Merlin enables HHS CSIRC to build an enterprise-wide view of cybersecurity for rapid threat assessment and disposition

Customer:
Department of Health and Human Services

Highlights:

- **Second largest CSIRC** in the federal government
- CSIRC responds to **over 6 billion** correlated security alerts per week
- CSIRC monitors activity on **more than 400,000 endpoints** across HHS and its 11 Operational Divisions
- CSIRC looks for Indicators of Compromise (IOCs), malware, suspicious behaviors, and anomalous events

Agency Requirements

Faced with the consistent growth and sophistication of cyberattacks, the operating divisions (OPDIVs) of the Department of Health and Human Services (HHS) took a variety of individual actions to protect their systems and data from malicious threats. This fostered the development of individual information security infrastructures within each of the various operating divisions where each program was "siloed" and grew based on disparate technologies.

This independent distribution of security tools did not allow for the central coordination of information security incident data across the Department. Correlation of attacks to identify mutual threats—which would allow all participants to benefit from information sharing—could not be performed. Countermeasure recommendations were not uniform across the department, leaving those without similar security technologies vulnerable to current cybersecurity threats.

Additionally, as the number and sophistication of cyber-attacks grew, so did the costs to maintain multiple overlapping cybersecurity infrastructures. Not only was there a duplication of infrastructure costs, there were also costs incurred in building defenses to new cyber-attacks in one operating division when a defense had already been created by another operating division.

A Centralized Security Solution

To improve the security posture across the Department, HHS partnered with Merlin International as its primary cybersecurity contractor. Merlin was tasked to create and implement a centralized solution— the Computer Security Incident Response Center (CSIRC)—as the primary component of an overall HHS Cybersecurity program under the direction of the HHS Chief Information Security Officer.

As a central clearinghouse, the CSIRC is responsible for protecting HHS computer systems and information across all OPDIVs, providing centralized expertise in security management and consulting services, and serving as a focal point for security information collection, incident processing and analysis, and overall security services management for the Department.

Extensive Department-wide security tools and capabilities have now been provided and standardized across all OPDIVs to develop a robust situational awareness of HHS's security posture and risk exposure. CSIRC's ongoing mission is to maintain, enhance, and leverage effective security technologies across the Department in coordination with the individual divisions.

HHS - Second largest CSIRC in the Federal government

Integrating Diverse Technologies

Implementing the HHS vision for a centralized cybersecurity clearinghouse proved to be a complex and challenging project. Merlin handled the task of identifying, integrating and operating a broad range of hardware and software network management and cybersecurity technologies to enable effective communication between components and ensure working data relationships. The Merlin team was able to implement the CSIRC project in under a year, creating a centralized cybersecurity system that now allowed the smooth flow of information between the numerous security components and with CSIRC personnel.

These technologies included:

- Agiliance RiskVision
- ArcSight Enterprise Security Manager (ESM)
- BMC Remedy
- CISCO Works
- FireEye
- Gigaman GigaVue
- Hitachi and NetApp Storage Area Network (SAN)
- IBM Tivoli/BigFix
- Juniper, Checkpoint, and Palo Alto firewalls, VPN, SA
- Lancope
- Multiple AV software components
- NetScout
- NetWitness Investigator, Informer
- SolarWinds
- TippingPoint Intrusion Detection System/Intrusion Prevention System (IDS/IPS)
- VMWare
- Websense
- Wireshark

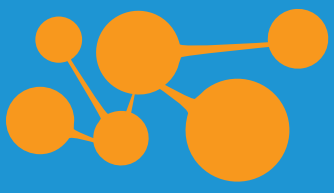
Maintaining Cyber Vigilance

Today, Merlin provides operational support services to HHS by delivering:

- 24x7x365 network security monitoring, analysis and security incident reporting
- Security operation center (SOC) IT engineering and operations support
- Threat analysis
- Research and engineering
- Vulnerability analysis
- Forensics and malware analysis

Having established a centralized cybersecurity program in an extremely short period of time, the CSIRC now deploys common alerts down to the operating division level, provides consistent monitoring across the Department, and coordinates events of interest. One key project element is a system of live dashboards—redrawn every three minutes based on daily threat feed updates—that show connections across the US and to foreign countries. This near real-time data gives the analysts an excellent visual representation to work with.

