THE AEROSPACE CORPORATION

Eirene Sceptre Cyber Defense Services

Nick Cohen
Cyber Defense Solutions Department

26 February 2019

© 2019 The Aerospace Corporation

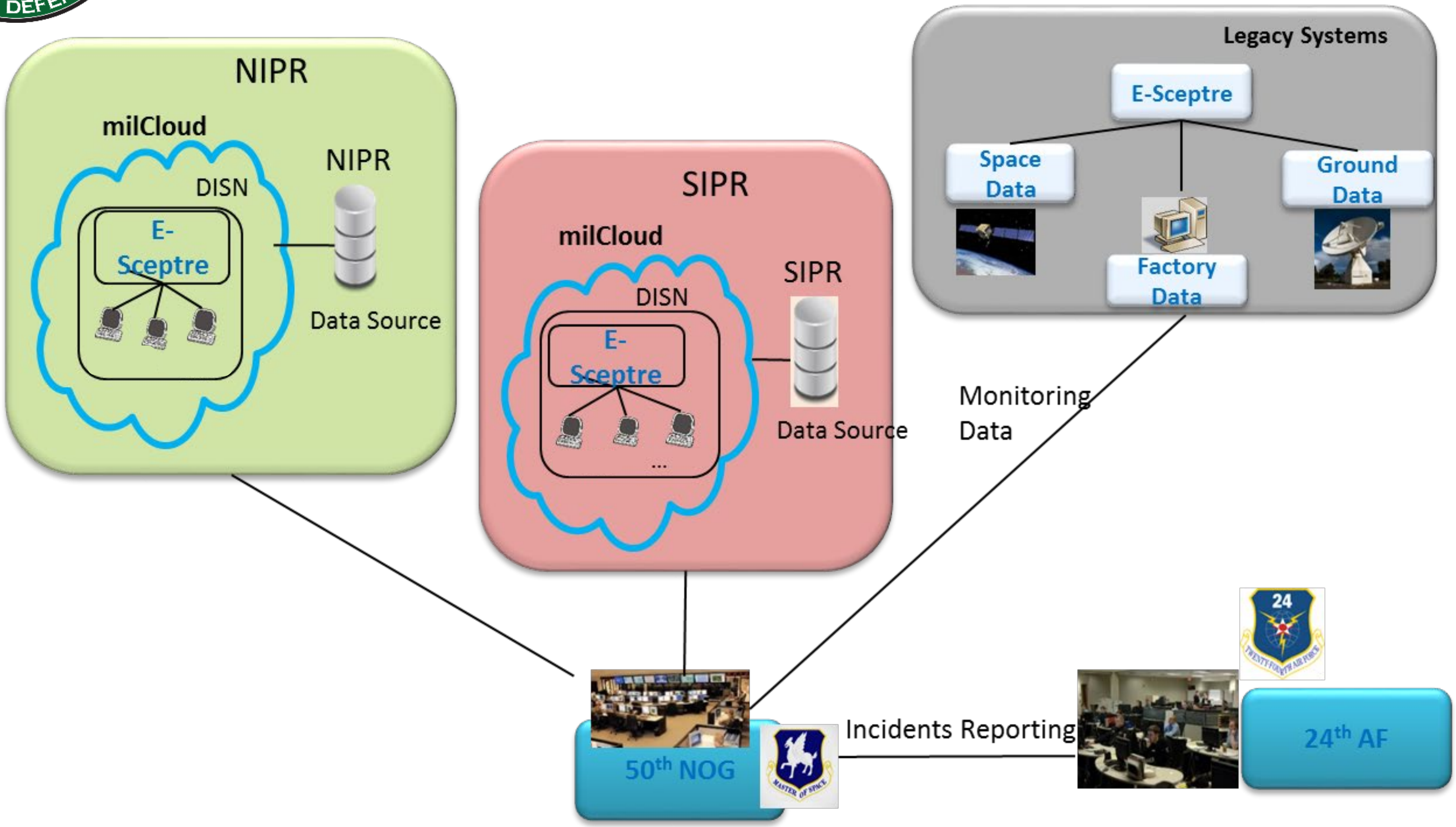
Overview

- Eirene Sceptre (E-Sceptre) Overview
- E-Sceptre Mission Benefits
- E-Sceptre Architecture and Capabilities

