27th ANNUAL FIRST CONFERENCE BERLIN
14-19 JUNE 2015

Defining and Measuring Capability Maturity for Security Monitoring Practices

Eric Szatmary

Dell SecureWorks Incident Response and Digital Forensics

Agenda

- Framing the Problem
- Security Monitoring Standards and Practices Crosswalk
- Shared Vision Use Case Development
- Key Event Sources for Security Monitoring
- Assessing Security Monitoring Capability Maturity
- Call to Action

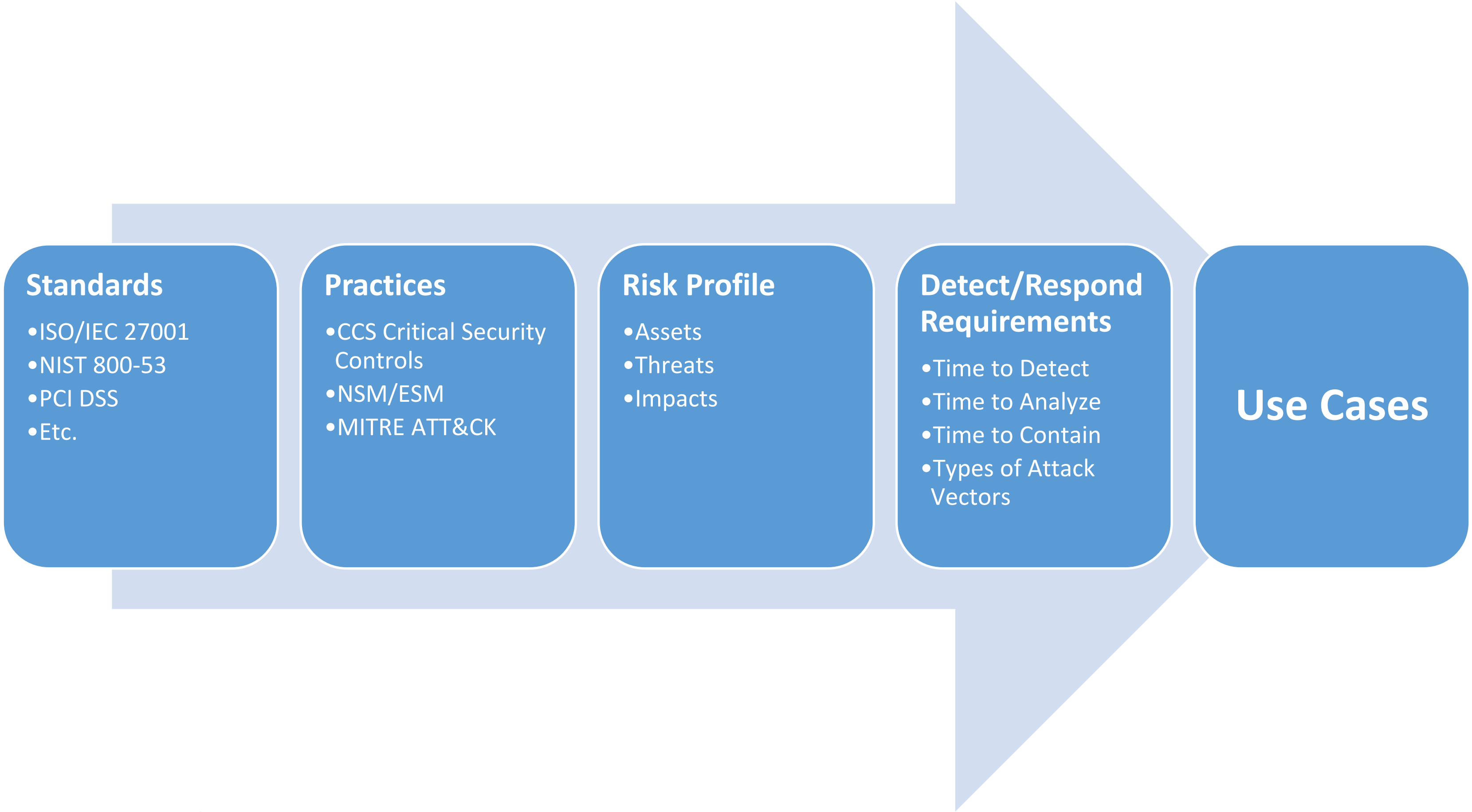
Which Picture Best Describes Your Network?

