES
11 SUSTAINABLE CITIES AND COMMUNITIES
12 RESPONSIBLE CONSUMPTION AND PRODUCTION
13 CLIMATE ACTION
14 LIFE BELOW WATER
15 LIFE ON LAND
16 PEACE, JUSTICE AND STRONG INSTITUTIONS
17 PARTNERSHIPS FOR THE GOALS

Initiative 6

Space Renaissance International

The Human Space Program

EarthLightFoundation

Expanding Frontiers

International Moonbase Alliance

OASA HongKong

Advance Space Civilization Initiative

Space Renaissance Italia

National Space Society

Space Tourism Society

Asgardia

Gen Space

Interstellar Foundation

Ecomodernist Society of NorthAmerica

SpaceFlight UK

Space Renaissance France

The Mars Society

Beyond Earth Institute

Reunion Island Space Agency

Space Value Foundation

Space Nation

Free Astro Science

Ogba Educational Clinic

Space Reanissance USA

Lifeboat Foundation

Space Development Foundation

The Moon Society

Space Development Steering Committee

Exo Tesla

Societé Nouvelle d'Astronomie

Informatics India

The Mars Society Espagna

Global Isos LLC

Lonestar Lunar

World Innovation Network

World's Fair Bid Committee Educational Fund

iDare Space Travel

UNAN-Managua

Caelus Foundation

Foundaciòn ALCASIV

Space Age Publishing Company

Polish Astronautical Society

Lunex

Hyperdrive Anthropology

Interstallar Performance Lab

International Foundation for Aviation and Development

International Space Elevator Consortium

Center for Global Agenda (CGA) at Unbuilt Labs

American Institute of Aeronautics and Astronautics

The Space Treaty Project

Space Renaissance Poland

Habitat Marte

4 OMID

Space 4 Climate

OTESPACE

Ares Learning

Space For Progress

Society for Space Culture

Space Base

bbcmgtAI LLC

SUSTAIN A VERSE

Mature Development BV

Space Career and Leadership Center

