IOT Security: Peraton's PCAR – An Automated Cyber Resilience Platform PCAR

Jeff Berlet
Senior Technology Director, Cyber Mission Sector
Peraton

On DoD networks, and on the Internet at large, there are an increasing number of non-traditional endpoints that require the ability to phone home for purposes like cloud storage of data and centralized management. DISA is investigating how to improve security of these IoT devices by better classifying IoT network traffic so that new security policies can be developed, and how to secure these devices against attack, both at the network level and on the device itself.

Solution - Peraton's Platform Cyber Assessment Resiliency (PCAR) is a platform to assess and enhance operational resilience for national mission platforms and critical infrastructure, including operational technology (OT) and IoT systems. PCAR anticipates, recovers from, and adapts to adverse conditions, stresses, attacks, or compromise.

The PCAR platform includes several next generation cyber capabilities including:

- CyberCI – Cyber Critical Infrastructure
- CyberMP – Cyber Mission Platform
- DCRA – Deep Cyber Resiliency Assessment
- CyberVAN – Cyber Virtual Assured Network
- C-SCRM – Cyber Supply Chain Risk Mitigation
- ThreatBoard – Threat Management Platform

PCAR implements a modular approach to deliver automated proactive cyber risk assessment and active cyber defense services. PCAR leverages the best of breed Hybrid Cloud, Data Lake, Data Streaming, Data Fabric and Heuristic Behavior Analysis technologies.

PCAR utilizes Peraton's digital-twin simulation software called CyberVAN. CyberVAN performs high-fidelity network terrestrial and satellite constellation modeling for real-time mission systems analysis. CyberVAN overlays real-world space-based cyberattack and countermeasure scenarios for evaluation.

PCAR offers Deep Cyber Resiliency Assessment (DCRA) to analyze how national mission platforms can be attacked. DCRA conducts assessments based on D4M adversary goals – Deny, Degrade, Disrupt, Destroy or Manipulate. DCRA performs advanced vulnerability analysis, penetration testing and remediation.

PCAR provides CyberCI and CyberMP solutions using Software Defined Network sensors for advanced continuous monitoring and insightful situational awareness of the nation's critical infrastructure and mission platform environments.

PCAR ingests network telemetry, detects notable events, performs edge and cloud analytics, generates alerts and insights via cognitive analytics.

PCAR uses contextual Heuristic Behavior Analysis for next generation threat detection, hunting, and classification using Peraton's ThreatBoard solution. We use clustering, classification, and deep learning techniques to detect unknown threats.

PCAR digitizes well-defined Security Operations Center (SOC) processes and procedures to speed incident response and risk mitigation.

PCAR includes Cyber Supply Chain Risk Management (C-SCRM) capabilities to ensure all software, hardware, subcomponents, and materials are secure, resilient, and cyber security compliant continuously.

In summary, PCAR offers customers end-to-end cybersecurity services to build cyber resilience for both IT and OT systems, networks, and data needed to maintain mission assurance. Keywords: Critical Infrastructure, Mission Platform, Hybrid Cloud, Data Lake, Data Streaming, Data Fabric, Heuristic Behavior Anomaly, Threat Hunting, Internet of Things, Operational Technology, Security Operations Center, Digital Twin, IT, OT, IoT, and SOC.