OR

- Do you centrally retain key logs, especially egress traffic and authentication logs?
- Have you studied your network traffic to know the difference between normal and abnormal?
- Are you hunting for threat actors on your networks, or are you likely the hunted?

For many environments, security monitoring practices are unmeasured and poorly managed

Security Monitoring Factors



Standards

- ISO/IEC 27001
- NIST 800-53
- PCI DSS
- Etc.

Practices

- CCS Critical Security Controls
- NSM/ESM
- MITRE ATT&CK

Risk Profile

- Assets
- Threats
- Impacts

Detect/Respond Requirements

- Time to Detect
- Time to Analyze
- Time to Contain
- Types of Attack Vectors

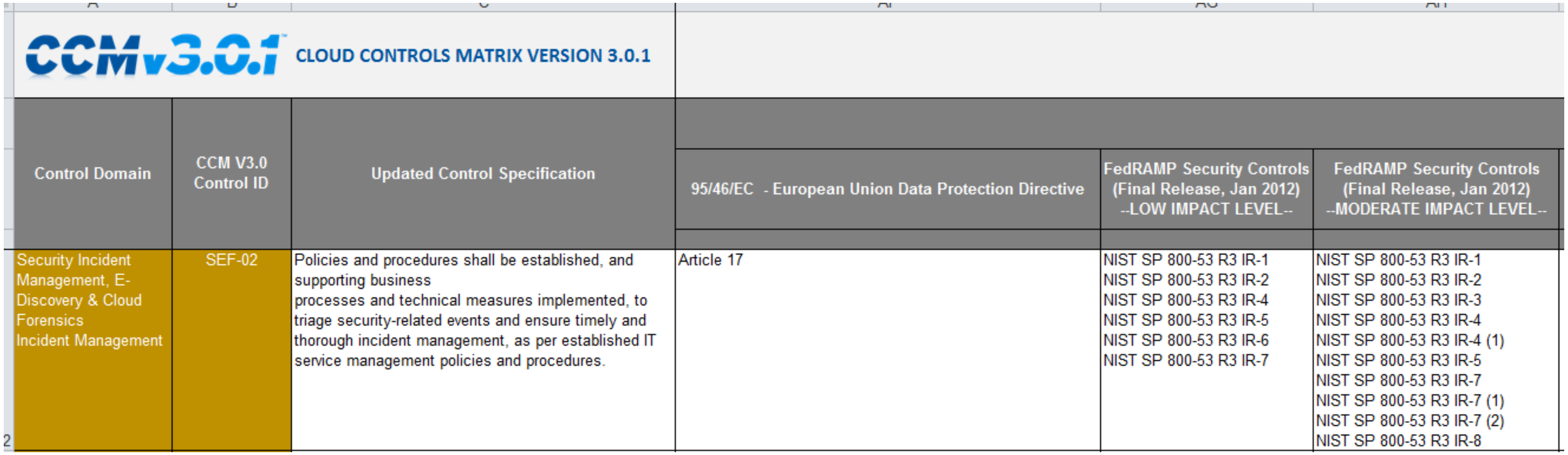
Use Cases

Crosswalking Standards and Practices

Crosswalking Standards

- DHS CRR and NIST CSF provide crosswalks for U.S. oriented control frameworks and regulations
- Cloud Security Alliance Cloud Controls Matrix provides 16 domains cross-walked to other industry-accepted security standards, regulations, and controls frameworks