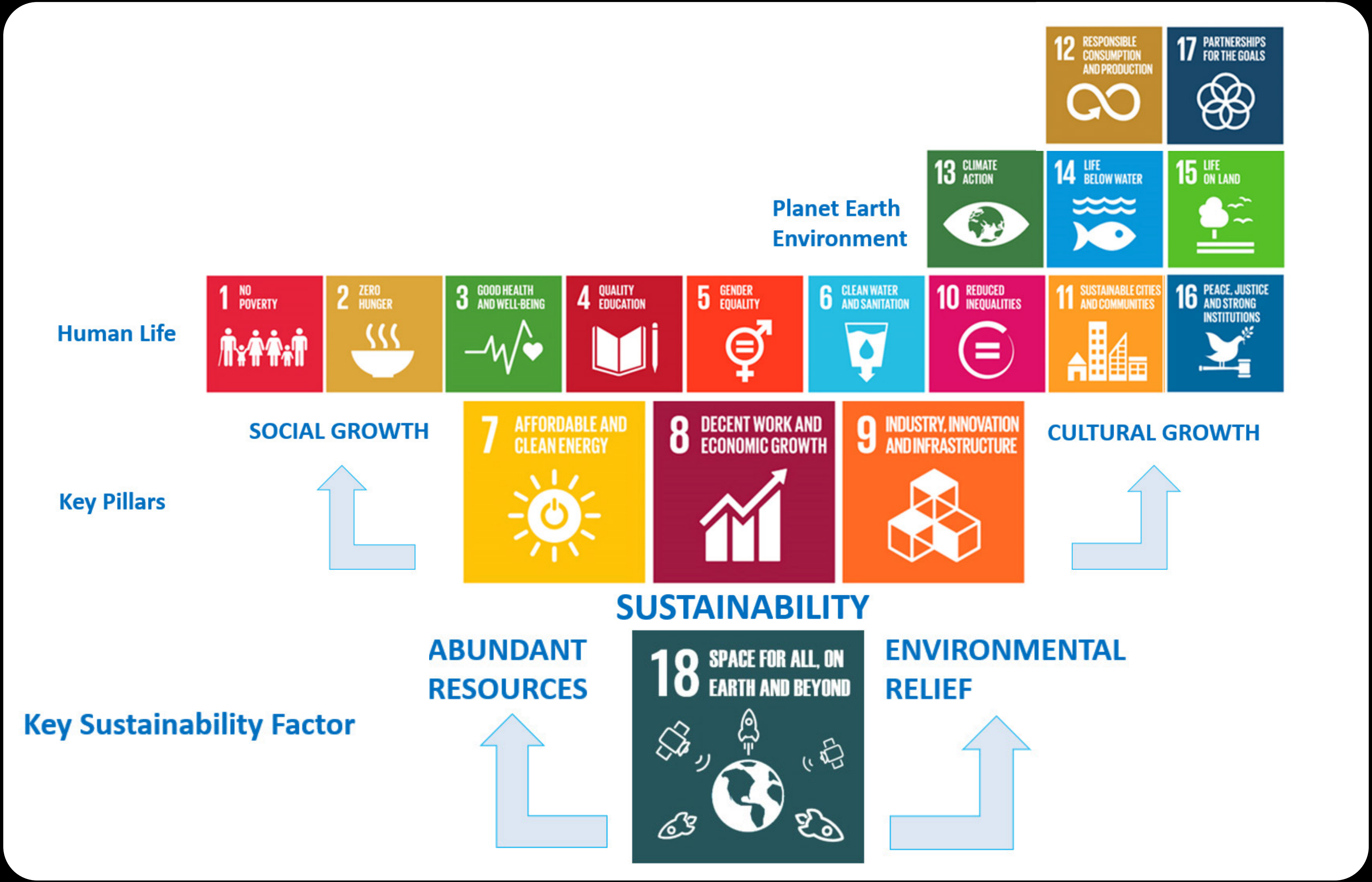
Riebens Computers

Africa VR Center and Campus

European Institute of Innovation for Sustainability

United Humanity of the Universe

Initiative 6



Planet Earth Environment

Human Life

SOCIAL GROWTH

CULTURAL GROWTH

Key Pillars

SUSTAINABILITY

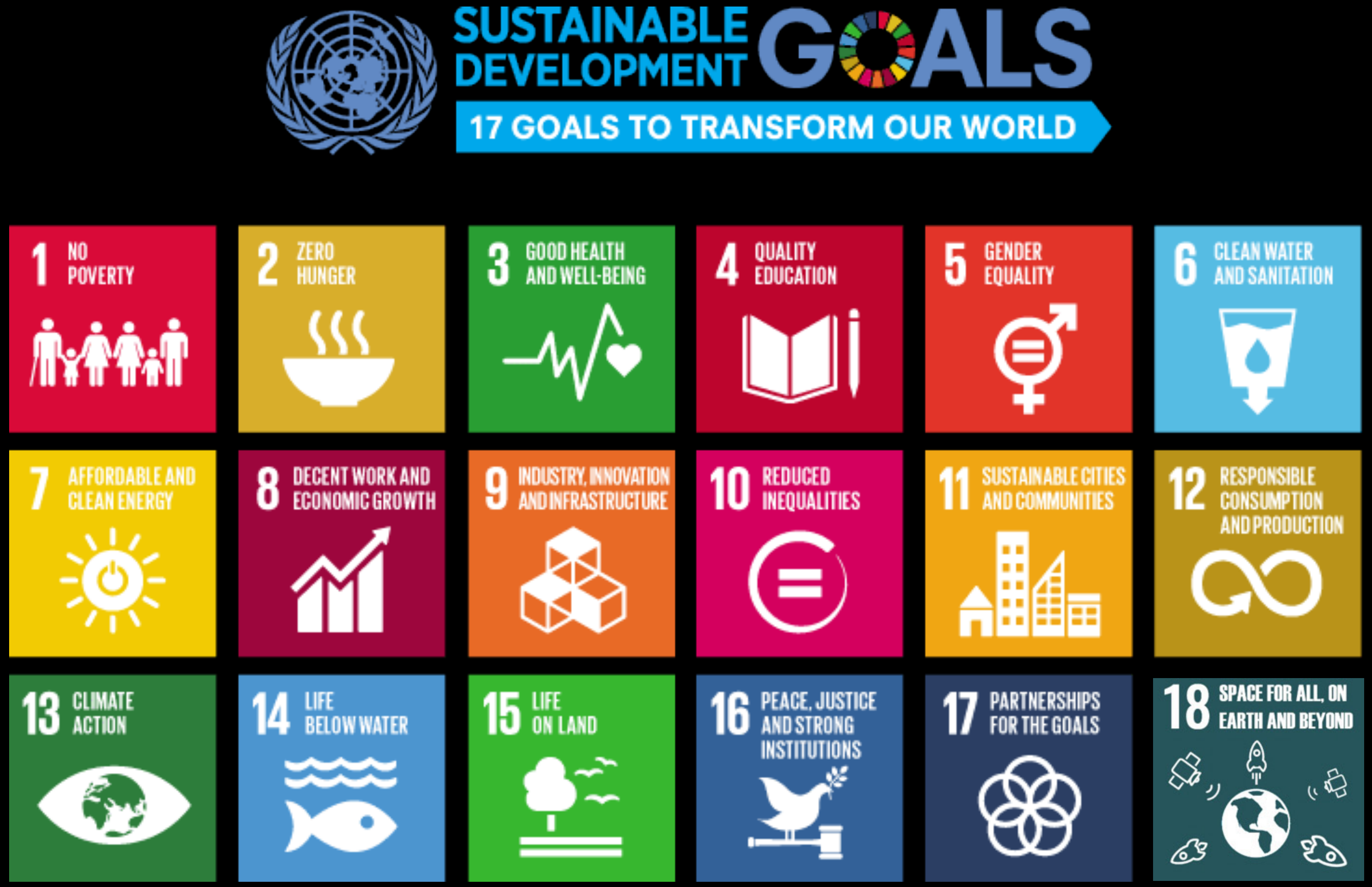
ABUNDANT RESOURCES

ENVIRONMENTAL RELIEF

Key Sustainability Factor

12 RESPONSIBLE CONSUMPTION AND PRODUCTION
17 PARTNERSHIPS FOR THE GOALS
13 CLIMATE ACTION
14 LIFE BELOW WATER
15 LIFE ON LAND
1 NO POVERTY
2 ZERO HUNGER
3 GOOD HEALTH AND WELL-BEING
4 QUALITY EDUCATION
5 GENDER EQUALITY
6 CLEAN WATER AND SANITATION
10 REDUCED INEQUALITIES
11 SUSTAINABLE CITIES AND COMMUNITIES
16 PEACE, JUSTICE AND STRONG INSTITUTIONS
7 AFFORDABLE AND CLEAN ENERGY
8 DECENT WORK AND ECONOMIC GROWTH
9 INDUSTRY, INNOVATION AND INFRASTRUCTURE
18 SPACE FOR ALL, ON EARTH AND BEYOND

