Peraton

WHITEPAPER

CYBER DEFENSE SITUATIONAL AWARENESS

With the outbreak of ransomware and cyber-attacks against government agencies, financial institutions and national power grids, agencies must respond quickly and use their own system and infrastructure knowledge to be effective against these adversaries. In 2016, Mandiant performed analysis on the traditional approach to remediating security problems, and for the calendar year 2015, they found that the median number of days to correct a problem was 146, with a 46-day average breach response time. The daily cost of a breach was $21,155, with 47 percent of those breaches reported by a third party. From discovery to remediation, that's an average of $3 million per breach, not counting any recovery costs (e.g. identity protection for stolen personally identifiable information). Of course, this does not take into account breaches of which an agency remains unaware.

Why has there been little improvement at addressing this problem; that is, responding to security problems timely or preventing intrusions? Threats are coming in fast and furiously; a slow and steady response is no longer productive.

For the data collected by the many commercial off-the-shelf (COTS) sensors and scanners, there is no defined relationship or correlation between one piece of data and another, especially between different vendors, therefore overall cybersecurity situational awareness cannot be discerned. To further complicate the problem, security data is siloed, meaning that one group may perform vulnerability scanning, while another performs and maintains event monitoring. Operations personnel typically focus only on the data needed to perform their function, and vendors build their products to satisfy this narrow scope. This data is pushed up to leadership where one report may show that an event was triggered and remediated; however, that report has no awareness of additional vulnerabilities or misconfigurations that are prevalent on those same systems. This results in poor decision making due to a lack of understanding around data relationships and an absent view of the big picture. Furthermore, a failure to relate this data to agency mission, logistics functions or any data that is important to the customer and there could be catastrophic results.

PERATON'S ROAD TO CYBER DEFENSE SITUATIONAL AWARENESS

Peraton has a rich heritage with cyber defense situational awareness (CDSA), originating with the Defense Information Systems Agency's (DISA) Continuous Monitoring (CM) program. Originally, our team members were tasked to monitor custom-built tools for the Department of Defense (DOD) and return that information to a custom-built dashboard that then calculated the risk posture for the environment. Then in 2015, a company which is now part of Peraton won Phase 1 of the Continuous Diagnostics and Mitigation (CDM) program for the Department of Homeland Security (DHS) Group E (medium and large civilian) agencies. The requirements, while similar to DISA's CM program, were more focused on integrating COTS products to provide much of the same data to a risk management dashboard with risk calculated every 72 hours. The notional solution architecture is shown in Figure 1 from DHS. With this program, we were the first to achieve Operational Readiness Review (ORR) approval amongst five other CDM competitors working for DHS. The company passed 34 gate reviews with DHS the first time through and was the first integrator to have all of our six civilian agencies conducting bi-directional communication and reporting with the DHS (higher level) federal dashboard.

