Evolving Continuous Monitoring to Cyber Situational Awareness

George Romas
13600 EDS Drive
Herndon, VA 20171
UNITED STATES

george.romas@hpe.com

ABSTRACT

Hewlett Packard Enterprise (HPE) has been developing a Continuous Monitoring capability for 3 years, integrating over 60 HPE and partner products to satisfy US Department of Homeland Security (DHS) and the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) requirements. The result is a solution that leverages customer product investments and can fill gaps with pre-integrated capabilities, focused on normalizing information at the data layer. We are able to easily extend this solution platform with functions that satisfy Cyber Defense Situational Awareness requirements, providing incident management capabilities that bridge the cyber and physical worlds.

1.0 RISING CYBER EVENTS

Hardly a week goes by without news of a significant cyber event that results in the loss of highly personal, financial, medical, or business-sensitive information. Frequently, these losses are attributed to flaws in the commercial software that powers our on-line world. The NIST RMF and the DHS' Continuous Diagnostics & Mitigation Program (CDM) were both established to assist public sector organizations in keeping up with, if not anticipating, some of the cyber threats that face those organizations that rely on the Internet.

Public sector organizations have embraced RMF to address these issues, using enterprise wide programs that continuously identify, prioritize, and document risks. The result is that an economical set of control measures (involving people, processes, and technology) can be selected to mitigate the risks to an acceptable level. This approach also begins the process of identifying the dependencies between assets and missions, executing incident response and remediation according to priorities, and generating an easily understood view of the overall security posture.

One of the direct benefits of the CDM program is dashboards that provide enterprise-wide views of the current status of basic security controls. If properly implemented and maintained, they reduce many of the common vulnerabilities Internet-facing technology creates. Hewlett Packard Enterprise (HPE) found a way to combine that information with mission asset information to create a more holistic view.

There are a number of challenges and obstacles to developing a solution that accomplishes the complex orchestration of capabilities needed. These include integrating a wide variety of products, evolving compliance-based processes to risk-based processes, associating cyber and physical assets to the mission space, and understanding the expanding volume of data.

2.0 MITIGATING THREATS

By focusing on data integration, we were able to integrate encryption technology that secures data in motion and data at rest. These functions, in turn, allowed us to more easily develop a shared services solution, focused on smaller agencies that may not have the technical resources and expertise to perform this work themselves. The intent is to "instrument" the endpoints, hosts, and local networks with "sensors." Thus securely sending that information to a shared service that will perform the more complex and compute-intensive aggregation, correlation, analysis, and risk scoring in a multitenant environment.

These capabilities form the basis of an open, flexible, and secure platform adhering to the principles of the RMF. When we reviewed the requirements for Cyber Defense Situational Awareness (CDSA), we realized that our extensive CDM integration work in our lab could be broadened to incorporate the products that would satisfy the full range of CDSA functions. We focused on four specific functions that bridge the current version of CDM to CDSA: incident response, courses of action (CoA), mission dependencies, and mission asset management.

The key innovation behind these four functions is relating cyber incidents and affected assets to specific missions and mission assets, for example, soldiers and equipment in the field. So, in a sample scenario, when an advanced persistent threat (APT) is detected, both a cyber incident response and mission incident response would be initiated. The APT should be remediated, but any related missions should be modified to protect people and equipment. The HPE solution provides the ability to manage by risk, respond to incidents, and apply courses of action to the mission space.

3.0 HEIGHTEN AWARENESS

A comprehensive cyber situational awareness (CSA) model is based upon analysis of millions of sensors, processing billions of files and web objects, and correlation of global network traffic flows against industry threat intelligence feeds and threat models. The results must be continuously shared within the organization, as well as with its external partners. The model must also extend to appropriate security metrics, security enforcement policies, controls and technologies, security management, operations workflow, and multi-level risk management reporting dashboards that can fuse analytics with mission dependencies.

HPE has quickly accomplished the transformation of our cybersecurity solution set because we have invested in performing the complex and difficult integration work, making it incredibly easy to plug in new technologies and functionality. We are able to do this by leveraging our world-class capabilities and proven experience in cybersecurity, enterprise service management, Big Data management, as well as analytics and risk management. We have leveraged the agile integration successes in the Center for Cybersecurity Innovation & Integration (C^2I^2) lab to rapidly begin CDM deployments to 6 US civilian agencies, well ahead of our competitors even though we were awarded the most recent task order. This methodology has also allowed us to quickly expand the functionality of our risk management solution, leading to development of CDSA capabilities for foreign public sector customers in the form of proofs-of-concept. The same process has influenced the development of Contextual Security Analytics and Mitigation (CSAM) capabilities for U.S. public sector customers in the form of proofs-of-concept. Through the convergence of these complementary solution sets, HPE is quickly developing an architecture that supports cyber situational awareness and mission assurance. By focusing on protecting your digital enterprise and empowering the data-driven organization, we are proving these advanced capabilities in our own labs, our customers' development environments, and our customers' production systems.

4.0 CASE STUDY #1

A large defense entity, NATO, developed a "use case" based set of scenarios, detailing various high, moderate, and lower priority situations. Each interested participant was asked to provide a detailed technical overview, describing what commercial off-the-shelf (COTS) technologies the participant could provide, and how those technologies would be integrated to address the specific sample scenarios.

Based on these presentations to the organization, HPE was one of only a small number of firms invited to provide a live capability demonstration of the proposed solution, initially using unclassified sample data provided by NATO. HPE was further "down selected" as one of two firms to undergo more rigorous testing and an initial implementation of the Cyber Defense and Situational Assessment solution at NATO's headquarter facilities, using classified data in a test environment.

5.0 CASE STUDY #2

The Continuous Diagnostics & Mitigation (CDM) program is a dynamic approach to fortifying the cybersecurity of government networks and systems. CDM provides federal departments and agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritizes these risks based upon potential impacts, and enables cybersecurity personnel to mitigate the most significant problems first. Congress established the CDM program to provide adequate, risk-based, and cost-effective cybersecurity and more efficiently allocate cybersecurity resources. The CDM program enables government entities to expand their continuous diagnostic capabilities by increasing their network sensor capacity, automating sensor collections, and prioritizing risk alerts based upon COTS tools, with robust terms for technical modernization as threats change.

HPE was awarded one of 17 blanket purchase agreements, which in turn, allowed us to win Task Order 2E to provide the HPE CDM Solution to the Department of Housing and Urban Development (HUD), Environmental Protection Agency (EPA), Small Business Administration (SBA), Department of Education (DoED), National Science Foundation (NSF), and the Nuclear Regulatory Commission (NRC). In addition, even though we were the last vendor awarded to deploy to medium / large agencies, we were the first to deliver full Phase 1 capabilities (hardware asset management, software asset management, configuration management, and vulnerability management) to one of our clients.

6.0 EVOLVING THE SOLUTION

As we mature our CDSA capabilities, our architectural roadmap includes a Big Data, analytic platform as the single authoritative data source. We are developing this platform as part of a separate offering—CSAM, which is built on state-of-the-art Big Data components:

- Open source: Hadoop, Kafka, Spark
- HPE products: Autonomy IDOL, Vertica

As we scale up CDSA data sources, our clients will gain unique insight on cyber events and how they relate to missions. Focusing on data and data integration simplifies the overall solution architecture. HPE continues to demonstrate its leadership in the cybersecurity space, not merely by providing technologies, but by providing innovative solutions that leverage our clients' current investments with our unique integration capabilities to better protect the enterprise.