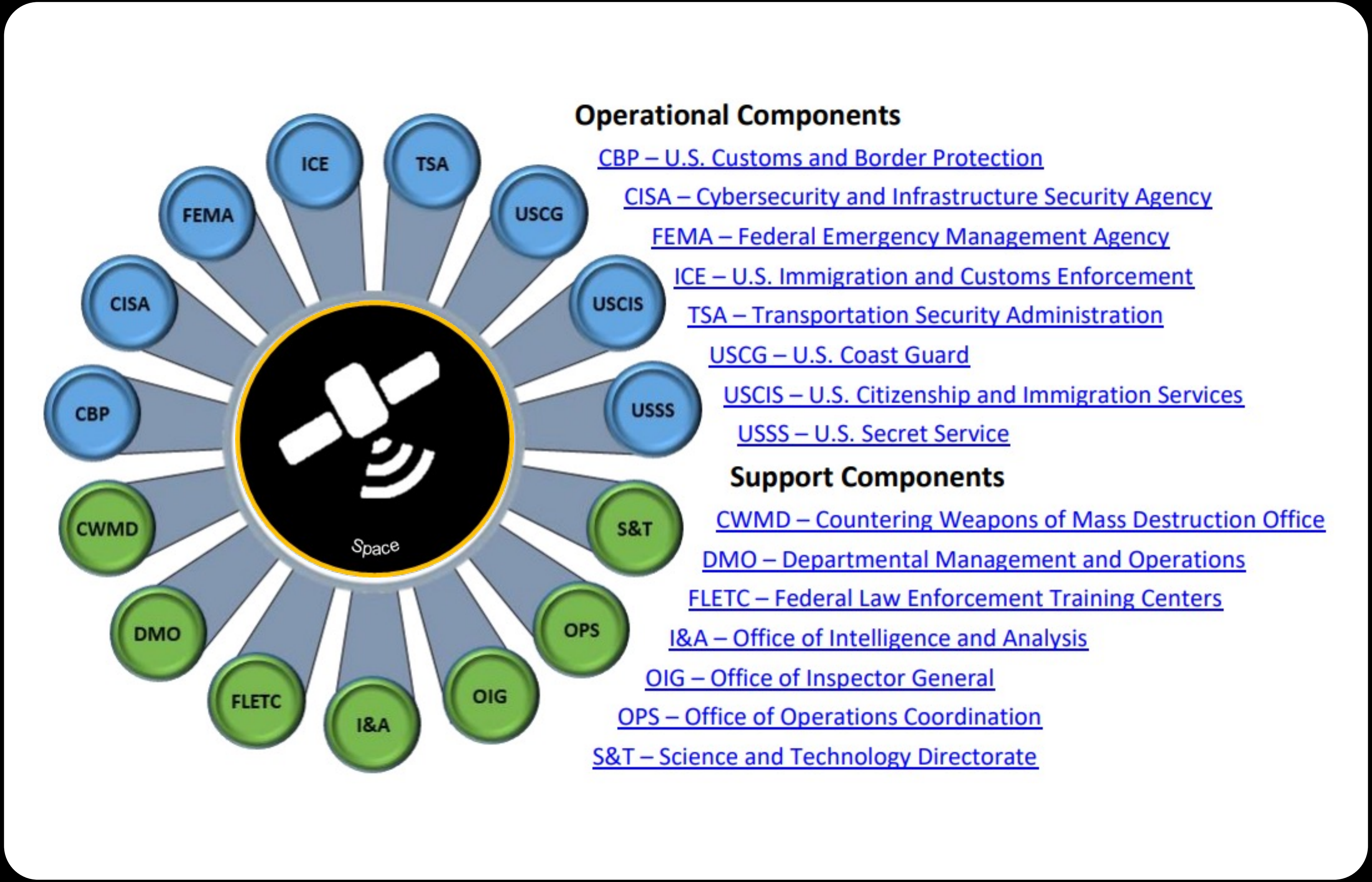
Initiative 6 - Interconnection: UN SDGs


SUSTAINABLE DEVELOPMENT GOALS
17 GOALS TO TRANSFORM OUR WORLD
1 NO POVERTY
2 ZERO HUNGER
3 GOOD HEALTH AND WELL-BEING
4 QUALITY EDUCATION
5 GENDER EQUALITY
6 CLEAN WATER AND SANITATION
7 AFFORDABLE AND CLEAN ENERGY
8 DECENT WORK AND ECONOMIC GROWTH
9 INDUSTRY, INNOVATION AND INFRASTRUCTURE
10 REDUCED INEQUALITIES
11 SUSTAINABLE CITIES AND COMMUNITIES
12 RESPONSIBLE CONSUMPTION AND PRODUCTION
13 CLIMATE ACTION
14 LIFE BELOW WATER
15 LIFE ON LAND
16 PEACE, JUSTICE AND STRONG INSTITUTIONS
17 PARTNERSHIPS FOR THE GOALS
18 SPACE FOR ALL, ON EARTH AND BEYOND

Initiative 7

THE WHITE HOUSE
WASHINGTON
DEPARTMENT OF LABOR
UNITED STATES OF AMERICA
DEPARTMENT OF COMMERCE
UNITED STATES OF AMERICA
THE DEPARTMENT OF THE TREASURY
1789
DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA
DEPARTMENT OF HEALTH & HUMAN SERVICES
USA
U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
DEPARTMENT OF STATE
UNITED STATES OF AMERICA
UNITED STATES DEPARTMENT OF AGRICULTURE
1862
1889
AGRICULTURE IS THE FOUNDATION OF MANUFACTURE AND COMMERCE
DEPARTMENT OF JUSTICE
QUI PRO DOMINA JUSTITIA SEQUITUR
DEPARTMENT OF TRANSPORTATION
UNITED STATES OF AMERICA
DEPARTMENT OF EDUCATION
UNITED STATES OF AMERICA
DEPARTMENT OF VETERANS AFFAIRS
UNITED STATES OF AMERICA
U.S. DEPARTMENT OF THE INTERIOR
MARCH 3, 1849
U.S. DEPARTMENT OF HOMELAND SECURITY
DEPARTMENT OF ENERGY
UNITED STATES OF AMERICA