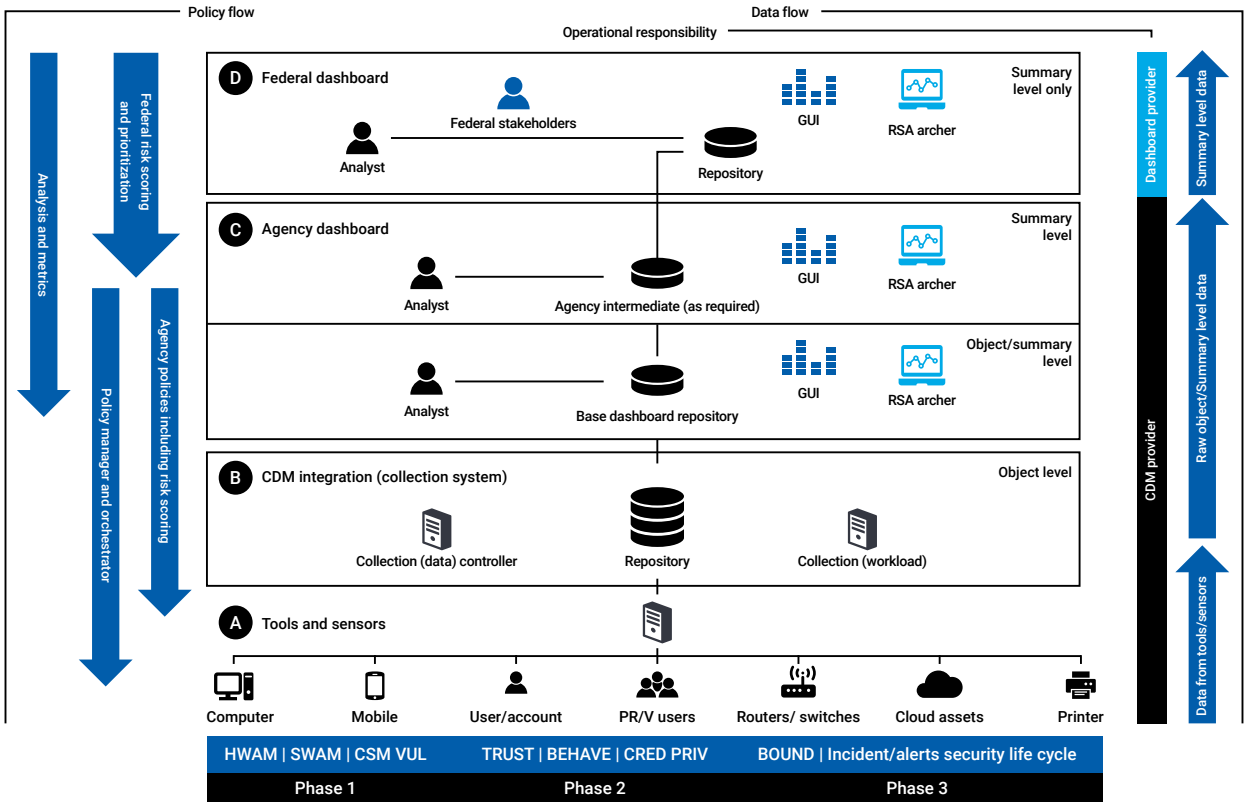

Figure 1: IDHS CDM architecture

We took these successes at DHS and applied them to the security and enterprise service management product integration problems most government agencies are facing today. Our architecture allowed us to extend our CDM solution to incorporate and satisfy CDSA requirements. Our integration platform facilitates added functionality and data sources. We correlated and mapped that data into relationships, building a model that operates in real world environments to display the big picture for a customer. We then made sure that this solution would be non-intrusive to the customer and would be flexible enough to operate in an established environment without a need to "rip and replace" existing organization's security tools that had already been procured and in use. More importantly, we understood from our CM heritage that the higher magnitude of informative data points coupled with a large number of diverse data points gives a higher accuracy in decision-making, providing a quicker turn around with actionable intelligence to reach situational awareness. An informative data point could be a threat, event, vulnerability or security incident on an asset. The magnitude of informative data points is important to note, and the entire environment should be scanned. Conversely, the number of diverse data points is also important. Having a variety of security or business information to pull from provides leadership accuracy in decision-making. See Figure 2 for additional details.

In May of 2015, the NATO Communication and Information Agency (NCIA) had released the Multi-National Cyber Defense Capability Development (MN CD2) Request for Information (RFI). This RFI's technology request aligned with our CDSA program features and road map. This RFI required that the company meet various functional requirements through several gate reviews, incorporate display functionality in a single pane of glass and install the solution in a secret environment for a demonstration to senior command staff from all 29 NATO member nations. Our solution was selected out of 40 other competitors and met more requirements than any other vendor solution. In addition, the demonstration solution was installed in NATO's secret environment in only three weeks' time.

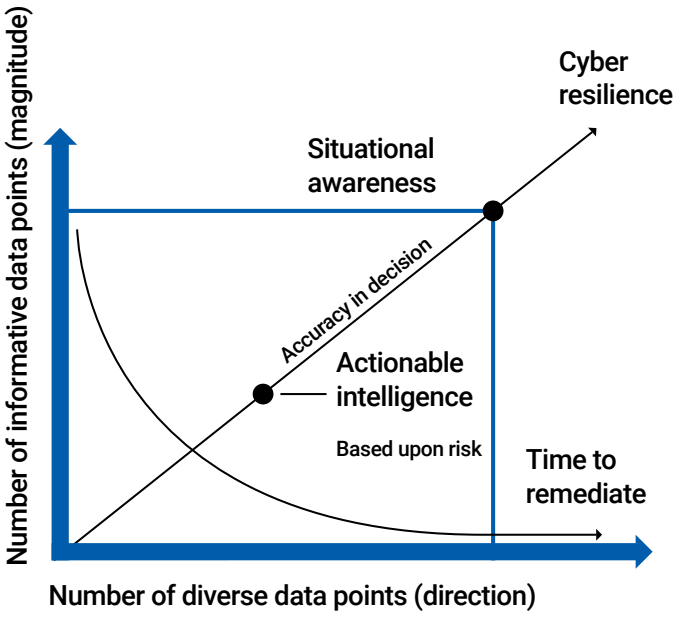

Figure 2: Informative data points vs. diverse data points

WHAT IS CYBER DEFENSE SITUATIONAL AWARENESS?

Our initial implementation of CDSA takes in data from more than 30 different data feeds from three different transport mechanisms. It augments a department or agency environment, displaying data on a geographical map or calculated in terms of risk posture for specific missions and the entire environment. CDSA relates data for threats, events, incidents, vulnerabilities, misconfigurations, hardware, software, mission data, organization hierarchy, blacklists and users. The CDSA platform has the ability to add other data inputs as needed. A key innovation is CDSA's capability to relate asset data directly to a mission. By relating individual hardware and software assets to mission services and mission applications, we are able to both calculate mission risk and the impact of cyber events on specific missions. The outputs are displayed in custom views and standardized reports, as well as threshold triggers, questionnaires and calculated courses of action. The end result is a big picture view of cyber resilience based on mission risk, criticality and priority.

CDSA ARCHITECTURE

We have taken all of our cybersecurity experience from the DISA and CDM programs and applied them to an architecture that can be federated and scalable, both horizontally and vertically. This is made possible by our data- and requirements-centric approach. Peraton spends significant effort up front to analyze customer requirements, determine what data and information is needed to satisfy those requirements, develop an appropriate canonical data model and determine which products / tools / sensors can supply the appropriate data.

On the next page is an example architecture for a typical customer. On the left is shown two of our application program interface (API) ingest tools. Currently, CDSA can support Representational State Transfer (REST) or Simple Object Access Protocol (SOAP) API ingests. Certificates and tokens are supported for improved security. Many products CDSA supports utilize a secure REST integration. Others support file transfers for Extract Transform and Load (ETL) functions (shown along the bottom). Peraton's CDSA solution supports more than 40 different file ingest variations for input into the solution. File ingests are secure;—if a file is placed on a share, our solution monitors that share and processes the file immediately upon arrival, so that sensitive security data is not left exposed. We also support the inclusion of encrypting tools such as Thales Vormetric to transparently encrypt all types of data stores.

Enterprise Service Bus

The Enterprise Service Bus (ESB) is at the center of the CDSA solution. It was chosen for its ability to loosely couple the data feeds from the scanners and sensors at the beginning of the tool chain with the dashboard displays at the top of the chain.