SMC Cyber Defense Need and Approach

- **DoD Joint Information Environment and Air Force level monitoring do not address space-specific data e.g. TT&C, health and status, commands**
- Aerospace developed a tool suite called "Eirene Sceptre" for space systems
  - *Knowledge of space, ground and launch systems and data*
    - Implement domain specific data analysis and intelligence
    - Develop threat models for space data
    - Develop early indication and warning on space data footprint and signatures
    - Cyber anomaly resolution for space systems
  - *Flexibility in deployment models, can adapt to mission requirements*
    - Cloud deployment
    - Local deployment for legacy systems
- Address evolving threats to space systems and improve cyber resilience
  - *Implement space-specific cyber defense on top of CDSP Tier II providers*
- Built-in redundancy and scalability to overlay with AF and DoD security tools
  - *When deployed on the cloud*

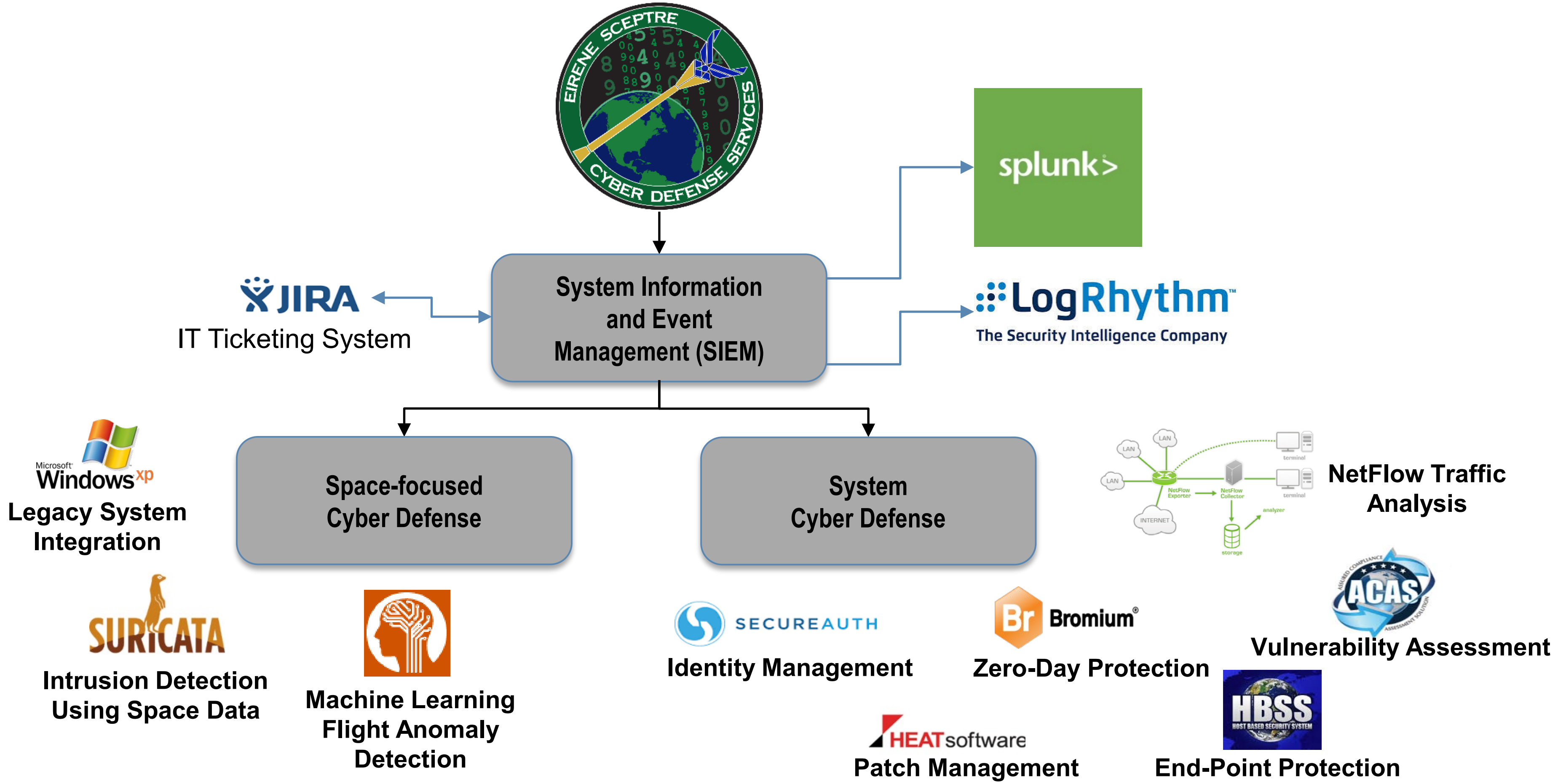
Eirene Sceptre OV-1



Adaptable to mission requirements
Redundancy and scalability built in to the cloud

Eirene Sceptre Cyber Security Services Overview

Cyber Security Services provide a service stack and expertise in space systems to bridge the gap of Cyber Security Service Provider (CSSP) & space weapon systems.