As a case in point, HP TippingPoint recently proved its value in the area of cloud-based file sharing. Any traffic going out over a Secure Socket Layer (SSL) connection is



CSIRC responds to over 6 billion correlated security alerts per week

merlin®

secure.performance

assumed to be encrypted, so it is typically not proxied; in other words, nobody is inspecting that traffic. But with technologies like Dropbox—where somebody can install a client inside the government network, connect out over SSL to share files, put the client on their home machine, and then access those files again—there is no way to know where Department data is going.

Merlin configured HP TippingPoint to alert the CSIRC in HP ArcSight about Dropbox and other peer-to-peer sites, and then use ArcSight's event graphs to generate a clear picture for management. As a result, CSIRC is now able to block this traffic at both the Department and operating division levels.

CSIRC manages an array of security tools and technologies across HHS to ensure a comprehensive and proactive defense against cyber-attacks.

CSIRC monitors activity on more than 400,000 endpoints across HHS and its 11 Operational Divisions

CASE STUDY

The Result: An Effective Cybersecurity Defense

Today, CSIRC tracks an ever-increasing number of alerts and logs anomalous "hits" against the **various servers, firewalls and other appliances that are scanned each second for activity**. At the Department level, CSIRC processes around 10 billion logs a week, with a couple hundred intrusions per day requiring additional investigation. This activity results in three to four cases per day processed in ArcSight and approximately half of these cases turn into incidents that are reported to US-CERT.

HHS is a large and complex organization, both politically and from a funding perspective. It covers an enterprise that spans all states, territories, tribal communities, and 10 foreign countries. Despite the sheer number of people, systems, and networks, the HHS Cybersecurity Project has been extremely successful in getting the various factions within the Department to standardize on key technologies and processes. HHS and the Merlin team have enabled CSIRC to establish a security infrastructure that:

- Allows detection and mitigation of malicious activity directed against HHS;
- Establishes a unified approach for information security;
- Strengthens and improves upon the security posture of the agency;
- Enhances protections to public health science, data and administrative systems;
- Delivers a sustainable solution that can be funded through normal funding cycles;
- Deploys/supports secure enclaves across the OPDIVs providing a federated approach to managing security; and,
- Staffs a 24×7 security operations center with properly trained personnel.

By streamlining the identification of threats and mitigating vulnerabilities, the result has been much more accurate identification of malicious activity on the network, reduced time to insight into security threats, less staff time required to detect and assess network intrusion events, and greatly enhanced security of HHS systems. Merlin's security implementation now provides an enterprisewide view of cybersecurity that enables the rapid assessment of the HHS infrastructure as previously unknown threats emerge—all with far more efficient use of taxpayer resources than was possible under the previous siloed approach.

About Merlin International

Merlin International is a leading provider of world-class system integration services and solutions that enable the U.S. Federal Government to better meet mission requirements and challenges. By combining a broad portfolio of best-of-breed information technology solutions with deep expertise and experience building and implementing solutions with quantifiable return on investment and long term sustainability, Merlin is preparing our Government for the future. Our core competencies are Cybersecurity, Infrastructure and Network Operations, and Enterprise Applications. The company is headquartered in Englewood, CO, with federal operations in Vienna, VA.

CS10059.0516-HHS-CSIRC

SOLUTIONS
solutions@merlin-intl.com
www.merlin-intl.com
T 1.877.430.3021

MERLIN GOVERNMENT CONTRACTS
SEWP# NNG15SC17B
GSA# GS35F0628Y

CORPORATE OFFICE
4B Inverness Court East | Suite 100
Englewood, CO 80112
T 303.221.0797 | F 303.496.1420

FEDERAL OPERATIONS
8219 Leesburg Pike | Suite 400
Vienna, VA 22182
T 703.752.2928 | F 703.752.2935

merlin®
secure.performance

CASE STUDY

www.merlin-intl.com/health