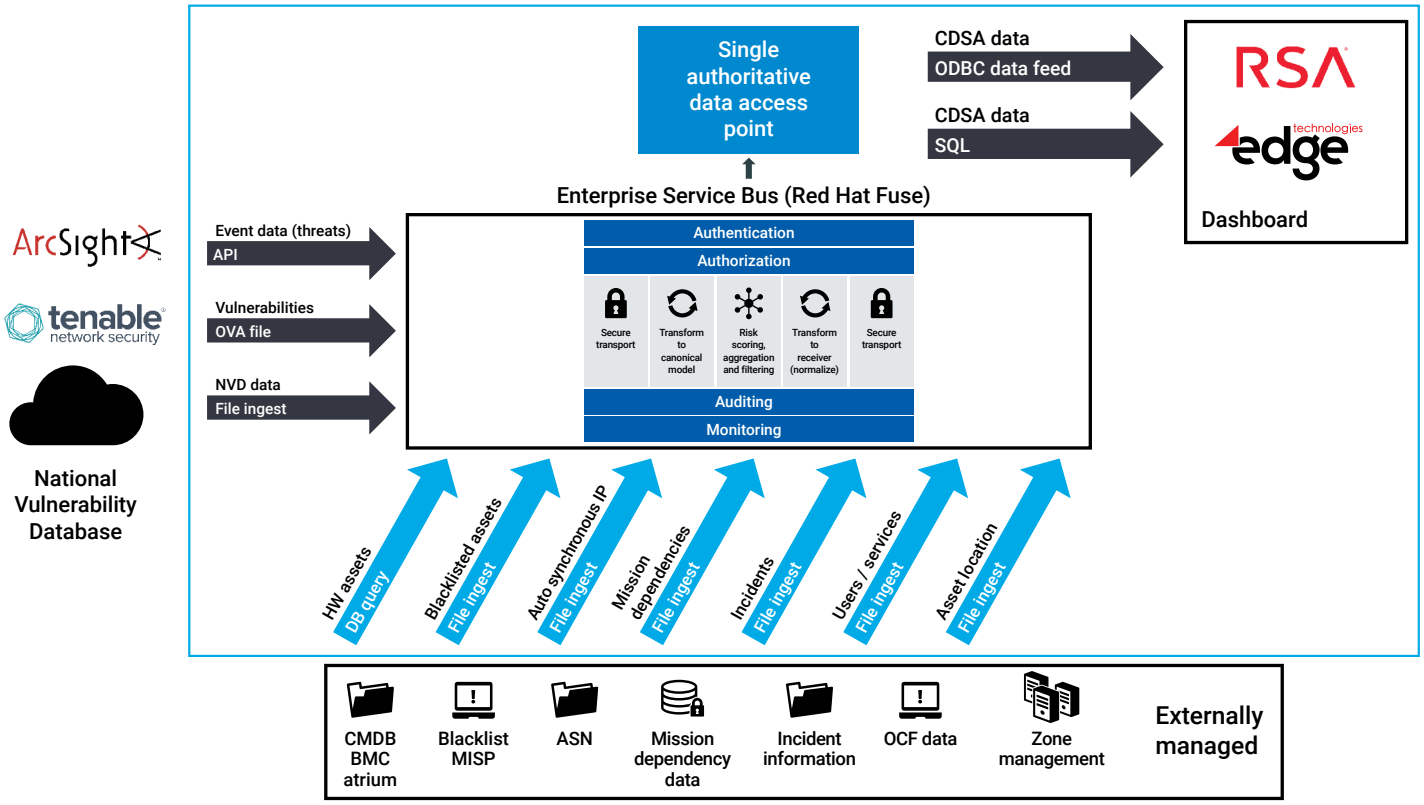

Figure 3: Notional CDSA architecture

If a scanner vendor changes the format of their data feed, there is no need to wait months for a new version of the dashboards to support it. Simply reconfigure the XML schema using our configurator tool and the ingests will be back up and running as they were prior to the vendor change. In our enhanced ESB, Peraton has incorporated significant innovation for CDSA. Some of our Intellectual Property is based on the security canonical model, normalization process and code, risk scoring and aggregation, logging optimization, scalability, and the rapid deployment tool (RDT).

ESB canonical model

Security content is similar throughout a typical infrastructure. A canonical model was created to support data ingestion of security and enterprise service management data. This canonical model is in use today and highly leveraged throughout customer organizations. The canonical model allows CDSA to re-use its security design pattern for different data formats. It also reduces costs and standardizes interfaces when integrating scanners and sensor systems. Ultimately this allows the interface to change quickly to adapt to new versions or tool enhancements. For example, if a scanner moves to version 10.X and "breaks" the REST API interface, the CDSA solution can modify its interface quickly to adapt or switch to a file interface to keep the dashboard up-to-date with its current risk posture, alleviating the customer from waiting months for the scanner sensor or the dashboard to adapt to this new format. Additionally, this allows Peraton to leverage a customer's existing investment in tools and products. For example, CDSA works equally as well with any of the current market leading endpoint security products.

Data transport

CDSA supports three main types of machine-to-machine data transport: web API through SOAP and REST, database query through MS SQL and Oracle, and file transfer by ingesting text, comma separated variable (CSV), JavaScript object notation (JSON), common event format (CEF), hypertext transfer markup language (HTML), and extensible markup language (XML). CDSA can process many standards such as the National Institute of Standards and Technology (NIST) Security Content Automation Protocol (SCAP), including Structure Threat Information eXpression (STIX), Trusted Automated eXchange of Indicator Information (TAXII), Common Vulnerabilities and Exposures (CVE), Common Configuration Enumeration (CCE), Common Weakness Enumeration (CWE) and DISA Security Technical Implementation Guide (STIG) Rule IDs. National Vulnerability Database (NVD) standards data is ingested regularly to complement current scanner results. CDSA can work in an online unclassified environment as well as in a classified off-line mode. Configuring connectors is easy to ingest new or modified data formats. For our NATO MN CD2 contract, CDSA was chosen for its capability to quickly adapt to changing data ingests as well as its ease of connection to legacy data types.

ESB normalization

CDSA normalizes all data at the ESB level. Data such as MAC addresses, IP addresses and date-time formats are all standardized for common usage throughout. MAC and IP addresses, along with other technical input data, are standardized to handle different identifiers from tool ingests. For example, a MAC address may use a hyphen instead of the

more common colon. The ESB will modify this to consistently use a colon. For language data, the ESB will utilize the language pack on the server to determine its format. This ensures that the country CDSA is operating in will, for example, display date and time in that country's native format.

Risk scoring and aggregation

By ingesting and managing data in a lightweight canonical form, CDSA can perform additional high-level functions like risk scoring, aggregation and filtering. CDSA can apply a weight or risk identifier to important endpoints that need to receive special attention when they are displayed on the dashboard. Hosts, or even a full enclave, can receive additional identifiers / flags that inform the CDSA user that severity implication is higher for these data points, gaining them additional attention at all levels of data usage beyond the aggregate layer.