Initiative 7



Operational Components

- CBP – U.S. Customs and Border Protection
- CISA – Cybersecurity and Infrastructure Security Agency
- FEMA – Federal Emergency Management Agency
- ICE – U.S. Immigration and Customs Enforcement
- TSA – Transportation Security Administration
- USCG – U.S. Coast Guard
- USCIS – U.S. Citizenship and Immigration Services
- USSS – U.S. Secret Service

Support Components

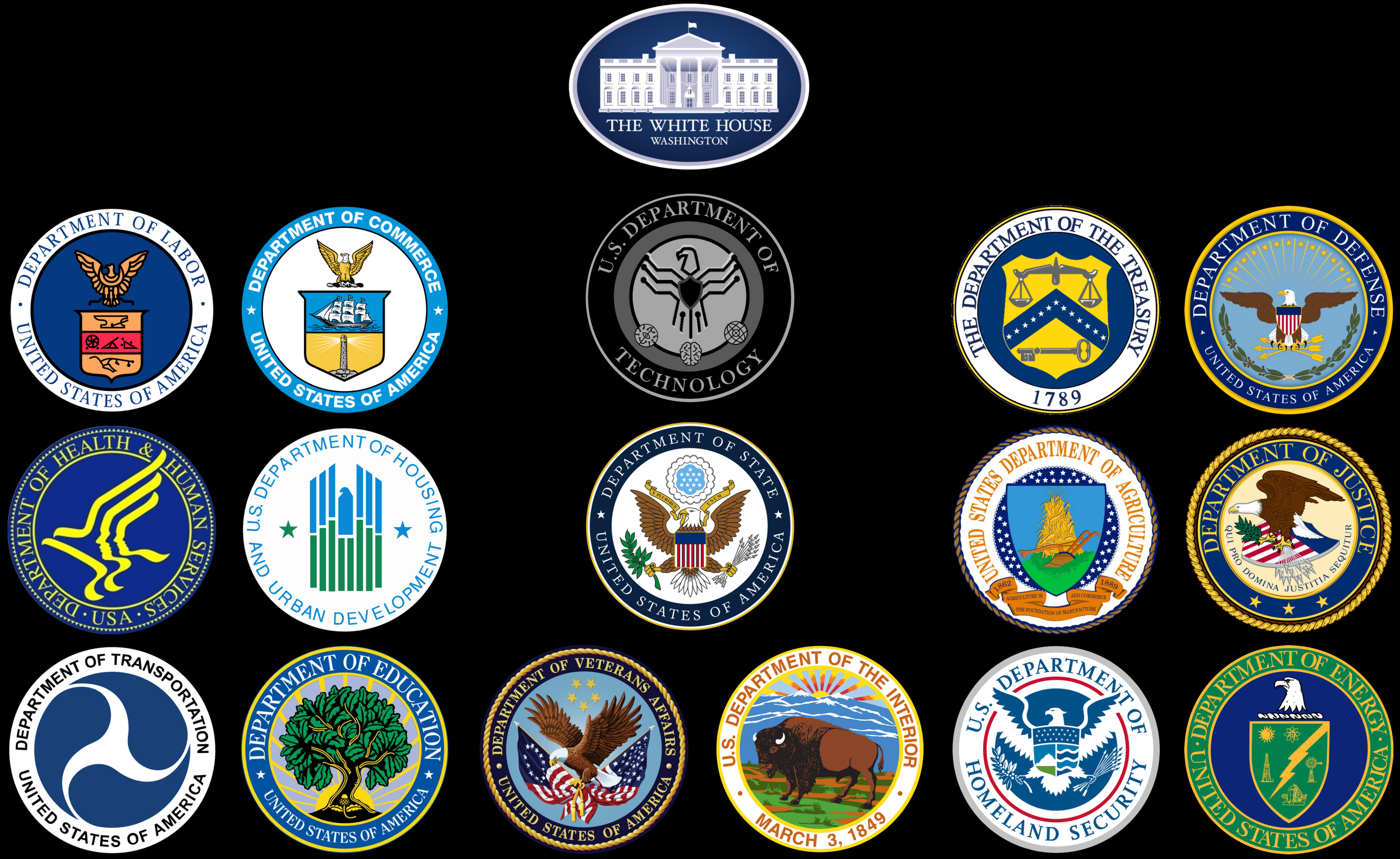
- CWMD – Countering Weapons of Mass Destruction Office
- DMO – Departmental Management and Operations
- FLETC – Federal Law Enforcement Training Centers
- I&A – Office of Intelligence and Analysis
- OIG – Office of Inspector General
- OPS – Office of Operations Coordination
- S&T – Science and Technology Directorate

