Developing an AI-Enabled Cybersecurity Model to Protect Satellite Systems from Cyber Threats

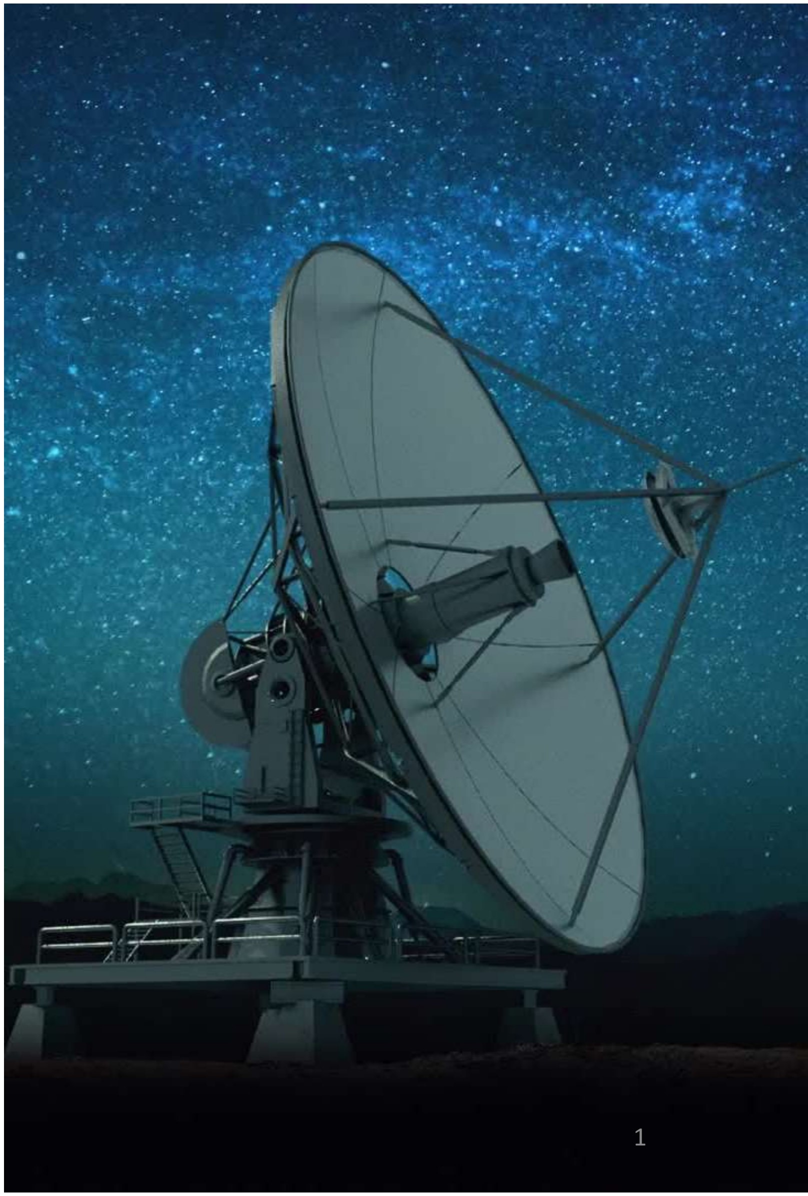
Presented by:

Alex Thach,

Team:

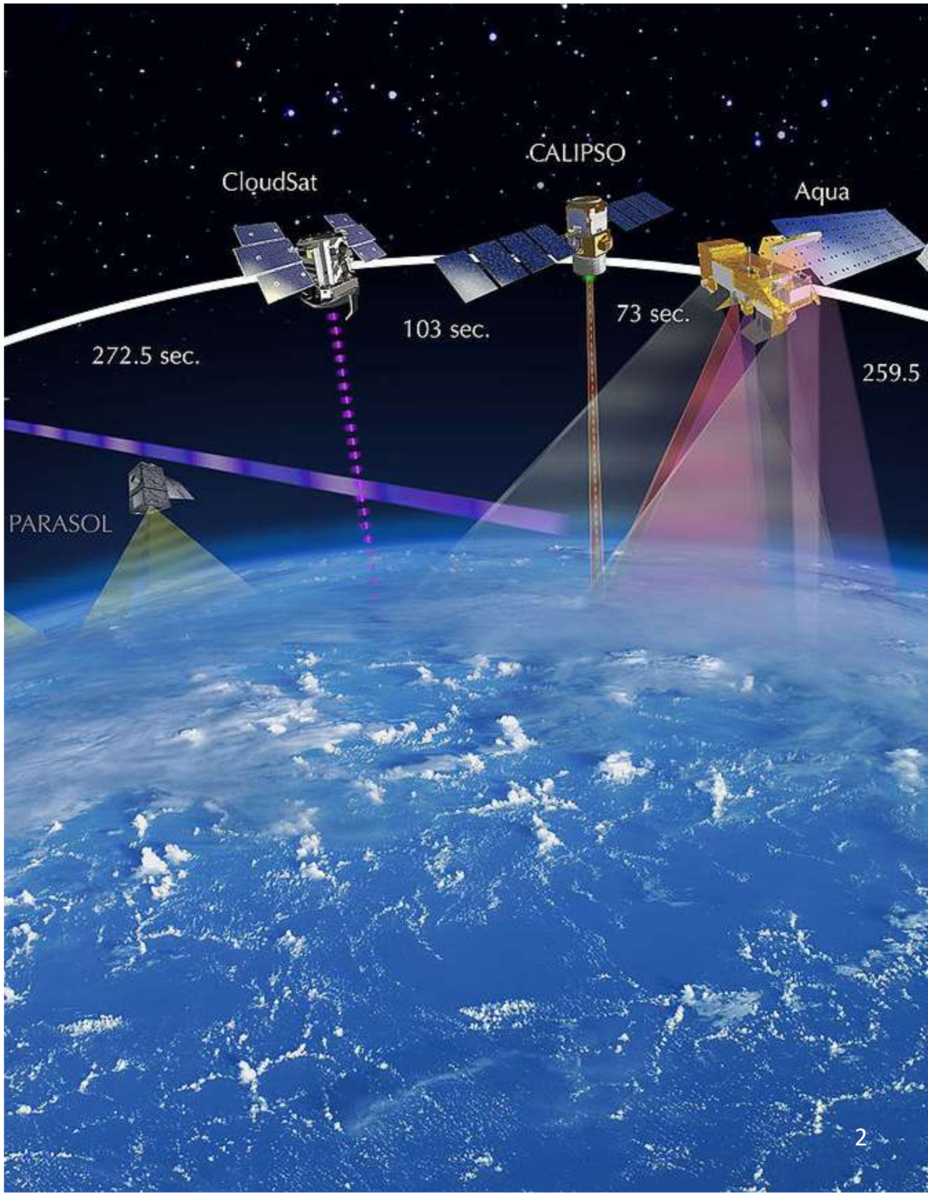
Nijanthan Vasudevan, Arjuna Karthikeyan Senthilvel Kavitha, Cassie Paoli,

Astrada Cyber Labs LLC & Drexel University - United States



The Role of Satellites in Today's World

- Indispensable Role: Satellites power vital functions - from GPS to global communications.
- Rapid Expansion: As tech advances, satellites govern more aspects of our lives.
- Cyber Threat Landscape: As importance grows, so does the attraction for cybercriminals.
- Security Imperative: Protecting satellite infrastructure is paramount for safety & reliability.

