Gigamon®

POINT OF VIEW

Aligning Agency Cybersecurity Practices with the Cybersecurity Framework

Leveraging Gigamon to Align Cybersecurity Budgets with Desired Business Outcomes

Agency Heads Made Accountable for Cybersecurity Risk Management

The President is now holding agency heads directly accountable for managing the cybersecurity risks to their enterprises. As directed by Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (Executive Order), and as clarified by the Office of Management and Budget (OMB) guidance[1], agency cybersecurity practices and posture will be evaluated by DHS and OMB. Agencies must provide a plan for mapping cybersecurity activities to the NIST Framework for Improving Critical Infrastructure Cybersecurity (Framework) and present an action plan to address gaps and unmitigated risks. Agencies are required to align IT budgets to address the gaps and deficiencies exposed through use of the Framework.

The Vital Role of Measurements and Metrics in Aligning Budgets with Desired Outcomes

For effective resource and budget allocation, agencies must be able to accurately measure both the threats to the enterprise infrastructure and the effectiveness of their cybersecurity tools. Accurate measurements are a prerequisite for achieving alignment between the cybersecurity risk management program and business goals. As stated in draft 1.1 of the Framework document, "The ability of an organization to determine cause-and-effect relationships between cybersecurity and business outcomes is dependent on the accuracy and precision of the measurement systems…the measurement system should be designed with business requirements and operating expense in mind."

Gigamon GigaSECURE Security Delivery Platform Aligns Cybersecurity Budgets with Desired Business Outcomes

Gigamon provides a Security Delivery Platform that maximizes network traffic visibility and optimizes cybersecurity tool performance to align cybersecurity budgets with desired business outcomes. The GigaSECURE platform delivers continuous and pervasive network traffic visibility to cybersecurity tools used in an enterprise. This visibility enables accurate and precise measurements that are essential to implementing an effective risk management strategy. Independent studies have shown that GigaSECURE optimizes cybersecurity tool performance and coverage, and reduces associated tool costs by 30 to 50 percent.[2]

- **Close the Visibility Gaps**: The GigaSECURE platform provides traffic visibility across all IT and Operational Technology (OT) operations for both physical and virtual assets in data centers, remote sites and the private and public cloud. The GigaSECURE platform eliminates monitoring blind spots to vastly improve the accuracy and precision of threat measurements and resulting metrics provided by cybersecurity tools.
- **Close the Budget Gaps**: The GigaSECURE platform optimizes the performance and coverage of cybersecurity tools utilized in the Framework core, providing each tool with customized data sets to maximize tool capacity while lowering tool CAPEX and OPEX requirements.
- **Close the Protection Gaps**: Once deployed on the network, the GigaSECURE platform allows for rapid upgrades and additions to the agency cybersecurity suites.

As noted in the Gartner Adaptive Security Architecture, found at **www.gigamon.com/gartner-security-model** continuous visibility is central to many security capabilities that map to the NIST Framework core – Protect, Detect, Respond, and also to Identify and Recover. The GigaSECURE Delivery Platform delivers network traffic visibility and reduces the cost of closing existing protection gaps and achieving target Framework profiles.

Gigamon and the Cybersecurity Framework Core

The following provides a mapping of network traffic visibility benefits and capabilities in the GigaSECURE platform to the relevant assessment criteria provided in Appendix 1 of the OMB MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES (M-17-25). The assessment criteria listed in the following section, compiled from the cybersecurity Framework functions – Identify, Protect, Detect, Respond, Recover – categories and subcategories, are a subset of the criteria that will be used by OMB to assess agency cybersecurity risk management practices.