Initiative 7

THE WHITE HOUSE
WASHINGTON
DEPARTMENT OF LABOR UNITED STATES OF AMERICA
DEPARTMENT OF COMMERCE UNITED STATES OF AMERICA
Space
THE DEPARTMENT OF THE TREASURY 1789
DEPARTMENT OF DEFENSE UNITED STATES OF AMERICA
DEPARTMENT OF HEALTH & HUMAN SERVICES · USA ·
U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
DEPARTMENT OF STATE UNITED STATES OF AMERICA
UNITED STATES DEPARTMENT OF AGRICULTURE 1862 1889
DEPARTMENT OF JUSTICE QUI PRO DOMINA JUSTITIA SEQUITUR
DEPARTMENT OF TRANSPORTATION UNITED STATES OF AMERICA
DEPARTMENT OF EDUCATION UNITED STATES OF AMERICA
DEPARTMENT OF VETERANS AFFAIRS UNITED STATES OF AMERICA
U.S. DEPARTMENT OF THE INTERIOR MARCH 3, 1849
U.S. DEPARTMENT OF HOMELAND SECURITY
DEPARTMENT OF ENERGY UNITED STATES OF AMERICA

Initiative 7

Initiative 7 - Department of Technology (DTECH)


THE WHITE HOUSE
WASHINGTON
U.S. DEPARTMENT OF TECHNOLOGY
DEPARTMENT OF LABOR UNITED STATES OF AMERICA
DEPARTMENT OF COMMERCE UNITED STATES OF AMERICA
THE DEPARTMENT OF THE TREASURY 1789
DEPARTMENT OF DEFENSE UNITED STATES OF AMERICA
DEPARTMENT OF HEALTH & HUMAN SERVICES USA
U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
DEPARTMENT OF STATE UNITED STATES OF AMERICA
UNITED STATES DEPARTMENT OF AGRICULTURE
DEPARTMENT OF JUSTICE
QUI PRO DOMINA JUSTITIA SEQUITUR
DEPARTMENT OF TRANSPORTATION UNITED STATES OF AMERICA
DEPARTMENT OF EDUCATION UNITED STATES OF AMERICA
DEPARTMENT OF VETERANS AFFAIRS UNITED STATES OF AMERICA
U.S. DEPARTMENT OF THE INTERIOR MARCH 3, 1849
U.S. DEPARTMENT OF HOMELAND SECURITY
DEPARTMENT OF ENERGY UNITED STATES OF AMERICA