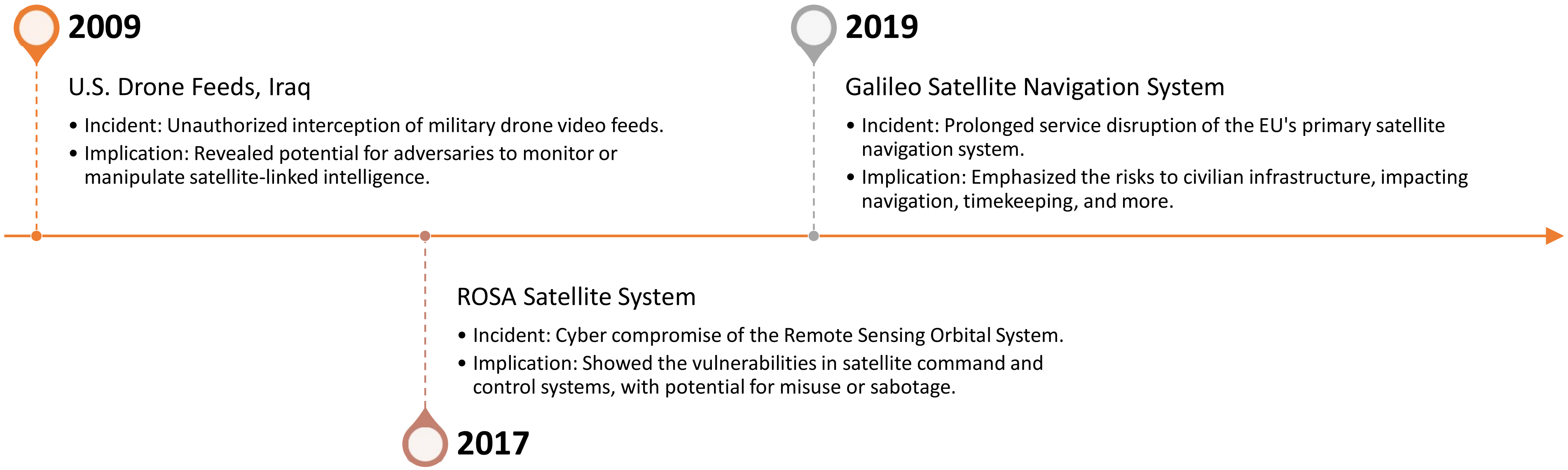


Satellite Cybersecurity Background : The Evolving Threat Landscape

- **Ground-Based Targets:**
  - In the early days of the internet, hackers targeted computer servers, networks, and infrastructure, as these were the most accessible and provided potential for financial gain or mischief.
- **Satellite Integration:**
  - This integration means satellite data breaches can have real-world, immediate impacts, such as disruptions in telecommunications or GPS failures.
- **Satellite Defense in Real-time:**
  - With satellites orbiting at great distances, immediate physical intervention is impossible. Thus, on-board systems must be equipped to identify, fend off, and recover from attacks autonomously or through ground-based commands.
- **Evolving Threats:**
  - Modern cyber threats are not just about brute force or simple malware. They involve advanced persistent threats (APTs), zero-day exploits, and sophisticated state-backed cyber operations.

IAC-23,D5,4,4,x80363 - 74th I

Notable Satellite Cyber Incidents : When Things Go Wrong



2009

U.S. Drone Feeds, Iraq

- Incident: Unauthorized interception of military drone video feeds.
- Implication: Revealed potential for adversaries to monitor or manipulate satellite-linked intelligence.

2017

ROSA Satellite System

- Incident: Cyber compromise of the Remote Sensing Orbital System.
- Implication: Showed the vulnerabilities in satellite command and control systems, with potential for misuse or sabotage.

2019

Galileo Satellite Navigation System

- Incident: Prolonged service disruption of the EU's primary satellite navigation system.
- Implication: Emphasized the risks to civilian infrastructure, impacting navigation, timekeeping, and more.

Traditional Cybersecurity Solutions : The First Line of Defense

- **Encryption:**
  - Technique: Ensures data transmitted to and from satellites is coded, preventing unauthorized access.
  - Limitations: New decryption techniques and quantum computing advancements can threaten the efficacy of existing encryption methods.
- **Segmentation:**
  - Technique: Dividing satellite systems into distinct zones or segments, preventing a breach in one area from compromising the entire system.
  - Limitations: As integration needs grow, maintaining efficient segmentation without hindering operations becomes challenging.
- **Physical Security:**
  - Technique: Safeguarding the satellite's physical components, ground stations, and uplink/downlink systems.
  - Limitations: Physical security can't counteract remote cyber threats, and securing expansive ground-based infrastructure is logistically complex.
- **Intrusion Detection Systems (IDS):**
  - Technique: Monitors and alerts of any unauthorized access or anomalies in the system.
  - Limitations: Sophisticated attacks can evade or disable IDS, and false positives can divert attention from genuine threats.