The network traffic visibility offered by the GigaSECURE platform optimizes tool performance and tool configuration to enable centralization and consolidation of cybersecurity monitoring tools. Agencies can eliminate the gaps and deficiencies in the Cybersecurity Framework Profiles and at the same time reduce the associated CAPEX and OPEX. The cumulative budgetary benefits of a GigaSECURE deployment are realized through optimization of the many cybersecurity tools needed to support the Framework functions, as listed below. A recent Forrester[2] report documents that a typical enterprise deploying GigaSECURE realizes a reduction in security costs of 50 percent and achieves a three-year return on investment of 153 percent, with the investment paying for itself in seven months.

Identify Function Assessment Criteria

Asset Management and Authorization

- The organization's hardware assets are covered by an enterprise-level automatic hardware asset inventory capability.
  - The GigaSECURE platform provides the network traffic visibility and tool optimization required for complete device discovery.
- The organization's unclassified networks possess a technology solution to detect and alert on the connection of unauthorized hardware assets.
  - *The GigaSECURE platform provides the network traffic visibility and tool optimization required for effective and complete detection of unauthorized hardware assets.*

Comprehensive Risk Management

- The organization implements appropriate baseline security controls based on mission/business requirements and policies.
  - The GigaSECURE platform optimizes the performance of individual cybersecurity tools and tool deployment configurations to enable implementation of the appropriate baseline security controls within the available budget.

Note on Identify Function: The Identify function has been highlighted as "foundational" to the Cybersecurity Framework. Many Federal agencies have verified this via their experience with the Continuous Diagnostics & Mitigation (CDM) Program Phase 1 deployment, which included the need to conduct physical and virtual device discovery to support a Hardware Asset Management (HWAM) solution. Without complete and accurate asset discovery, the effectiveness of all other CDM solutions is degraded, leading to higher levels of risk for various systems. Complete and accurate device discovery proved much more difficult to achieve than originally anticipated, with network infrastructure unable to effectively provide and filter enterprise network traffic to the HWAM tools. DHS was facing the possibility of having to "supersize" the HWAM tools in order to cope with the issue, or accept the heightened risk to systems from degraded CDM solution performance.

DHS resolved the issue by deploying network traffic visibility with the GigaSECURE platform across many Federal agencies, and in the process obtained pervasive network traffic visibility across IT operations, consolidation and centralization of HWAM tools and custom data sets to the HWAM tools to maximize tool throughput and performance.

Protect Function Assessment Criteria

Network Protection

- The organization's unclassified networks are assessed for vulnerabilities using Security Control Automation Protocol (SCAP) validated products.
  - *The GigaSECURE platform provides the network traffic visibility required for effective deployment of Security Control Automation Protocol (SCAP) validated products.*
- The organization's unclassified networks are covered by a capability that blocks unauthorized devices from connecting.
  - *The GigaSECURE platform provides the network traffic visibility required for the effective use of Network Access Control solutions to block unauthorized devices from connecting.*
- Organizations possess an Insider Threat program deemed by the National Insider Threat Task Force to be at Full Operating Capacity.
  - *The GigaSECURE platform provides the network traffic visibility, including Metadata and NetFlow, across all IT and OT operations for both physical and virtual assets in data centers, remote sites and private/public clouds, which is required for effective Insider Threat detection.*

Detect Function Assessment Criteria

Anti-Phishing Capabilities

- Incoming email traffic passes through anti-phishing and anti-spam filters at the outermost border mail agent of server.
  - *The GigaSECURE platform optimizes the deployment configuration and performance of anti-phishing and anti-spam filters.*
- Incoming email traffic is analyzed using sender authentication protocols.
  - *The GigaSECURE platform ensures that all email traffic is provided to the email traffic analyzer for correct analysis. Monitoring data can be limited to only email traffic.*
- Incoming email traffic is analyzed using a reputation filter.
  - *The GigaSECURE platform ensures that all desired email traffic is forwarded to the reputation filter for analysis.*
- Incoming email traffic is analyzed to detect for clickable URLs, embedded content and attachments.
  - *The GigaSECURE platform optimizes the deployment configuration and performance of email content and attachment analysis solutions. Emails with hyperlinks or attachments can be filtered and delivered to email content analysis solutions.*
- Incoming email traffic is analyzed for suspicious or potentially nefarious attachments and opened in a sandboxed environment or detonation chamber.
  - *The GigaSECURE platform optimizes the deployment configuration and performance of analysis solutions conducting file detonation.*

