

Solution Brief: Addressing the MITS Standard with ArcSight

Government of Canada Operational Security Standard

ArcSight products support federal government departments in complying with the mandatory security requirements specified in MITS and the Government Security Policy.

Highlights

- Develop graduated safeguards to protect your critical assets
- Create a workflow policy documenting security changes
- Respond quickly to security incidents and minimize damage

MITS Background

As of December 31, 2006 all Government of Canada (GoC) departments and agencies should be in compliance with the MITS (Management of Information of Technology Security) standard. The MITS Standard requires Canadian federal departments to protect the security of information and IT assets under their control, and design an IT security strategy outlining how they will protect information throughout its life cycle.

ArcSight Security: Supporting the MITS Standard

The MITS regulation is comprised of three parts. Part I is the introduction. Part II discusses developing a security baseline, roles, responsibilities and departmental policy guidelines. Part III details specific technical and operational safeguards. ArcSight's suite of products support many of the components of MITS, with special emphasis placed on the regulations stated in Part III sections 13-18.

Section 13: Graduated Safeguards

This encompasses segregating sensitive information and services thus allowing more restrictive and possibly expensive safeguards to be focused on a more limited array of assets.

Within ArcSight's Enterprise Security Management (ESM) solution, graduated safeguards can be further expanded to the monitoring and analysis of assets. Some mission-critical assets (servers, applications, networks, data centers) may have dedicated visual analytics, reports and analysis features specifically designed for them, while others are treated more generally. Being able to choose which assets receive a greater portion of computing and human resources allows for greater scalability and increases operational efficiencies and effectiveness among analysts.

Section 14: Processes that Support Security

This includes general controls such as configuration management and change control, problem reporting/help desk, capacity planning, and system support services (e.g. trusted time and event logging).

From a networking perspective, ESM can work in conjunction with ArcSight's Network Configuration Manager (NCM) solution to:

- Ensure changes can be applied consistently and vendor agnostically
- Follow the appropriate approval/escalation process and integrate with help desk solutions
- Automatically document changes and audits and report on both
- Seamlessly roll back changes should a problem arise



ArcSight ESM can also ensure that the logs are being collected in a secure method and that critical variables such as time are properly calibrated.

Section 15: Active Defense Strategy

This incorporates prevention, detection, response and recovery. Because prevention safeguards can be defeated, departments have to be able to detect incidents rapidly, respond quickly to contain damage, and recover systems and data in a timely manner.

At the core of detection capabilities is ArcSight ESM which leverages event collection, normalization, categorization, correlation, prioritization, anomaly detection and pattern discovery along with advanced visualization and investigation capabilities to discover security events. Using a mix of real-time events, technical and business-relevant asset information, vulnerability information and other related data points, ArcSight can quickly detect and prioritize malicious activity. Additionally, by using a response solution such as the ArcSight Threat Response Manager (TRM), ArcSight can rapidly respond and contain. For example, the following actions can occur automatically or with human intervention:

- Alert can be created in the form of a page, e-mail, SMS, or help desk ticket
- Asset may be segregated to a quarantined VLAN
- Asset may be blocked at a layer-3 (IP) or layer-2 (MAC)
- User ID may be disabled, blocking logical and/or physical access
- Custom scripts or applications can be executed

Section 16: Prevention

This ranges from physical and storage media security to personnel and data security along with technical safeguards.

In order to achieve return on investment for preventative solutions, they must be leveraged with an extensible monitoring solution. For example, in addition to traditional assets, many ArcSight customers use ESM for physical and telephony monitoring and proprietary and legacy solutions. This ensures that the value the preventative measures are providing doesn't stop at prevention, but also integrates in the overall monitoring strategy.

Section 17: Detection

This consists of determining everything from denial-of-services attacks and system performance anomalies to attempts to gain unauthorized access and unknown attacks. Security audit logs for all IT systems are the minimum requirement.

Incident detection is a cornerstone of ArcSight's solution; ArcSight ESM's powerful analytic capabilities are designed for monitoring in the most demanding environments. The capabilities of ArcSight ESM are equally applicable to perimeter security, insider threats, and regulatory compliance. Additionally, ArcSight is engineered for use with both real-time and forensic data.

Section 18: Response and Recovery

This contains provisions for incident response coordination, identification, prioritization, reporting, recovery and post-incident analysis.

By using ArcSight as the focal point within an organization's security strategy, event collection, analysis and response can be leveraged through a single solution. Having prioritized output linked to the flexible network response and configuration capabilities allows for increased operational efficiencies, reduced risk, and greater return on investment. Finally, ArcSight's built-in incident collaboration, case management, reporting and integration with third party help desk solutions makes it an obvious choice for end-to-end incident management before, during and after an incident.

About ArcSight

ArcSight, a leader in Security and Network Information Management, delivers mission-critical solutions for security, network and IT operations that enable enterprises to turn operational data into action. ArcSight solutions address today's complex enterprise networks that span multiple organizations and corporate business initiatives. By comprehensively collecting, analyzing, managing and responding to security and network data, ArcSight solutions mitigate information risk for real-time threat management, compliance reporting and automated network response. ArcSight's customer base includes leading global enterprises, government agencies and MSSPs.

ArcSight, Inc.

5 Results Way, Cupertino, CA 95014, USA
www.arcsight.com
email: info@arcsight.com

Corporate Headquarters: 408 864 2600
EMEA Headquarters: +44 870 351 6510
Asia Pac Headquarters: 852 2166 8302

© 2007 ArcSight, Inc. All rights reserved. ArcSight, ArcSight ESM and ArcSight TRM are trademarks of ArcSight, Inc. All other product and company names may be trademarks or registered trademarks of their respective owners. 03/07