The Need for Advanced Solutions

Beyond Traditional Measures

Limitations of Traditional Cybersecurity Measures:

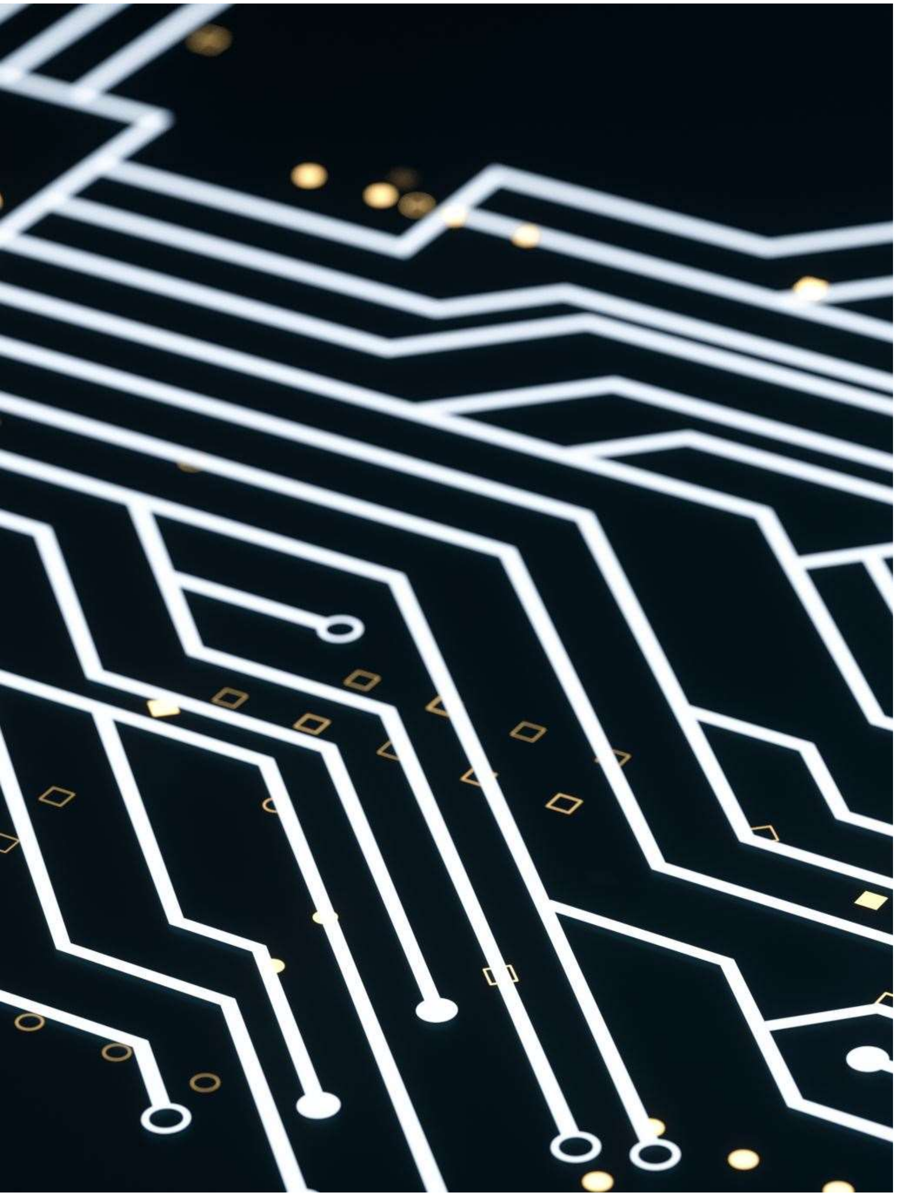
Reactivity: Traditional measures often focus on reacting to known threats rather than proactively identifying and countering emerging ones.

Patch Management: Constantly updating security patches can lag the discovery of new vulnerabilities.

Static Defense Mechanisms: Conventional firewalls and intrusion detection systems may not be equipped to handle evolving and sophisticated threats.

Call for Proactive Solutions:

- **Predictive Analytics:** Utilize AI and machine learning to anticipate patterns indicative of potential threats.
- **Behavioral Analysis:** Analyze network behavior to identify anomalies and potential intrusions.
- **Threat Intelligence:** Constantly updated databases and feeds that provide insights into current global threat landscapes.
- **Adaptive Security Architectures:** Dynamic security measures that can evolve based on the threat encountered.