Malware Defense Capabilities

- Endpoints are covered by an intrusion detection system.
  - *The GigaSECURE platform optimizes the deployment configuration and performance of intrusion detection systems.*
- The organization's assets are scanned for malware prior to an authorized remote access connection to the unclassified network.
  - *The GigaSECURE platform optimizes the coverage and performance of network access control solutions.*

Exfiltration and Other Defense Capabilities

- Inbound network traffic passes through a web content filter, which provides anti-phishing, anti-malware, and blocking of malicious websites.
  - *The GigaSECURE platform optimizes the deployment configuration and performance of web content filters. The platform provides options for both out-of-band and in-line bypass deployment of the web content filter, with the filter receiving only the desired data.*
- Outbound communications traffic is checked to detect encrypted exfiltration of information.
  - *The GigaSECURE platform supports decryption of SSL/TLS-encrypted traffic for tools deployed in-line, using an In-line bypass configuration, or for tools deployed out-of-line. By offloading the compute-intensive SSL/TLS decryption function to the GigaSECURE platform and adopting a "decrypt once, analyze multiple times" architecture, the performance of the cybersecurity tools increases significantly.*
- Emails are processed by systems that quarantine or otherwise block suspected malicious traffic.
  - *The GigaSECURE platform optimizes deployment configurations and performance of blocking tools.*
- The organization has the ability to detect attempts to access large volumes of data and investigate such instances.
  - *The GigaSECURE platform provides the complete network traffic visibility needed to support data loss prevention solutions. The GigaSECURE platform also generates NetFlow/IPFIX records with contextual metadata to enable accelerated analysis and prevent inappropriate data access and exfiltration.*
- EINSTEIN tools are fully implemented.
  - *The GigaSECURE platform provides optimized tool deployments at the Agency Trusted Internet Connection (TIC) to enable complete and optimized implementation of EINSTEIN monitoring.*

Respond Function Assessment Criteria

Planning and Process

- The organization mitigates all significant vulnerabilities within 30 days of notification.
  - *The GigaSECURE platform enables rapid upgrades and additions to the cybersecurity tools needed to support continuous monitoring in the context of risk management, without interfering with ongoing cybersecurity protection and with significantly reduced Change Management costs.*

Evaluation and Improvement

- The organization has institutionalized a process of continuous improvement incorporating advanced cybersecurity practices.
  - *The GigaSECURE platform enables rapid upgrades and additions to the cybersecurity tools needed to support continuous monitoring in the context of risk management, without interfering with ongoing cybersecurity protection and with significantly reduced Change Management costs.*

Recover Function Assessment Criteria

- Personnel Impact Processes - For those cases in which personally identifiable information (PII) has been or potentially could have been compromised, it is imperative that the organizations have in place capabilities to notify affected persons and provide them with necessary identification protection tools and services.
  - *The GigaSECURE platform provides advanced filtering capabilities, enabling identification of PII within a packet, enabling analysis devices to quickly determine if PII was compromised, and allowing acceleration of the notification function.*

GigaSECURE Security Delivery Platform from Gigamon

Gigamon is the market leader in network visibility, with 59 percent market share in the government vertical according to a May 2017 market share analysis done by the third party analyst firm IHS. The GigaSECURE Security Delivery Platform supplies attached tools with complete network traffic visibility from across complex, distributed and virtualized networks to eliminate monitoring blinds spots that can compromise cybersecurity and increase the risk to systems. The GigaSECURE platform aggregates network traffic, applies intelligent processing in real-time and forwards custom data sets to the cybersecurity monitoring and analysis tools. The coverage and performance of each tool is optimized, with each tool getting only the data needed to perform the assigned analysis while the costs required to deploy and support each tool is significantly reduced. The GigaSECURE platform supports both out-of-band and in-line configurations for optimized tool deployments, with options to provide decryption of SSL/TLS-encrypted traffic for both out-of-band and in-line tools. The GigaSECURE platform generates NetFlow/IPFIX records enriched with contextual metadata to analysis tools as required to enable accelerated analysis.