Logging

With secure data transport, there must be a secure audit or logging capability to record data transport details, determine final state of the transported data, and understand the data itself. These characteristics enable availability of the information for audit or examination at a later date. The security aspect of logging is very important, as all sensitive log information must be protected at rest; otherwise, this information poses a significant vulnerability if compromised. CDSA incorporates the use of tools such as Thales Vormetric to protect data at rest. Any data that is written to a file store is encrypted transparently, and the system only allows access to those personnel or services authorized. The CDSA solution also utilizes data in motion protection through SSL (i.e., TLS).

Scalability

An ESB is a scalable method for data transport, adding efficiency and performance to enterprise communications. By making an ESB the core of the CDSA architecture, our solution inherits that same scalability and flexibility. CDSA can scale both horizontally and vertically to satisfy the most complex federated environments. That means the core aggregate ingest layer (layer B from Figure 1) can have multiple ESBs acting as ingest or export points to forward data, or multiple ESBs can exist to extract, transact and load data alongside other ESBs. Data can then be routed to where it is needed, balancing out compute resources by efficiently using processing power.

Unique asset identifier

Most security projects are built as siloes and are unable to share the security data. Peraton has a rich heritage of working with disparate data sources to find the meaningful relationships and build a big picture view of actionable situational awareness information. Data types are able to carry metadata that can be leveraged to build relationships. From Peraton's experience, building these relationships is critical to success. Our team has worked hard to develop these relationships based on real world experience. Some standardized models do not take real world techniques or processes into operations. The CDSA team has found that a significant amount of infrastructure security data relates to either an asset or a user (there are some complex variations to this). Due to this property, care must be taken to use a repeatable methodology when applying these relationships; otherwise, operations can halt due to transaction and/or database locks. The first step in the process is ensuring a unique asset exists. This is not an "easy button" approach; but a process that must be followed, starting with a solid algorithm, for uniquely identifying an asset. Peraton has focused on four pieces of information to build that unique asset identifier: fully qualified domain name (FQDN), host name, MAC Address and IP address. This process has given CDSA an approximate 99 percent success rate.

CDSA takes this quaternary information and applies available component data to the process. This process continually runs to uniquely identify the asset. The flow takes priority when all four fields of information are present, as well as when some combination of three of the four component fields are available. In that case, the process designates certain components that take precedence to uniquely identify and match the asset. This process can be altered when, for instance, a customer environment utilizes unique IP addressed assets. The use of guaranteed unique IP addressed assets is not the norm, but places CDSA in a strong position to utilize IPv6 when available in customer environments.

Data storage

Driving the effectiveness of CDSA, pertinent data is stored in a Single Authoritative Data Access Point (SADAP). This could be a data lake, data warehouse or a simple Microsoft SQL database. Having the data in a central repository supports archival, analytics, interactive and ad-hoc queries. The SADAP supports data pulls from both the eGRC dashboard as well as the Wnear-real time geographical dashboard. We have created innovative processes to ensure writing to the asset and user tables does not cause transaction locking or contention when inserting, updating or editing. It is also important to point out that CDSA supports big data through this SADAP approach. Analytics can be performed with COTS products on the CDSA data in the SADAP. Finally understanding that the SADAP will contain very sensitive organization data, it is fully secured leveraging the Thales Vormetric technology discussed earlier.

Cloud status

Currently CDSA supports cloud implementations. Peraton has placed the CDSA environment in a market leading cloud platform, which supports rapid deployment. CDSA can work in a full cloud deployment or hybrid model where scanners and sensors remain on premise for localized support. Deploying new CDSA base models can be performed in hours for a clean new cloud instance for customer environment support.

Compliance

It is important to note that the CDSA solution runs in a DISA STIG environment. Peraton applies Group Policy and various security controls to the solution environment to ensure it satisfies government compliance requirements. This also ensures that authorization and accreditation (A&A) can be obtained following an agency's or department's process. Peraton configures each solution to match the customer's environment and ensure proper compliance. The CDSA solution can also be used to check itself and can determine compliance gaps or improper configuration for specific controls prior to A&A. In many cases, these compliance results from our lab, can be supplied to the customer to expedite the process.

Dashboard display

The Peraton security team has chosen two dashboard products for the CDSA solution—a near-real-time geographical dashboard and an enterprise governance risk and compliance (eGRC) dashboard. Following Peraton's vendor impartial approach, these two dashboards were chosen as best of breed in their respective categories. CDSA can operate with different vendor dashboards, per the customer's choice. Currently we are working to create a single pane of glass view into each dashboard.

Near real time geographical view

This dashboard pulls data directly from the SADAP. It displays data in a high-resolution view that includes support for the following: graphing, tables, geographical charts, lists, heat maps, tree views and donut charts. The new suite of products for this dashboard is completely HTML 5 and uses third party controls, if desired, for geographical maps and displays. The ability to create new or customize existing displays is inherently built into this product; this gives the customers the flexibility to design their dashboard according to their specific requirements and policies. Customers are able to administratively configure views and dashboards to their liking.

Enterprise governance risk and compliance (eGRC) dashboard

The eGRC dashboard is one of the most popular Risk Management Framework (RMF) products available today. It allows an organization to view its entire environment in terms of security risk. Risk can be calculated by the dashboard as data is ingested, or can be supplied directly from the ESB. It also has the ability to apply various risk scores over many data fields, including identifying assets that carry a higher weighting for increased risk prioritization. The eGRC dashboard can create reports when triggered by data ingest, initiating workflow when a risk threshold has been met or exceeded. The CDSA eGRC solution has been configured so that when a threshold—configurable based upon data—has been met or exceeded, a task workflow with recommended courses of action (CoAs) is sent to the specialist for remediation. The specialist receives a link to log in to the CDSA incident response system with the exact steps to follow based upon the department's or agency's CoA guidelines. Peraton has recently enhanced this flow to include questionnaires, based on the type of incident that can drive the course of action taken. For example, questions could include, "Does this incident / vulnerability / etc. impact more than 100 users?" or "Does this put the agency mission at risk?" These questions are built into the system so that the course of action can be tailored towards impact. The end result is a common set of responses for specialists, analysts or administrators at any level of experience.