AI's Role in Enhancing Cybersecurity : The AI Revolution

- **Anomaly Detection:**
  - **Deep Learning:** Using neural networks to analyze massive datasets, AI can identify subtle, unusual patterns that might be indicative of a security breach.
  - **Continuous Monitoring:** AI systems can monitor network traffic 24/7 without fatigue, ensuring that anomalies are spotted the moment they occur.
- **Predictive Analysis:**
  - **Forecasting Threats:** AI algorithms can analyze past attacks and current network behaviors to predict future threat vectors.
  - **Risk Assessment:** Determine which assets are most at risk based on past incidents and current configurations, enabling prioritized defense measures.
- **Automated Response:**
  - **Instantaneous Reaction:** Upon detecting a threat, AI systems can instantly initiate predefined security protocols, minimizing damage.
  - **Dynamic Countermeasures:** Based on the nature of the intrusion, AI can adapt its response strategy for optimal defense.

AthenaDetect - An AI-Driven Solution

Holistic Integration:AI (Artificial Intelligence):

Capabilities: Anomaly detection, predictive analysis, automated responses.

Benefit: Dynamic, adaptive, and real-time security enhancements.

SIEM (Security Information and Event Management):

Capabilities: Real-time collection and analysis of security alerts from various hardware and software assets.

Benefit: Centralized security data processing for faster threat detection and incident response.

SOAR (Security Orchestration, Automation, and Response):

Capabilities: Automates responses to security incidents, coordinating actions across diverse solutions.

Benefit: Reduces response times and human intervention needs during security events.

SPARTA Framework:

Capabilities: SPARTA offers guidelines for satellite security, addressing space-system TTPs. It equips professionals with actionable info on spacecraft threats.

Benefit: Using SPARTA ensures adherence to top satellite security standards, boosting space asset resilience.

Athena Detect Architecture : Overview

Central Infrastructure

- **AI Core Engine:**
  - **Function:** Processes vast amounts of data to identify patterns, threats, and anomalies.
  - **Benefit:** Provides real-time threat detection, predictive analysis, and automated response for enhanced security.
- **Elasticsearch:**
  - **Function:** A highly scalable open-source search and analytics engine that allows for real-time data retrieval and analysis.
  - **Benefit:** Enables rapid and efficient processing of large datasets, allowing the AI Core Engine to operate effectively and offer actionable insights quickly.
  - https://www.elastic.co/downloads/
- **SPARTA Framework Integration:**
  - **Function:** SPARTA delivers comprehensive guidelines and best practices for satellite security, addressing space-system Tactic, Techniques, and Procedures (TTP).
  - **Benefit:** Ensures AI and Elasticsearch components adhere to industry-leading satellite security standards, enhancing the infrastructure's resilience and reliability.

Athena Detect Architecture : Overview

Edge Devices/On-Premises Systems

- **Lightweight AI Models:**
  - **Function:** AI models tailored for edge devices, requiring minimal computational resources while still offering effective threat detection and response.
  - **Benefit:** Enables even devices with limited processing capabilities to benefit from advanced AI-driven security measures, ensuring a wider coverage of protection.
- **Data Collection Modules:**
  - **Function:** Gathers relevant data from edge devices/on-premises systems and forwards it to the central infrastructure for further analysis.
  - **Benefit:** Provides real-time visibility into the operations of edge devices, allowing for timely detection and response to any security events or anomalies.

System Integration : Open-Source Tools & Solutions

Satellite Telemetry Tools

- **SatNOGS:**
  - Facilitates tracking, communication, and data reception from various satellites.
  - Provides a scalable, open-source, and community-driven platform for satellite telemetry, enabling a decentralized approach to receiving data.
  - https://satnogs.org/
- **GNU Radio:**
  - Enables receiving, decoding, and processing of satellite signals. Flexible and customizable, allowing for the design and implementation of a variety of satellite communication protocols and systems.

Firewall Solutions

- **pfSense**:
  - Function: Provides network firewall protection and a range of related security features.
  - Benefit: Offers a robust, scalable, and flexible platform for securing network infrastructure, with a wide range of plugins and extensions.
- **Suricata**:
  - Function: Monitors network traffic, identifies potential threats, and can actively intervene or passively monitor depending on the configuration.
  - Benefit: Multi-threaded, efficient, and compatible with major OSs, making it a versatile tool for real-time intrusion detection.