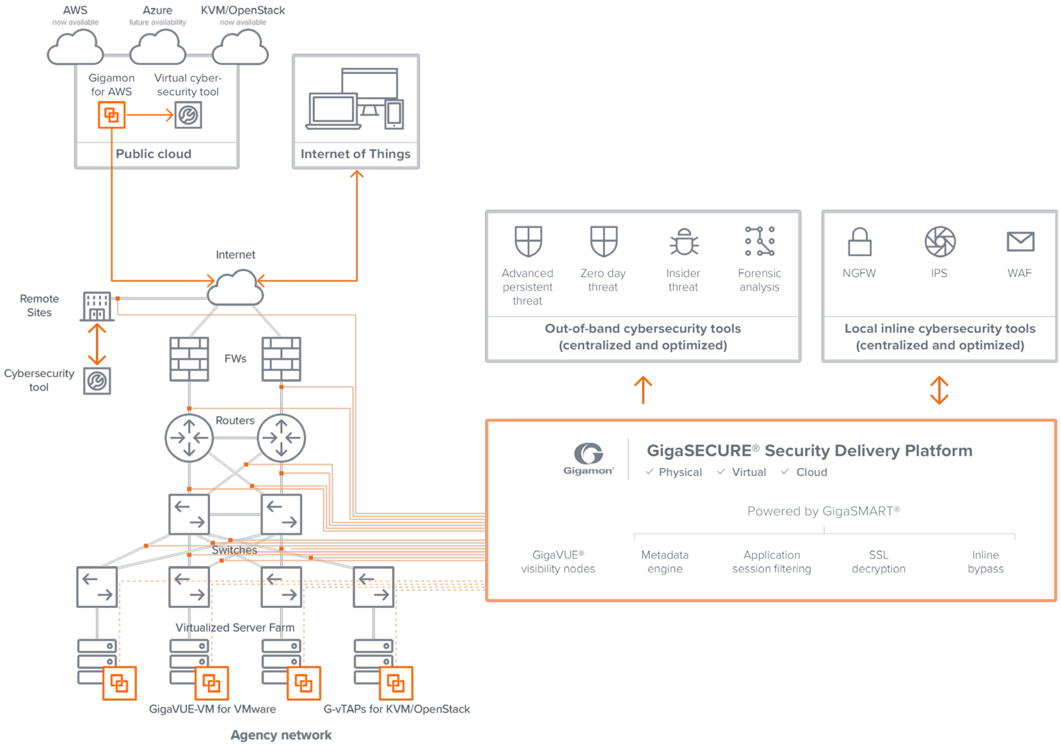

Figure 1: The GigaSECURE Platform maximizes network traffic visibility and optimizes cybersecurity tool performances to align cybersecurity budgets with desired business outcomes.

[1] Mick Mulvaney, "*Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*," M-17-25, MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES, May 19, 2017.
[2] *The Total Economic Impact™ of Gigamon*, Forrester, April 2016.

About Gigamon

Gigamon provides active visibility into physical and virtual network traffic, enabling stronger security and superior performance. Gigamon's Visibility Platform and GigaSECURE®, the industry's first Security Delivery Platform, deliver advanced intelligence so that security, network and application performance management solutions in enterprise, government and service provider networks operate more efficiently and effectively. See more at www.gigamon.com, the **Gigamon Blog**, or follow Gigamon on **Twitter**, **LinkedIn** or **Facebook**.