USE CASES FOR THE PERATON CDSA SOLUTION

Our solution's use cases can be adapted to any set of mission requirements. All of the current use cases that CDSA satisfies provide our customers with enhanced and actionable information, allowing users to more easily identify inherent weaknesses and malicious events that can impact critical missions. The use cases described below can be modified to support any data the agency chooses to input into the system.

Knowledge of a mission at risk

CDSA has the ability to link assets to mission services and mission applications. It can geographically display the mission area so users can visually see the mission location impacted. On the same screen, CDSA lists all the information about an asset, the threats or incidents on that asset and how that impacts services or applications. The mission is geographically rendered so the user can determine if a high-risk asset is impacting a mission service or application. Commanders may then have the choice to move the service onto another asset that is lower risk to retain mission success. See Figure 4 for an example view of a mission that is at risk.

Knowledge of an attack

CDSA has the ability to link threats or incidents on the same subnet. This information may indicate an attack. Showing other incidents occurring on the same subnet can reveal other unusual activity or indicate the probability of an attack (see Figure 5). Furthermore, placing these incidents or threats on a timeline shows the CDSA user recurring incidents or problems open for an unusually long time. This timeline approach provides attack vector references to assist in pinpointing problem areas.

Risk workflow and alerting

CDSA provides knowledge for ranking the customer environment in terms of risk. Ranking these indicators of compromise allows the user to prioritize what problems they can remediate or mitigate first. CDSA utilizes an eGRC dashboard to show this risk prioritization. It takes it a step further by providing alerting and workflow so that the warfighter or cybersecurity specialist can remediate the problem in the same manner as headquarters' personnel as well as the boots-on-the-ground supporting the mission. This is accomplished automatically by user-configured thresholds and distribution alerts.

Once a threshold is reached, an email or alert is sent to the user group responsible for that area. This email contains information on the discovered threats or vulnerabilities. When personnel click on the link presented to them in the alert, they are brought back to the system to receive full information on the incident. Based on the type of Indicator of Compromise (IoC), a questionnaire is created that probes the user for additional information, with questions similar to "How many systems does this affect?" or "How many users are currently impacted?" Answers to these questions may warrant a different course of action (CoA) than a standard response to remediate the issue. These answers, coupled with system information, drives a set of actions that enforce a consistent remediation or mitigation according to the agency's or department's processes already in place. It is important to note that the CDSA workflow can integrate with existing workflow systems or replace manual processes as needed. See Figure 6 for an example of a threshold breach in a phishing attempt. See Figure 7 for an example questionnaire with derived courses of action.

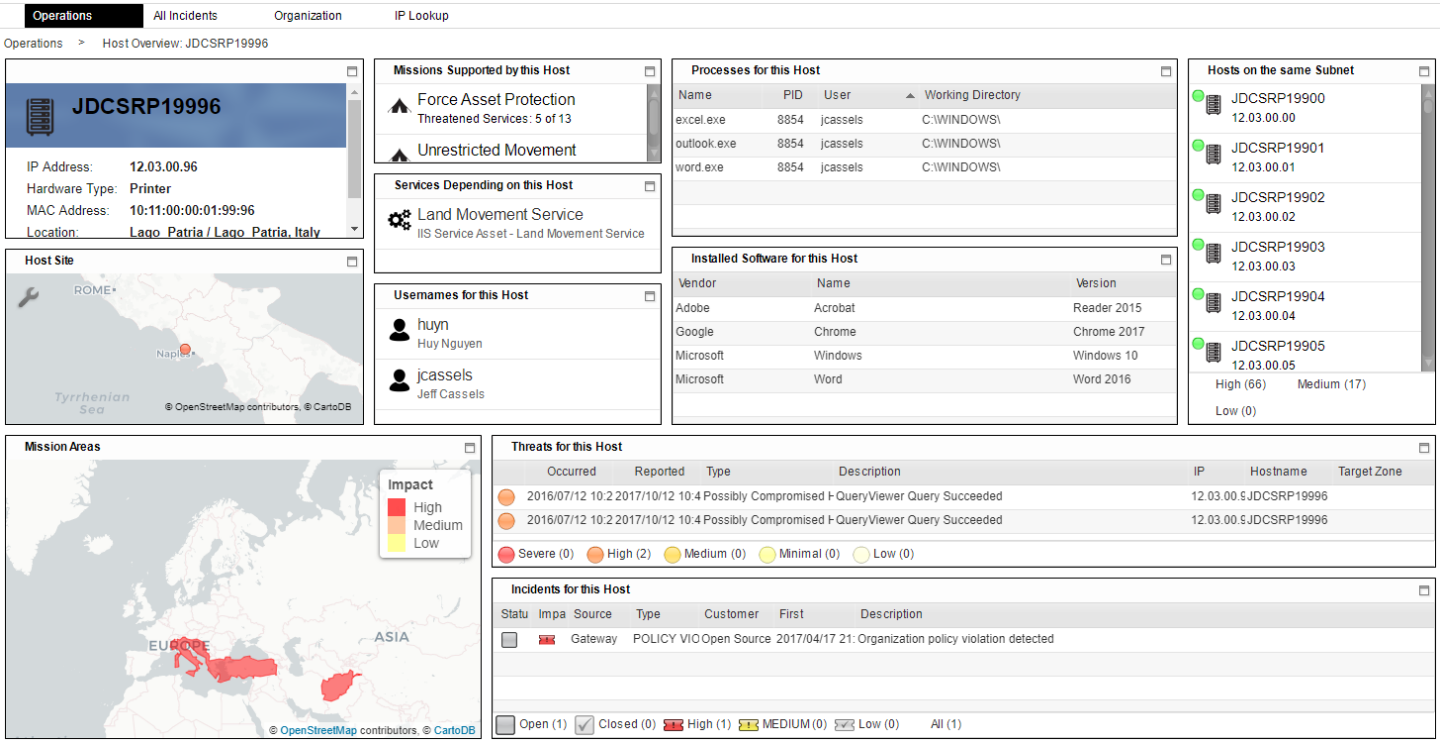

Figure 4: Incidents and threats that render a mission in southern Europe and Asia at risk

Vulnerability mitigation and prioritization

CDSA has the ability to ingest data from multiple vulnerability scanners and sensors. This information is coupled with asset information and additional vulnerability information from the National Vulnerability Database. The dashboard displays the proscribed information—department, organization or asset risk—along with the detailed information listing problem remediation or mitigation steps. Figure 8 shows an example of vulnerability scan results. All dashboard screens are configurable to customer requirements.