Initiative 8

Initiative 8

Initiative 8

Initiative 8

DeEvolution

Initiative 8 - Star Corps

Star corps

Initiative 9 - Inclusion: Everyone

Inclusive of

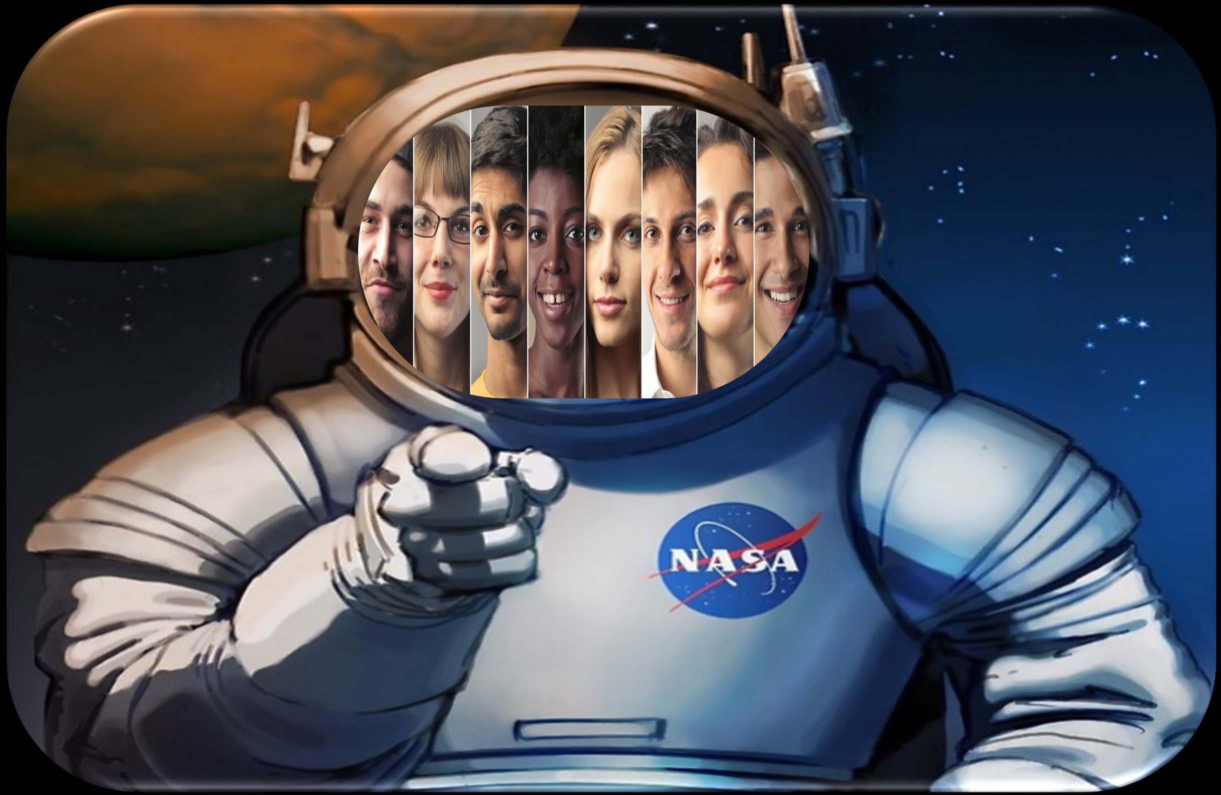
- Every Demographic
- Every Non-STEMer
- Every Background
- Every Community
- Every Experience
- Every Affiliation
- Every Discipline
- Every Diversity
- Every STEMer
- Every Domain
- Every Interest
- Every Subject
- Every Identity
- Every Profile
- Every Ability
- Every Talent
- Every Grade
- Every Major
- Every Level
- Every Field
- Every Skill
- Every Gift
- Every Age
- EveryOne!

People

Fun for

- All Aerospace-Fans
- All Problem-Solvers
- All Flight-Engineers
- All Videographers
- All Nature-Lovers
- All Entrepreneurs
- All Technologists
- All Star-Gazers
- All Journalists
- All Storytellers
- All Developers
- All Innovators
- All Musicians
- All Designers
- All Dreamers
- All Engineers
- All Scientists
- All Creatives
- All Thinkers
- All Builders
- All Aviators
- All Gamers
- All Makers
- All Writers
- All Coders
- All Artists
- All You!

There's a Place In Space For Every Face



ARTEMIS

Strategic Earthshot Initiative

★ Educate ★ Employ ★ Energize ★ Engage ★ Enable ★

May the cyber - Space
Work Force Be with You

Thank

You

The Sky's not the Limit…Anymore

Robert S. Katz
rsk@win.ngo
+1.301.983.6700

World
Innovation
Network

LinkedIn

https://win.ngo/li

https://www.linkedin.com/in/robert-scott-katz/

SPACE ISAC

VALUE OF SPACE SUMMIT 2023

Co-hosted by AEROSPACE