System Information and Event Management (SIEM)

IT Ticketing System

Space-focused Cyber Defense

System Cyber Defense

Legacy System Integration

NetFlow Traffic Analysis

Intrusion Detection Using Space Data

Machine Learning Flight Anomaly Detection

Identity Management

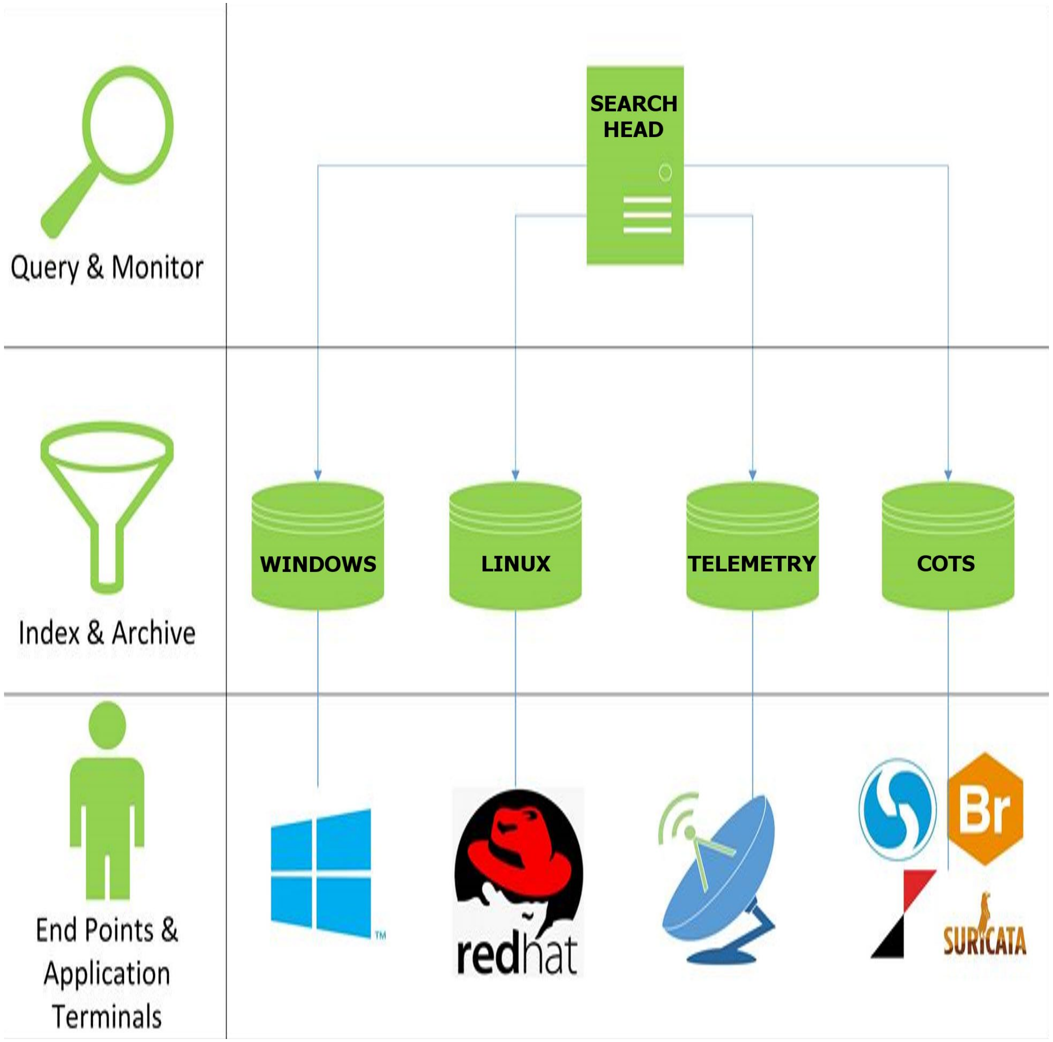
Zero-Day Protection

Vulnerability Assessment

Patch Management

End-Point Protection

Eirene Sceptre – Splunk Architecture Overview

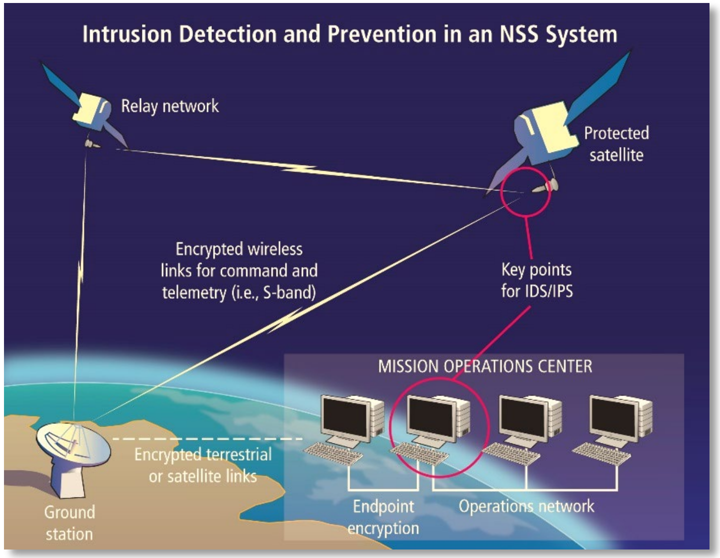


Accomplishments

- Integrated and monitoring two mission applications, both received Interim Approval to Test (IATT)
- Participated in cyber experiments
- Demonstrations for several Air Force space programs
- Developed space-focused capabilities:
  - *Tailored monitoring toolkits to scan mission data (e.g. telemetry, health & status, commanding string) for cyber analysis and intelligence*
  - *Developed early indication and warning on intruders using space data*
  - *Developing Satellite-as-a-Sensor, monitoring unexpected anomalies and early indications*