FUTURE OF CDSA

CDSA integrates the tools to correlate applicable data; the resulting situational awareness provides organizations the power to protect their systems, environment, missions and people. So what are the next steps for CDSA? Natural extensions to CDSA being developed by Peraton include: auto remediation, command and control, user threats, big data, mission systems, incident response simulation and training, cloud and predictive scanning.

Auto remediation

CDSA is more tightly interconnecting all security systems and components to enable auto-remediation (not requiring human intervention). Today the scanning cycle takes place, which feeds information to other systems that will facilitate pushing patches and re-configuring or modifying a system. Peraton is developing our CDSA system to automatically push patches and re-configurations to customer machines. This enhancement to CDSA takes advantage of integrations with Microsoft (MS) Windows Server Update Services (WSUS) or MS Systems Center Configuration Manager (SCCM).

Eventually, this auto-remediation will include modification or supplementing overarching policies and their dissemination across an enterprise.

Command and control

Following the use cases detailed in previous sections, CDSA is implementing command and control operations. Currently, if a vulnerable asset is jeopardizing a mission, the service running on that asset must be moved to another asset to protect the mission. Automatically moving the service could be problematic without human intervention to determine other impacts. For example: the mission's service in jeopardy requires Java OpenJDK version 10 and OpenJDK on the target server is only at version 9. This would need to be corrected by an OpenJDK upgrade on the target. To automatically solve a problem such as this, Peraton proposes a step-based approach to implement a full command and control paradigm.

The overall steps to perform the command and control actions would be the following:

- Understanding of the compute resources and software the service is currently operating on
- Understanding of the target compute resources and software that is available for mission failover
- Comparison between the source and target destination to calculate any gaps in resources
- Determination of any gap in resources to be satisfactory for automatic relocation of mission service to occur
- Restart and re-connect of mission service and applications on failover target

User threats

Since CDSA currently relates data back to an asset and its infrastructure, the next progression is relating this information to the people that use, maintain and operate these systems. For example, if the system shows an asset or group of assets that are vulnerable or continue to show as vulnerable on the customer's dashboard, this could indicate that there is an insider with malicious intent. Linking asset information to data that shows a user's escalated privileges on these assets, inordinate amount of time accessing these assets, or is operating out of the normal bounds for their user group or role could indicate malicious intent that should be investigated. Peraton is currently working with multiple vendors to provide the capability to investigate and relate these occurrences.

Big data

Peraton's CDSA solution currently has the ability to store data to any storage location, big data included. Adding dedicated big data information can provide CDSA with the ability to bring additional knowledge to the solution. Analytics on social media data, archived data or raw sensor feeds can augment the user data previously mentioned. Analysis and visualization tools can perform detailed analytics, which then can be fed back into CDSA for increased knowledge of both internal and external behaviors, threats and risks within the environment. Peraton has currently piloted solutions that focus on insider risk and geolocation / mapping of intelligence assets.