Example Incident Management Crosswalk



CCMv3.0.1 CLOUD CONTROLS MATRIX VERSION 3.0.1

Control Domain	CCM V3.0 Control ID	Updated Control Specification	95/46/EC - European Union Data Protection Directive	FedRAMP Security Controls (Final Release, Jan 2012) --LOW IMPACT LEVEL--	FedRAMP Security Controls (Final Release, Jan 2012) --MODERATE IMPACT LEVEL--
Security Incident Management, E-Discovery & Cloud Forensics Incident Management	SEF-02	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures.	Article 17	NIST SP 800-53 R3 IR-1 NIST SP 800-53 R3 IR-2 NIST SP 800-53 R3 IR-4 NIST SP 800-53 R3 IR-5 NIST SP 800-53 R3 IR-6 NIST SP 800-53 R3 IR-7	NIST SP 800-53 R3 IR-1 NIST SP 800-53 R3 IR-2 NIST SP 800-53 R3 IR-3 NIST SP 800-53 R3 IR-4 NIST SP 800-53 R3 IR-4 (1) NIST SP 800-53 R3 IR-5 NIST SP 800-53 R3 IR-7 NIST SP 800-53 R3 IR-7 (1) NIST SP 800-53 R3 IR-7 (2) NIST SP 800-53 R3 IR-8

Use these types of tools to help frame conversations with regulatory stakeholders and customize as necessary. Be sure to review the underlying control frameworks for any updates.

ISO/IEC 27001 Controls

- **Limited** number of security monitoring controls and subject to varying interpretations
- Examples:
  - A.12.2 Protection from Malware (**one sub-control**)
  - A.12.4 Logging and Monitoring (**four sub-controls**)

NIST 800-53 Controls

- **Several** security monitoring controls and subject to varying interpretations
- Examples:
  - Audit And Accountability Control Family (**12 sub-controls**)
  - System And Information Integrity Control Family (**three sub-controls**)
  - Incident Response Control Family (**three sub-controls**)

PCI DSS 3.1 Requirements

- **Many** security monitoring related controls and subject to varying interpretations
- Examples:
  - Requirement 10: Track and monitor all access to network resources and cardholder data (**32 sub-requirements**)
  - Requirement 11: Regularly test security systems and processes (**two sub-requirements**)
  - Requirement 12: Maintain a policy that addresses information security for all personnel (**one sub-requirement**)

