ELASTIC FOR CDM DEFEND

Introduction to the Elastic Stack

As the creators of the Elastic Stack (Elasticsearch, Kibana, Beats, and Logstash), Elastic builds tools that make security data usable in real time and at scale. With a search and analytics engine that indexes data on ingest, Elastic makes data queryable right away and in real time. It is also flexible and scalable so security practitioners can manage growing data needs and provide a more complete picture of their agency's security posture.

Continuous Diagnostics and Mitigation (CDM) requires new cyber analytics techniques to track and address what is happening on the network. With the speed, scale, flexibility, and API-driven compatibility of Elastic, government agencies can ingest and query massive amounts of data for effective threat detection. Elastic products are currently included on the DHS-Approved Products List and are available from GSA via SIN 132-44.

CDM DEFEND

The CDM program, managed jointly by the US Department of Homeland Security and the General Services Administration, has moved through its first two implementation phases with a focus on what and who is on federal government agency networks. Now the program has advanced into Phase 3, which is geared toward what is happening by identifying and managing network activity. Phase 3 includes services collectively known as Dynamic and Evolving Federal Enterprise Network Defense, or DEFEND, to expand federal agency expertise on network management and protection strategies.

CDM goals are to provide capabilities for dynamic monitoring of security controls for network and perimeter components, host, and device components, data at rest and in transit, and user behavior. In today's ever-changing threat environment, meeting these goals requires advanced cyber analytics that can handle tens of petabytes of structured and unstructured data.

To advance its governmentwide cyber awareness and monitoring objectives, DHS recently selected ECS Federal, who is partnering with Elastic to implement a new cyber analytics ecosystem, the CDM Dashboard II. With a simplified technical architecture, the new Dashboard will draw on Elastic tools including Elasticsearch and Kibana to significantly accelerate data ingest. The Dashboard will also ensure trusted interoperability with robust APIs and streamlined interagency information sharing for timely cyber threat awareness and response.

From Threat Detection to Threat Hunting

The level of data handling, query and response, and real-time threat identification required for effective CDM implementation requires a new cyber security technique — threat hunting. Cyber threat detection can no longer rely solely on a series of queries geared toward past behavior that look for anomalies in large, static data sets. To address the dynamic nature of the environment, threats must be addressed proactively and interactively as they develop and evolve.

 © 2019 Elasticsearch B.V. All rights reserved.

elastic

Elasticsearch is a powerful, API-driven search engine that indexes data upon ingest. This allows agencies to build threat analytics platforms that manage petabytes of data, deliver results in seconds, and enable analysts to submit ad hoc queries on unstructured data.

In a robust threat hunting model powered by Elastic, analysts have the freedom to go where the data, coupled with their intuition and knowledge, leads them, and do it quickly. If analysts note anomalous network traffic or an unusual incident, they need to be able to formulate queries about the data and the event on the fly, rather than rely on preset questions against specific data sets. Older security information and event management (SIEM) approaches do not afford this ad hoc flexibility. Elastic does.

Threat hunting is not a replacement for ongoing cybersecurity efforts. Rather, it complements enterprise network defense activities by advancing threat detection capabilities for organizations of any size.

Flexibility & Speed for Advanced Cyber Analytics

Elastic makes data immediately available for analysis, unlike alternative approaches that index data only when requested, adding significant delays to the threat identification process. Further, Elastic leverages all data for analysis — structured (log files), semi-structured (packet capture or PCAP), and unstructured (full text). Legacy tools cannot analyze unstructured data.

Another consideration in Phase 3 DEFEND is data volume and retention. Many government agencies are required to retain large amounts of data indefinitely. Elastic manages petabyte-sized datasets efficiently, effectively, and instantly, enabling analysts to do their jobs successfully at scale. With Elasticsearch, query result times can be reduced to seconds from the minutes or even hours required by legacy technologies.

Compatibility to Expand Agency Capabilities

Elastic open source search tools work with and complement the cyber tools and legacy architectures that agencies must use. With an extremely open architecture leveraging RESTful APIs, Elastic components can be used independently or as a full stack depending on each user's specific requirements. Data and processing can easily be shared with other big data platforms using connectors. Organizations need not abandon familiar legacy tools to supplement their capabilities with the performance and scalability of Elastic.

Elastic Supports CDM DEFEND

Elastic provides the power to handle more data, and more kinds of data, with unprecedented speed and accuracy. As an open source technology, Elastic supports incremental approaches to introducing threat hunting to existing risk management strategies. An annual subscription model with no limits on data ingest allows government agencies to scale well into petabytes of data for less cost than many legacy systems. And Elastic is designed to work well with existing log and security analytics tools so organizations can optimize and extend prior investments.

Elastic products are currently on the DHS-Approved Products List and are available from GSA via SIN 132-44. The Elastic team understands agency CDM requirements, including individual and collective cybersecurity concerns and operational strategies. Consequently, we are well prepared to work with partners selected to support agency Phase 3 DEFEND programs.

The Elastic federal team is available to answer any questions you may have.
Visit elastic.co/federal or email cdm@elastic.co for more information.

 © 2019 Elasticsearch B.V. All rights reserved.

elastic