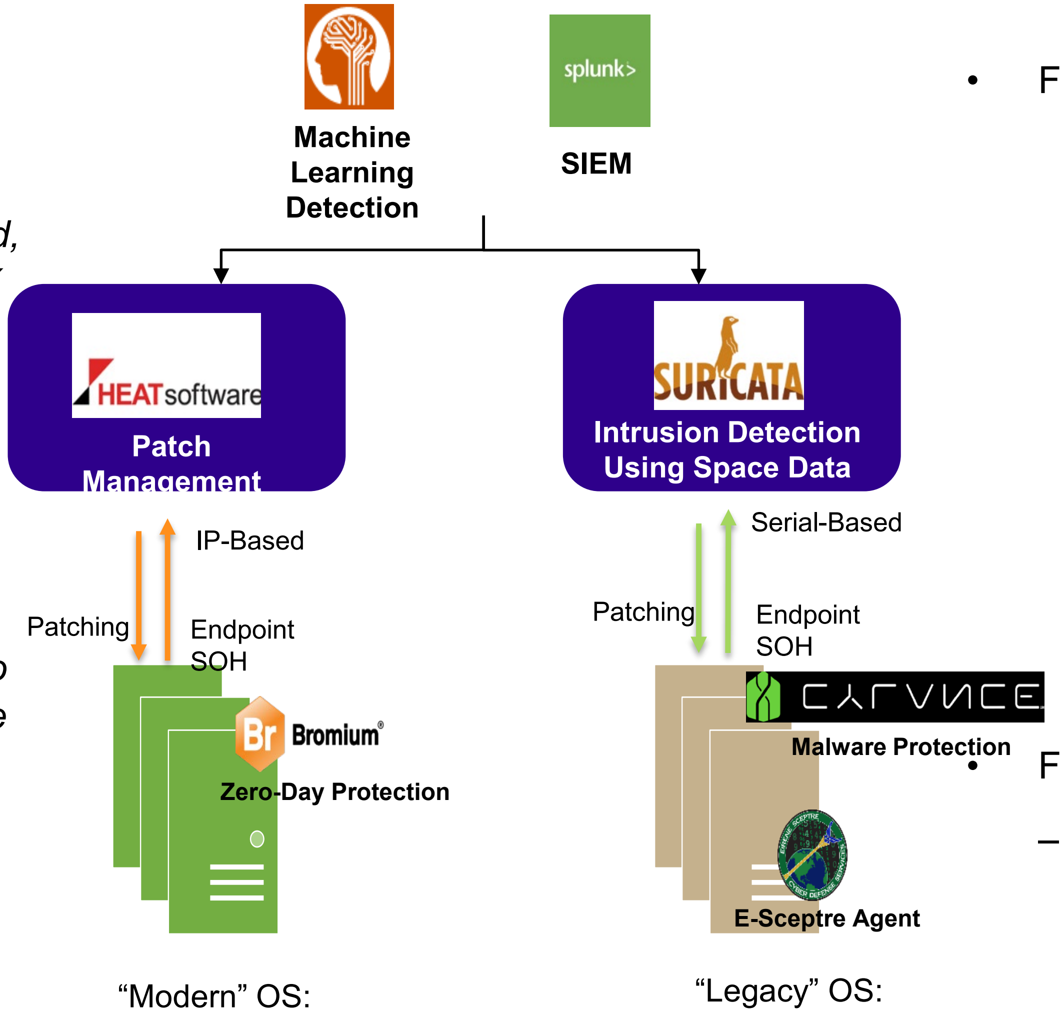
Intrusion Detection in Space Systems

- Limited characterizations of the threats, vulnerabilities and mitigations for the space segment and the space to ground interfaces
- Continuous monitoring for intrusions can alert operators to attacks in real-time
- Extensive research and experience using IDSs and IPSs in ground networks, but require adaptation to work with space systems and specialized protocols
- Sceptre IDS uses detection methods from existing IDSs such as Suricata to detect cyber attacks and feed alerts through Eirene Sceptre


Intrusion Detection and Prevention in an NSS System
Relay network
Protected satellite
Encrypted wireless links for command and telemetry (i.e., S-band)
Key points for IDS/IPS
MISSION OPERATIONS CENTER
Encrypted terrestrial or satellite links
Ground station
Endpoint encryption
Operations network

Legacy System Integration

- For “modernized” endpoints:
  - *Modernized: Win XP onward, Linux, IBM AIX or Solaris*
  - *Use Heat (or ARAD/Tanium) to scan and patch the endpoints*
  - *Use Cylance to detect malware patterns **



- For “Legacy” Endpoints:
  - *Legacy: DOS to Win 95, 98*
  - *Use Eirene Sceptre light-weight deployable agents to collect system SOH, processes information, and vulnerabilities*
  - *Use Cylance to detect malware patterns **
- For serial interfaces:
  - *Use Eirene Sceptre serial taps to collect system and network information*

Space Flight Anomaly Detection and Analysis

- State-of-health anomalies
- Command sequence anomalies
- Malware with unknown signature
- Abnormal data trends

Data-Driven Detection

- Satellite state-of-health data and sensor telemetry provide insight into satellite behavior
  - *Is the behavior normal or abnormal?*

- Data-driven vs. Rules-based detection
  - *Detect and predict unexpected behavior*
  - *Identify correlations between many variables*
  - *Adapt to dynamic situations*

