RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

CHANGE

Challenge today's security thinking

SESSION ID: SPO-R06A

Obtaining Enterprise Cyber-situational Awareness

Eric J. Eifert

Sr. Vice President
Managed Security Services
DarkMatter

Agenda

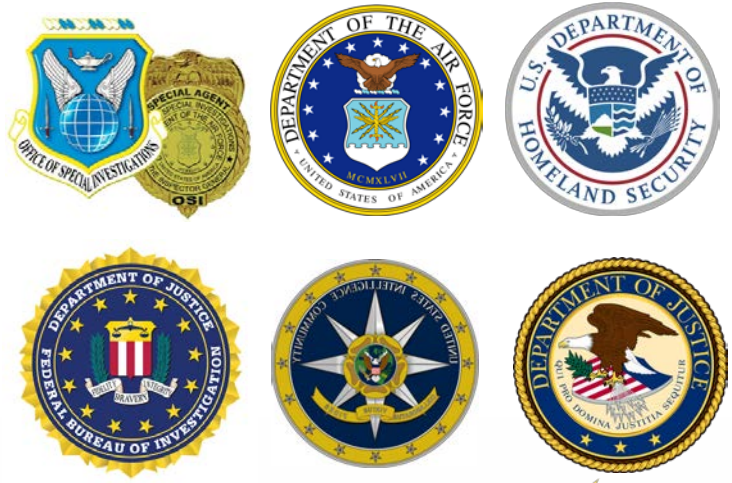
- My Background
- Key components of the Cyber Situational Awareness - What ?
- Key rationale for Cyber Situational Awareness - Why ?
- Implementing Cyber Situational Awareness - How ?
- Final Takeaway

Agenda

- My Background
- Key components of the Cyber Situational Awareness - What ?
- Key rationale for Cyber Situational Awareness - Why ?
- Implementing Cyber Situational Awareness - How ?
- Final Takeaway

My Background

- Over 20 years experience in Cyber Security
  - Special Agent investigating cyber crime and computer intrusions
  - Program Manager for large U.S. Cyber Security Operations Centers
  - Executive running cyber security line of business ($125+M)
- Adjunct professor teaching graduate students cyber investigations



DARKMATTER

GEORGE MASON UNIVERSITY

Agenda

- My Background
- Key components of the Cyber Situational Awareness - What ?
- Key rationale for Cyber Situational Awareness - Why ?
- Implementing Cyber Situational Awareness - How ?
- Final Takeaway

What is Cyber Situational Awareness?

Visibility

At the most basic level it is having true visibility across your own environment

- Knowing what is on your network…
- Knowing how your network is configured…
- Knowing who is on your network…

Intelligence

At an intermediate level it is understanding external influences and their relevance to your environment

Integration

At an advanced level it is the integration of all this information to allow continuous monitoring and rapid decision making

Agenda

- My Background
- Key components of the Cyber Situational Awareness - What ?
- Key rationale for Cyber Situational Awareness - Why ?
- Implementing Cyber Situational Awareness - How ?
- Final Takeaway

Why Visibility

Visibility Type	Rationale
Hardware	Knowing what hardware is in the environment as well as when new hardware is introduced to the environment allows you to ensure they conform with your secure baseline and are authorized devices
Software	Software vulnerabilities, bugs and security updates are common, knowing if you are vulnerable and rapidly resolving your vulnerable state is critical
Configuration	Maintaining a secure configuration baseline is important to prevent unauthorized access and subversion of defenses
Identity and Access	Confirming the identity of authorized users as well as ensuring they have access to the appropriate resources and data sources
Data	Knowing what data within your organization is sensitive allows you to focus your resources on what is most important

Practical Examples

- On 23 Sep 2015 Cisco released a new version of its IOS Software to resolve a critical RSA-Based User Authentication Bypass Vulnerability
  - How quickly could you determine 1) if you had a vulnerable Cisco device on your network and 2) was it configured to use RSA-Based User Authentication?
- Firefox 41 fixes 30 vulnerabilities
  - Can you quickly determine who is impacted?

Why Intelligence

Intelligence Type	Rationale
Vulnerabilities	Understanding what vulnerabilities exist within your environments as well as when new vulnerabilities are discovered allows for rapid remediation
Threat Actors	Understanding the types of adversaries targeting you and their motivation helps to focus resources and security investments
Adversarial Capabilities	Up to date knowledge of the specific tactics, techniques, procedures, and technologies being used by an adversary allows for better detection
Government	Government agencies have access to rich threat intelligence that can be leveraged to gain better insight into the threat landscape
Industry	Industry peer groups can provide insight into sector specific cyber threats as well as share lessons learned to increase your security posture

Why Integration

Integration Type	Rationale
Diverse Technology	Proper integration of diverse technologies reduces the potential for the introduction of security weaknesses
Legacy Technology	Legacy applications running on insecure hardware and software need to be known and mitigated through other means
Logs and Diagnostics	Diverse log and diagnostic formats can make it difficult to leverage the content for decision making
Visualization	Aggregation of information into a dashboard for decision makers helps prioritize and speed up the decision making process
Automation	Acting at the speed of cyber to mitigate issues reduces the potential of cyber events

Agenda

- My Background
- Key components of the Cyber Situational Awareness - What ?
- Key rationale for Cyber Situational Awareness - Why ?
- Implementing Cyber Situational Awareness - How ?
- Final Takeaway

How to increase visibility (1/2)

- Obtain leadership support for a continuous monitoring program focused on people, process, and technology
- Deploy hardware asset management technologies that will provide a comprehensive list of technologies deployed and monitor changes
- Deploy software asset management technologies that will provide a comprehensive list of software installed and on which devices
- Deploy configuration management technologies that will provide a comprehensive list of the secure configurations across all devices
- Deploy a vulnerability management capability to understand the vulnerable state of the enterprise on an ongoing basis

How to increase visibility (2/2)

- Implement an Identity and Assess Management capability that will allow you to understand who is accessing the environment, from where, and with what privileges
- Conduct information and data discovery to understand what type of sensitive information is within your environment, where it is stored, and in what format
- Deploy technologies that will provide you access to full content network traffic (internal and external) for advanced analysis
- Develop a dashboard that will consolidate and correlate data feeds to provide decision makers with full visibility into the environment

How to increase your intelligence

- Monitor feeds from the technology vendors utilized within your environment to obtain vulnerability information
- Receive feeds from vulnerability research firms to stay current on discovered vulnerabilities and bugs that can be exploited
- Obtain information from cyber threat intelligence providers
- Develop partnerships with government information sharing organizations to send and receive threat information
- Develop partnerships with industry peers to share threat information between similar organizations

How to better integrate

- Understand the technology landscape within the organization and influence the roadmap with an focus on better integration
- Attend user conferences to obtain best practices from other organizations with similar environments
- Understand the Application Program Interfaces (APIs) of the technologies in use and how to leverage it for integration purposes
- Understand the format of data feeds and how to normalize the information into a common useable format
- Develop an integration laboratory to test configurations and integrations prior to deployment

Agenda

- My Background
- Key components of the Cyber Situational Awareness - What ?
- Key rationale for Cyber Situational Awareness - Why ?
- Implementing Cyber Situational Awareness - How ?
- Final Takeaway

Final takeaway

- Ultimate goal is to increase your cyber security and rapidly detect, inform, and respond to reduce the probability of a successful cyber security event

- Evaluate your organization's maturity across visibility, intelligence, and integration

- Consider performing a formal gap assessment to determine what is necessary to achieve your desired cyber situational awareness

Questions?