NDR/XDR Solutions

- **Zeek (formerly known as Bro):**
  - Function: Analyses network traffic, extracts logs, and identifies suspicious activities.
  - Benefit: Beyond traditional IDS capabilities

TheHive Integration & SOAR Responses : Automated Responses with TheHive

- **TheHive** as the Integrated Incident Management Platform: Centralized platform for incident tracking and management. Seamless integration with other security tools for holistic incident response. Real-time collaboration among incident response teams.
- **SPARTA TTPs** Recognition and Automated SOAR Responses: Identification of Tactics, Techniques, and Procedures (TTPs) using SPARTA. Automation of Security Orchestration, Automation, and Response (SOAR) based on recognized TTPs. Enhanced security posture with proactive and reactive measures.
- Feedback Loop with AI Core Engine for Continuous Model Refinement: Machine learning models that learn from every incident. Continuous refinement of response strategies based on feedback. Ensuring the AI core engine stays updated with the latest threat landscape.

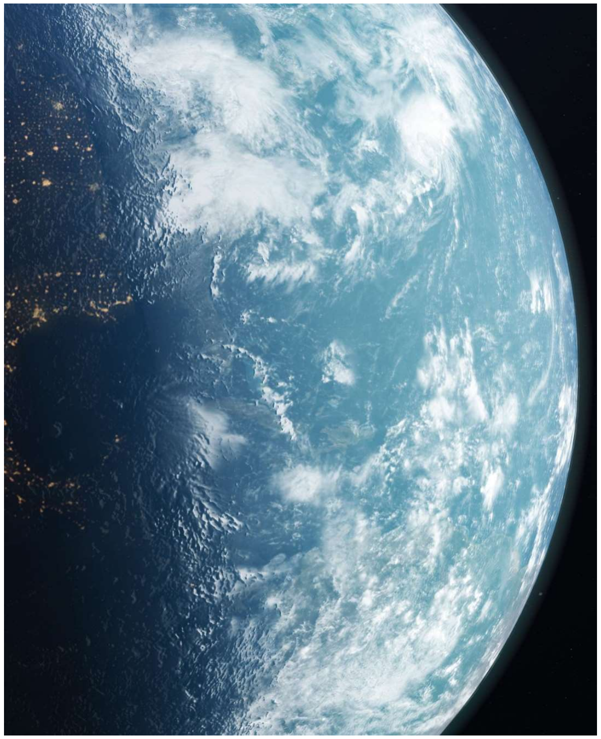
Collaborative Defense : Strengthened Defense

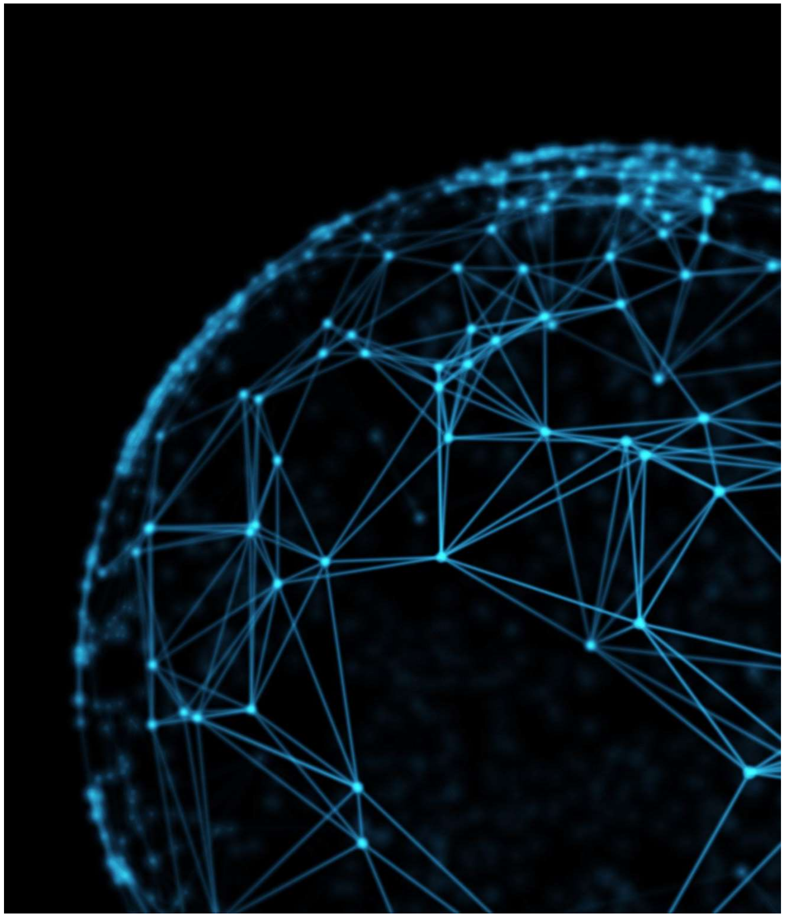
- Integration of TheHive with SPARTA insights and SOAR for a unified threat view, streamlined communication, and enhanced decision-making.
- TheHive's real-time collaboration and centralized incident management combined with SPARTA's advanced threat hunting and TTP identification.
- SOAR's automated response actions, reduction in manual tasks, and faster threat containment.
- Efficient threat response through proactive hunting, incident prioritization, automated workflows, and team-based incident management.
- Enhanced satellite cybersecurity with 24/7 surveillance, data encryption, regular audits, and training for satellite