- Utilize both data-driven and rules-based approaches to capture a variety of anomalies

Team

Eirene Sceptre Technical Team:

- Aerospace Cyber Engineering and Protection
  - Scott Niebuhr
  - Kris Horton
  - Brenda Taylor
  - Michelle Yohannes

- Aerospace Engineering Technology Group
  - Andre Chen
  - Nick Cohen
  - Idriys Harris
  - Eric Frechette
  - Mike Williams
  - Denny Ly
  - Don Wonders
  - Pablo Settecase
  - Dale Schroeder
  - Jerry Lien
  - Chibueze Ogamba
  - Dan Balderston
  - Alexandria Garland
  - Jackie Andrade

Acronyms

AF	Air Force
AFNET	Air Force Network
AFSCN	AF Satellite Control Network
AMPS	Automated Meteorological Processing System
AS&W	attack sensing & warning
CDSP	Cyber Defense Services Provider
CONOPS	Concept of Operations
CM	Continuous monitoring
CSRIT	Cyber Security Review & Integration Team
CSSP	Cyber Security Service Provider
DCO	Defensive Cyberspace Operations
DISA	Defense Information Systems Agency
DMZ	Demilitarized Zone
DoD	Department of Defense
DoDAF	DoD Architecture Framework
DoDIN	DoD Information Network
ELS	Enterprise Level Security
ESD	Electronic Schedule Dissemination
FedRAMP	Federal Risk and Management Program
GPS	Global Positioning System
IDS/IPS	Intrusion Detection/Prevention System
JIE	Joint Information Environment
JMS	JSpOC Mission System
JSpOC	Joint Space Operations Center
KPP	Key Performance Parameter
KSA	Key System Attribute
LADO	Launch, Anomaly, and Disposal Operations
MSO	Managed Services Office
NOMS	Network-Independent Open Source Messaging Service
NOSCs	Network operations and security centers
NS4R	Network Security SATCOM System Synchronization Roadmap
OPIR	Overhead Persistent Infrared
SBIRS	Space-Based Infrared System
SIEM	Security Information and Events Management
SMC	Space and Missile Systems Center
TT&C	Telemetry, Tracking, & Control
XUI	External User Interface
ULA	United Launch Alliance
UAM	User activity Monitoring