CyberC4:ALERT

Cyber Situational Awareness for Satellite Ground Networks

KRATOS | RT LOGIC

Overview

As satellite networks move toward end-to-end Internet Protocol (IP) environments, the attack surface for cyber threats is increasing. These new risks are placing mission operations and sensitive data at a heightened risk for compromise.

RT Logic's CyberC4:Alert is the first Security Information Event Management (SIEM) system specifically for satellite networks that provides network administrators and information security officers with real-time situational awareness and incident response.

CyberC4:Alert provides comprehensive situational awareness, continuously monitoring for threats by gathering cyber security event data from across the network. Its correlation engine with user-defined rules and policies prioritizes events by their severity, alerting users of system threats, performance issues, and compliance violations through a flexible drill-down dashboard.

Architecture

One important foundation for cybersecurity situational awareness is implementation of a SIEM that monitors and consolidates data from the independent security devices such as firewalls and IDSs into a single dashboard. CyberC4:Alert is the only SIEM with features specifically for satellite ground networks, such as:

- Automated real-time DIACAP compliance reporting
- Plug-ins for mission unique SATCOM equipment
- Central location for situational awareness

Real-Time Reporting for Complete Situational Awareness

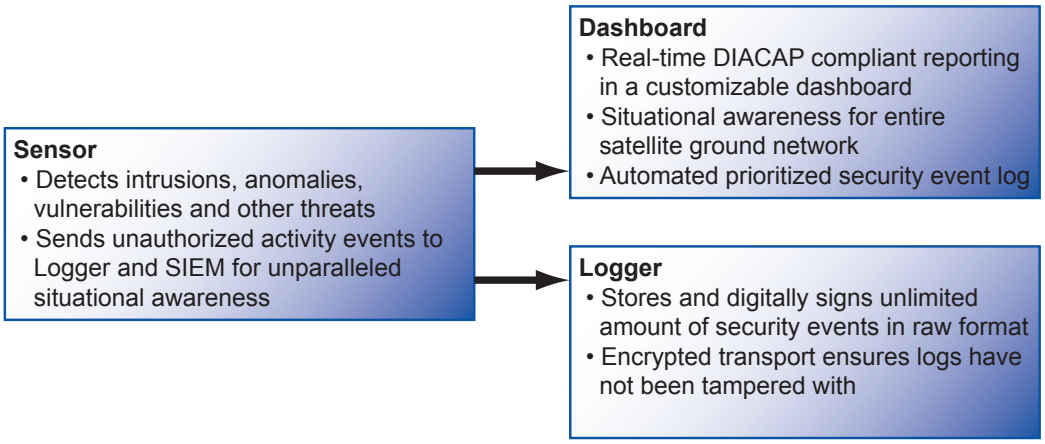
CyberC4:Alert is composed of three software modules, including Dashboard, Sensor, and Logger, which together collect, analyze, and report on security event data for immediate internal and external threat management, DIACAP compliance, and forensics.

Key Features

- Automated real-time DIACAP compliance reporting
- Plug-ins for mission unique SATCOM equipment
- Central location for situational awareness

Providing End-to-End Satellite Network

- Security
- Real-time event processing engine cross-correlates and prioritizes security and mission assurance events
- Automated vulnerability assessments and intrusion detection for risk management
- Forensically secure centralized logging
- Customizable dashboard with charts, graphs, and tables for superior situational awareness



Network Protection Features

- Wireless, network, and host intrusion detection
- Plugins for RT Logic and SATCOM mission unique equipment
- User-customizable Rules and Policy library developed specifically for SATCOM/SCIF environments
- Dashboard widgets for tracking mission assurance events
- Analytic tools for forensic investigation
- Digitally signed and time-stamped log events
- Network discovery, host enumeration, and asset management functions
- Advanced operational and investigative SEIM Analytics
- Out-of-the-box and customizable DIACAP compliance reporting
- Wireless, host and network IDS/IPS
- SAN/NAS Interoperability provides unlimited storage scalability
- Data feed for continuous updates (also available on quarterly DVD)