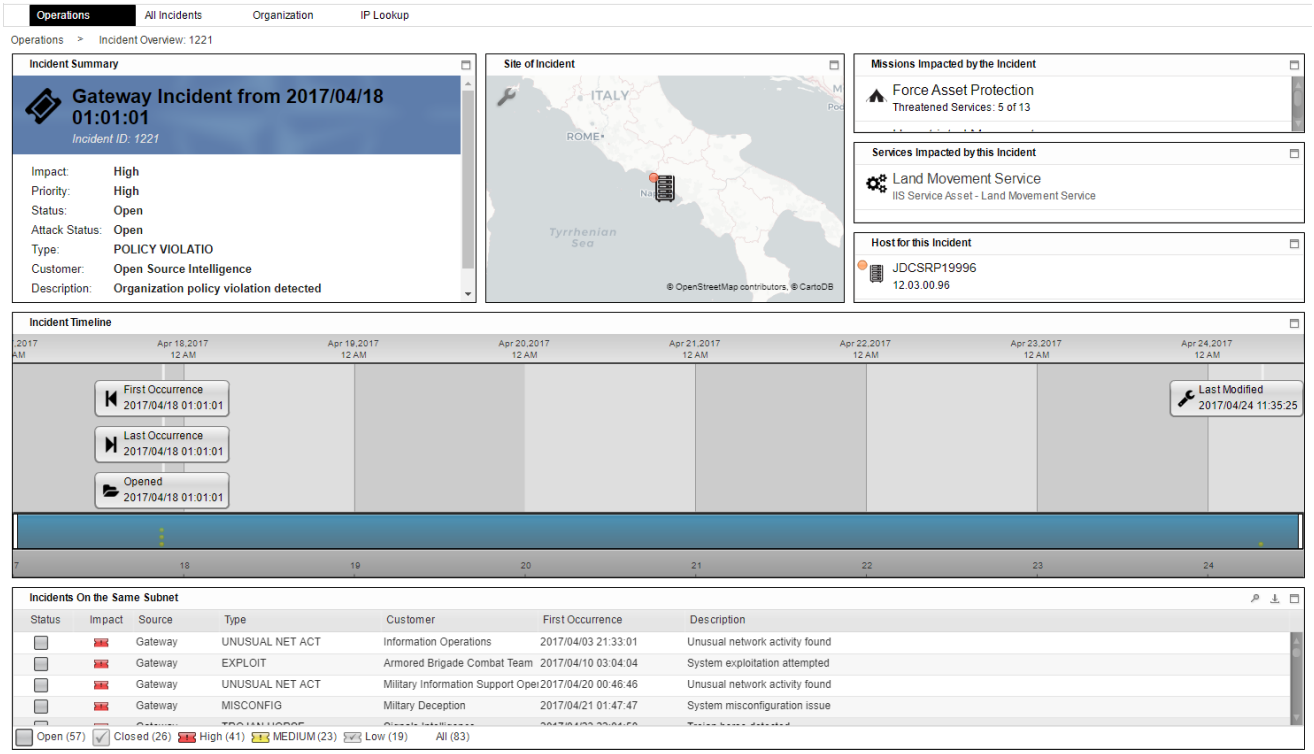

Figure 5: Incidents on the same subnet with a timeline of events

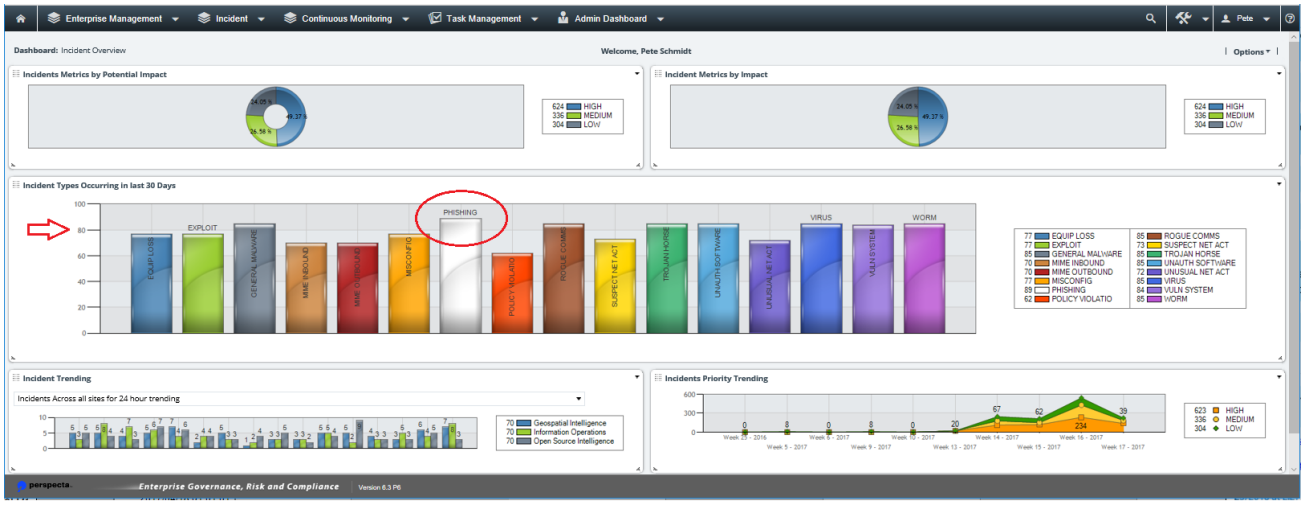

Figure 6: Phishing attempt has breached 80 incidents in 30 days

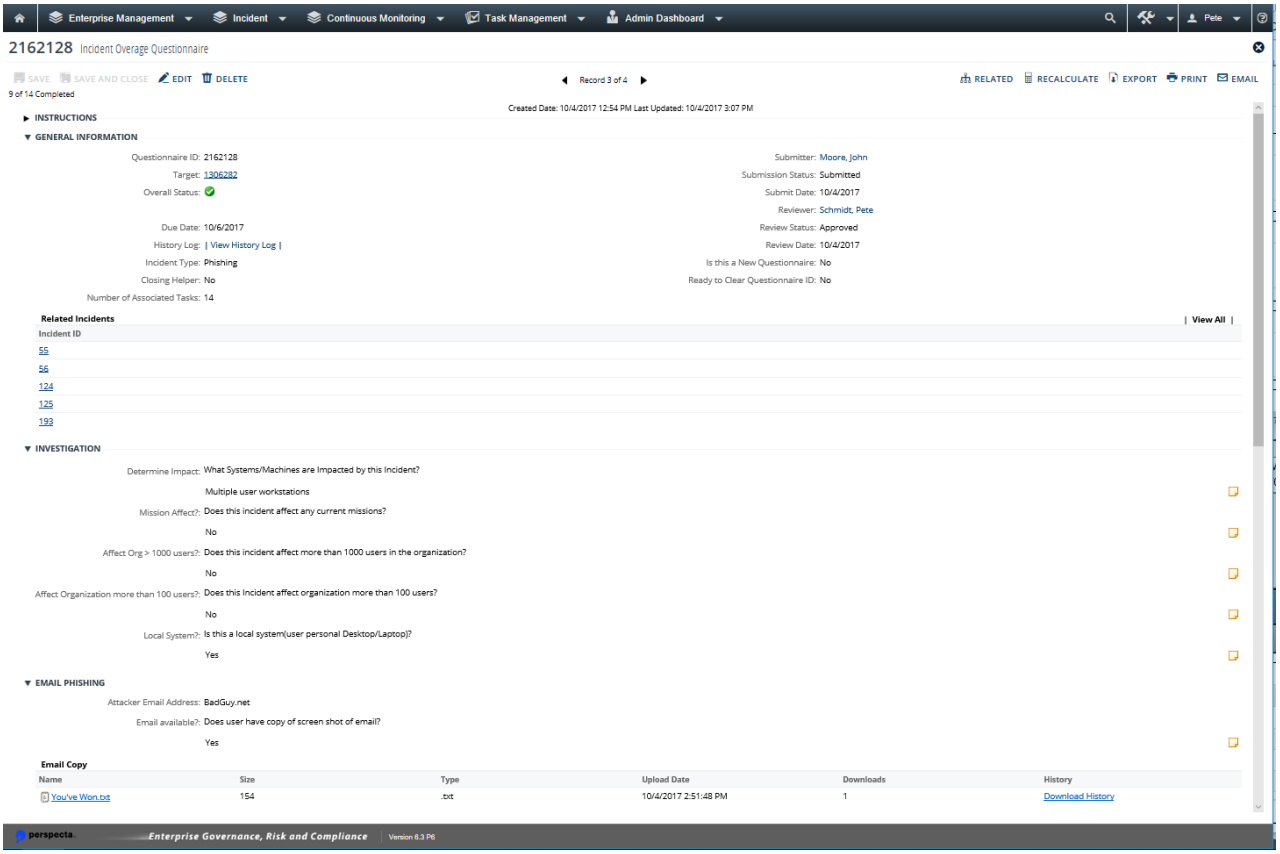

Figure 7: Questionnaire example, shown with phishing type

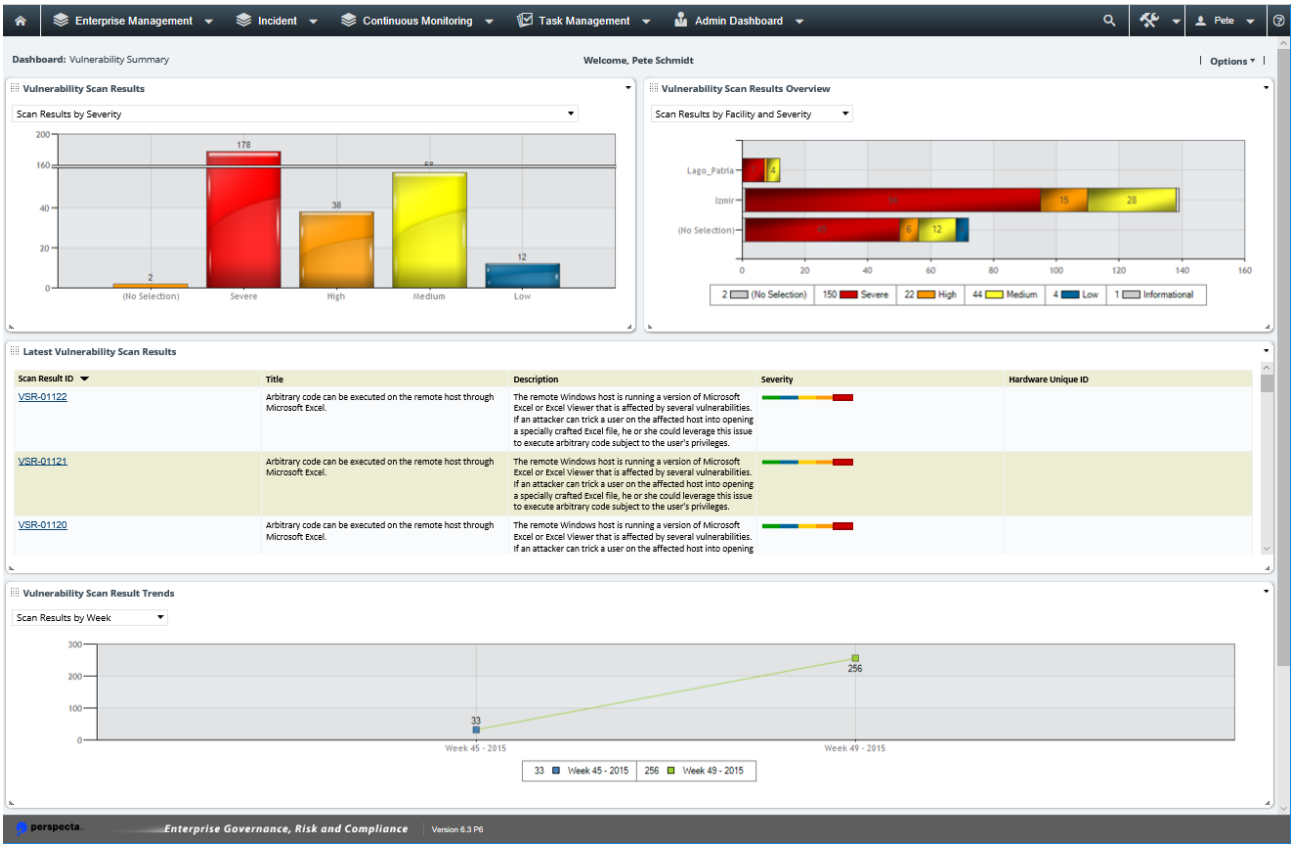

Figure 8: Vulnerability management

Mission systems

Today CDSA obtains its mission information from file, database or direct system integration. Mission hierarchy and links to services and assets could be provided from CDSA directly. Having the core information local to the solution makes systems operations easier and more flexible. CDSA already has the facility for capturing relationships between missions and the environment's infrastructure. Peraton engineers are currently creating an innovative system for linking, managing and relating military missions to the assets and services that support them.

Incident response and simulation and training

As described above, Peraton has developed the ability to define, create, update and execute CoAs. The intent is to record the execution, performance and effectiveness of a particular CoA. As that information is collected and analyzed, it can be leveraged to run simulations to both improve overall quality of CoAs and to use as a training tool for security operators.

Cloud

We have worked with a market-leading cloud provider to host a virtualized version of CDSA that can improve solution delivery or operate in a shared services model. Peraton is continuing to evolve CDSA into a native cloud service, utilizing cloud provider containers and microservices. As sensors and scanners become hosted in the cloud, CDSA is able to communicate with these scanners and ingest their security data.

