CYBERSECURITY

CYBER THREAT HUNTING WITH ADVANCED ANALYTICS

Combining the use of threat intelligence, analytics, and automated tools with human smarts.

Raytheon's global experience with critical cybersecurity efforts has allowed us to develop a deep understanding of the serious cyber threats and their potential impacts to mission-critical systems and commercial interests. We understand our customers' need for a highly scalable system due to ever-growing business demands for enterprise connectivity of various channels resulting in proliferation of data. We use advanced analytics to identify threats that have the potential to disrupt the customer environment and negatively impact their mission and business. In addition to understanding the need to deliver advanced cybersecurity analytic capabilities, Raytheon also recognizes the importance of performing comprehensive training. Training can provide expertise in the tactics, techniques, and procedures (TTPs) necessary for analysts to become skilled in cyber threat hunting (CTH) and the ability to adapt to the ever-changing threat landscape.

Benefits

- Proactive threat hunting to minimize impact to the enterprise
- Real-time ingestion of application and system logs and network data
- Search against commercial and open source cybersecurity feeds
- Correlation and alerting
- Security information and event management (SIEM) and enterprise asset integration
- Flexible intelligence ingestion
- Centralized alerts console
- Quicker turnaround on threat hunting
- Entity-based profiling to detect anomalies
- Advanced statistical analysis and machine learning capabilities

The Problem

In today's dynamic world of global business, securing and earning the trust of customers is critical to any successful business. Keeping business data protected against cyber threats is one of the biggest challenges facing both businesses and governments alike. Increasingly sophisticated network attacks and cybersecurity threats make it ever more difficult to sustain business performance and growth.

Currently, protecting enterprise networks relies on a mix of disparate tools from a variety of vendors. As a result, CTH processes for monitoring, detection, and prevention involve complex system integration and maintenance. Security practitioners struggle to learn too many tools, deal with repetitive mundane tasks, rely on static rules, sift through too many false positive alerts, and have no centralized view of data. Maintaining expensive tools, finding the right talent, managing an ever-growing list of users and assets, and thwarting increasingly sophisticated attacks put a strain on enterprise security programs.

Raytheon

CYBER THREAT HUNTING

The Solution

Raytheon's approach to CTH combines the right tools and training to help customers proactively identify non-obvious signs of adversary activity affecting the enterprise. Cyber threat hunters develop threat models based on threat intelligence and knowledge of security data available within the advanced analytics platform. These threat models are presented to cybersecurity analysts in the form of custom alerts, reports, dashboards, and detection signatures which aid in the monitoring and investigation of security events.

Tools

The heart of Raytheon's CTH with Advanced Analytics solution is supported by a real-time framework that integrates a variety of open source technologies into a centralized tool for security monitoring, detection, and prevention, coupled with machine learning algorithms to detect anomalies. The solution is a feature-based extraction mechanism that can generate a profile describing the behavior of an entity. Entity-based profiles define what normal behavior looks like and then models can be built to help identify anomalous behavior. The solution is highly scalable, modular, extensible, and configurable, and is seamlessly integrated with the Hadoop ecosystem, which can process millions of events per second and store petabytes (PBs) of data.

Training

Raytheon's knowledge transfer plan and training follows a ground-up approach. Raytheon coordinates vendor training of increasing complexity, from introductory to more advanced levels. Trainees start with basic certifications, move to system tool and system/network administrative training and then progress to hands-on CTH maintenance and operations training, supplemented with knowledge transfer programs led by Raytheon's CTH experts.

Full Capabilities and Services

Raytheon offers full capabilities and services to support our CTH platforms through the provision of on-premise network security and system infrastructure, operations support tools, and processes.

Raytheon network design principles incorporate industry best practices for network architecture, focusing on security, resiliency and overall performance. We use a layered approach consisting of data diodes, firewalls and endpoint protection devices. The network design enhances availability through server redundancy via VMware hosts, to provide high availability and shared resources to help prevent single points of failure within the infrastructure network services and applications.

We also provide an operational support network which enhances the availability, collaboration, and operational security of the CTH mission using the servers, infrastructure, and open source tools and technologies, as well as commercial-off-the-shelf products. As an example, Raytheon's solution provides tools such as RSA servers to administer authentication policies; a request tracker for incident response ticketing; SolarWinds for monitoring and managing the network and infrastructure; and Linux, VMware and Windows servers. Our use of virtualized components for operations reduces the risk of CTH interruption and increases the overall CTH capability.

Raytheon
Intelligence, Information and Services
22260 Pacific Blvd.
Dulles, Virginia
20166 USA

raytheon.com

Raytheon.com
@Raytheon
Raytheon
@raytheoncompany
Raytheon

Raytheon