Recent Satellite Cybersecurity Incidents :

The Global Cyber Cold War

- Nation-states prioritize taking control of another nation’s satellite infrastructure and destroying it or rendering it useless.
- Shutting down a competing nation’s satellites stops real-time communications, cuts off situational awareness of operating units across militaries, and halts navigation.
- Denying a competing nation’s access to space is quickly becoming the most dangerous weapon in the stealth world of cyber warfare.
- Satellites and access to space are essential for national security. By 2030, there will be an average of 1,700 satellites launched per year, and governments will continue to fund 75% of satellite manufacturing and launching.
- The global satellite communication (SATCOM) market size was estimated at $77B in 2022 and is expected to grow at a compound annual growth rate (CAGR) of 9.7% from 2023 to 2030.
- Credit: https://venturebeat.com/security/building-more-cyber-resilient-satellites-begins-with-a-strong-network/





Why Satellites Are Strategic Targets : Militarization of Space

- In an article listed as 2022 Challenges to Security in Space report: “Space is being increasingly militarized. Some nations have developed, tested, and deployed various satellites and some counter-space weapons. Certain nations are developing new space systems to improve their military effectiveness and reduce any reliance on space systems.
- The agency cites known physical and cyberattacks on ground-infrastructure, space situational awareness sensors that can monitor and target satellites and attempts at jamming navigation and communication satellites.
- Directed energy weapons that can blind imagery satellites, anti-satellite weapons (ASAT) missiles that can destroy low earth orbit (LEO) satellites and create dangerous debris, and orbital weapons that can damage or tamper with satellites either are in development or have been deployed.
- Cyber attackers have long been targeting satellites, and the disruption of satellite data is an example. Threat actors continue to fine-tune their tradecraft to disrupt ground control stations, jam or spoof satellite communication links, deliver malware into satellite control systems, and use AI to find new attack patterns that will go undetected.
- Credit: https://venturebeat.com/security/building-more-cyber-resilient-satellites-begins-with-a-strong-network/

Hack-A-Sat Competition

Hack-A-Sat: A Real-world Testbed

- Introduction: Annual event by US Space Force at DEF CON in Las Vegas, challenging hackers to find satellite vulnerabilities.
- Purpose: Identify and address satellite system vulnerabilities and recognize top cybersecurity talents.
- Real-World Emphasis: Simulates actual satellite environments, highlighting the importance of securing space data and systems in the face of increasing cyber threats.

Team Krautsat’s Insights:

RISC-V Smash Baby Challenge:

- **Description:**
  - Provided: RISC-V-32 binary.
  - Hint: Potential stack buffer overflow.
  - Hosting: QEMU (suggesting executable stack).
- **Analysis:**
  - Tools: Ghidra for static analysis.
  - Observations: Small C program, flag retrieval from the FLAG environment variable, and specific input requirements ("ACEG").
- **Solution Approach:**
  - Exploit buffer overflow to manipulate program's execution.
  - Likely tools: Ghidra (static), dynamic analysis tools.

Team Poland Can Into Space's Insights

Objective: Decode a WAV file containing digital transmission.