Predictive scanning

Predictive scanning is an innovative area that utilizes an analytics engine to analyze risk exposure and zero day vulnerabilities. Without launching any scans, CDSA would predict the impact and risk exposure to allow a user to remediate or mitigate these threats immediately. Relating the knowledge of the asset and software running on it, the CDSA system will be able to forecast risk exposure prior to a pre-designated patching schedule or the expected (announced) release of a patch or mitigation.

CDSA SUMMARY

CDSA eliminates data in silos and provides mission-focused situational awareness so that an accurate response can be immediately executed to mitigate threats. Without this knowledge, threats and IoC's can go unnoticed and cause significant harm to the customer environment.

CDSA provides our customers with the power to protect their systems, environment, missions and people. Without this integrated approach, organizations are destined to operate security tools in isolation rather than taking a comprehensive view of the security architecture. Our data-centric approach to cybersecurity and mission assurance also allows us to perform in-depth analytics to determine internal and external threats to an organization's mission.

For more than five years, we have invested in this approach. Instead of developing narrowly focused solutions based on RFP requirements, we believe in developing a comprehensive, standards-based solution that we can augment according to specific organization requirements. Our investment has allowed us to solve the complex integration problems needed to make this approach a reality for very demanding end customer environments (e.g., DHS, NATO and DOD).

Peraton

LEARN MORE AT

PERATON.COM

12975 Worldgate Drive
Herndon, VA 20170-6008