Approach:

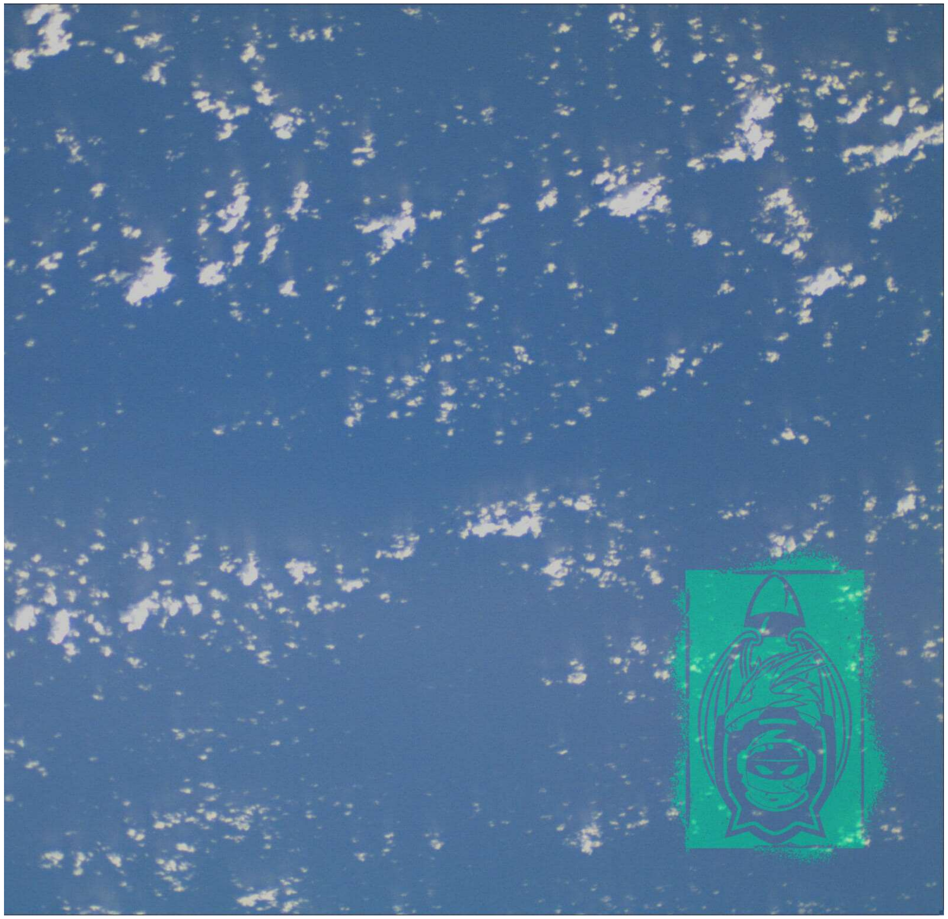
- Used GNURadio for demodulation and decoding.
- Shifted signal to complex domain using hilbert transform.
- Demodulated BSPK signal using symbol sync, phase sync, and constellation decoder.
- Decoded packets to obtain the flag.

Leavenworth Street Challenge:

Objective: Navigate a maze.

Approach:

- Analyzed a provided Docker image with Deno and an executable.
- Identified a maze structure and an error indicating a missing module.
- Realized the server expects a solver to be uploaded.
- Aimed to reverse-engineer the provided executable for further insights.



Expert Insights – Competitor on Hack-A-Sat : Competitor’s Perspective

Consulting Cyber Architect's Perspective on Hack-A-Sat

Hack-A-Sat Objective: Highlighted that genuine security isn't just about obscurity or difficulty in access. Satellites, like computers, face similar security challenges.

- **Trend:** As space access becomes more affordable, satellite security challenges expand rapidly.
- **Interdisciplinary Collaboration:** SPARTA is a starting point, but collaboration from the start is key. As more entities venture into space, the attack surface grows. Success lies in merging engineering disciplines early in system designs.

Conclusion : Satellite Cybersecurity in the Digital Age

- **AI-Enabled Satellite Cybersecurity:** Emphasized the transformative potential of AI in enhancing real-time satellite cybersecurity.
- **Recent Satellite Cyber Incidents:** Highlighted the increasing militarization of space and the strategic targeting of satellites in cyber warfare.
- **Hack-A-Sat Competition:**
    - Teams like "Poland Can Into Space" and "Krautsat" showcased innovative solutions to complex challenges.
    - Emphasized the importance of interdisciplinary collaboration for future satellite security.
- **Athena Detect:** Introduced as an AI-driven solution integrating SIEM, SOAR, and the SPARTA framework for advanced satellite security.
- **Consulting Cyber Architect's Perspective:** Stressed the significance of Hack-A-Sat and the need for early and frequent interdisciplinary collaboration.

Q&A Session

- "Thank you for your attention. I'm now open to any questions, discussions, or feedback you may have."