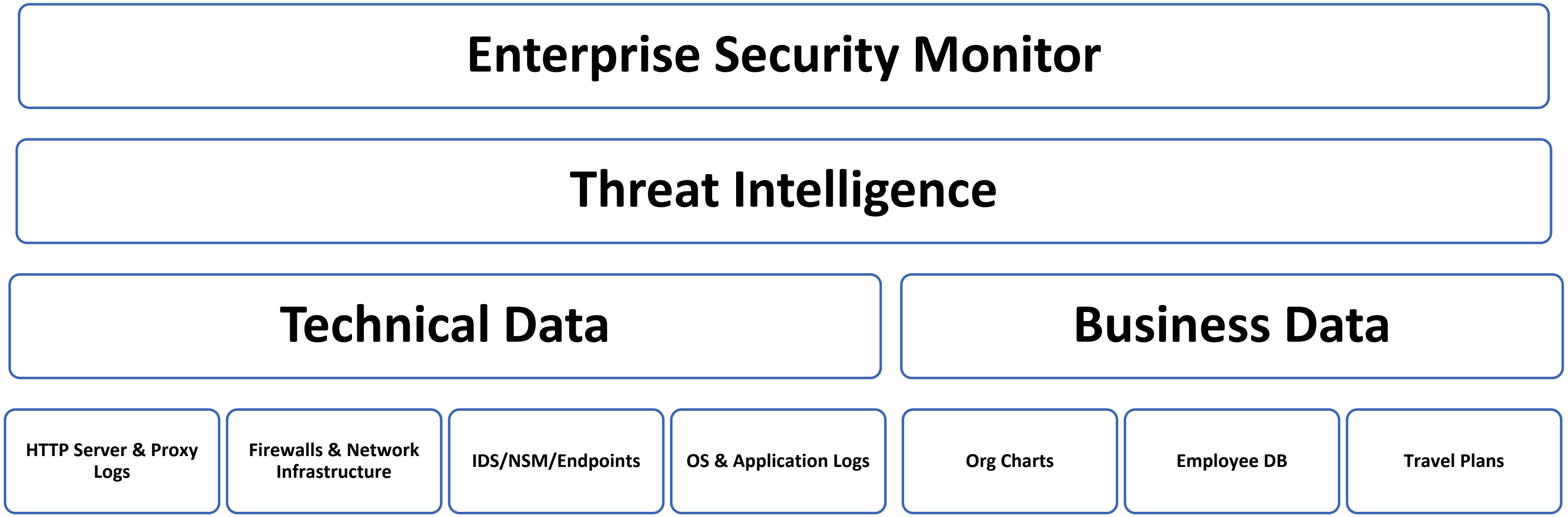
CCS Critical Security Controls

- **Some** security monitoring related controls and subject to varying interpretations
- Examples:
  - CSC 5: Malware Defenses
  - CSC 13: Boundary Defense
  - CSC 14: Maintenance, Monitoring, and Analysis of Audit Logs
  - CSC 16: Account Monitoring and Control
  - CSC 17: Data Loss Prevention
  - CSC 19: Secure Network Engineering

Bejtlich's Network Security Monitoring Framework

- Useful framework for categorizing security monitoring data types:
  - Full content data
  - Extracted content data
  - Session data
  - Transaction data
  - Statistical data
  - Metadata
  - Alert data

Bianco’s Enterprise Security Monitoring Framework



Enterprise Security Monitor

Threat Intelligence

Technical Data

Business Data

HTTP Server & Proxy Logs

Firewalls & Network Infrastructure

IDS/NSM/Endpoints

OS & Application Logs

Org Charts

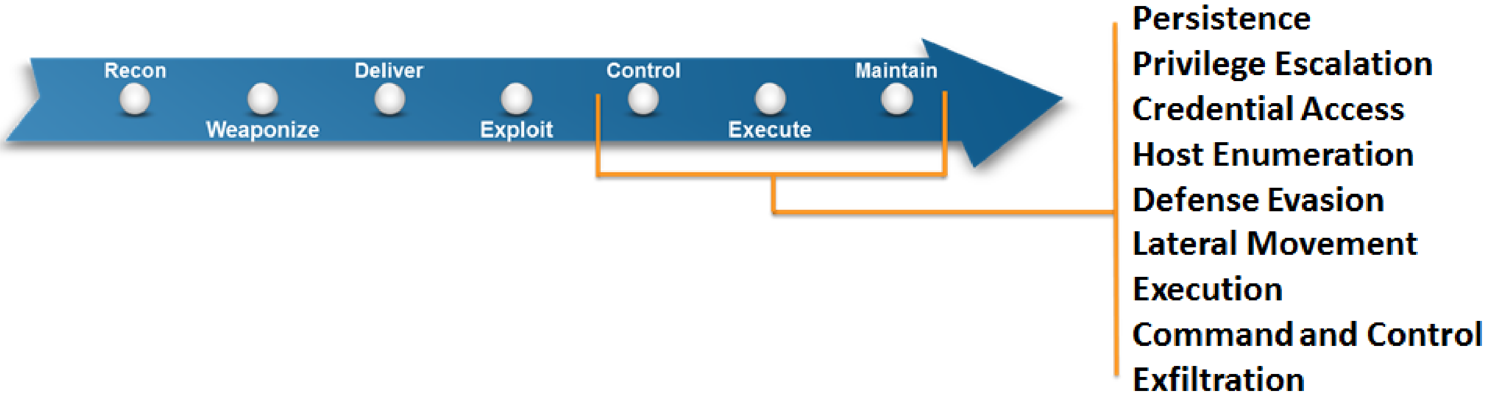
Employee DB

Travel Plans

Useful meta-framework for categorizing all possible monitoring sources within an organization

MITRE ATT&CK Categories

Adversarial Tactics, Techniques, and Common Knowledge



Persistence
Privilege Escalation
Credential Access
Host Enumeration
Defense Evasion
Lateral Movement
Execution
Command and Control
Exfiltration

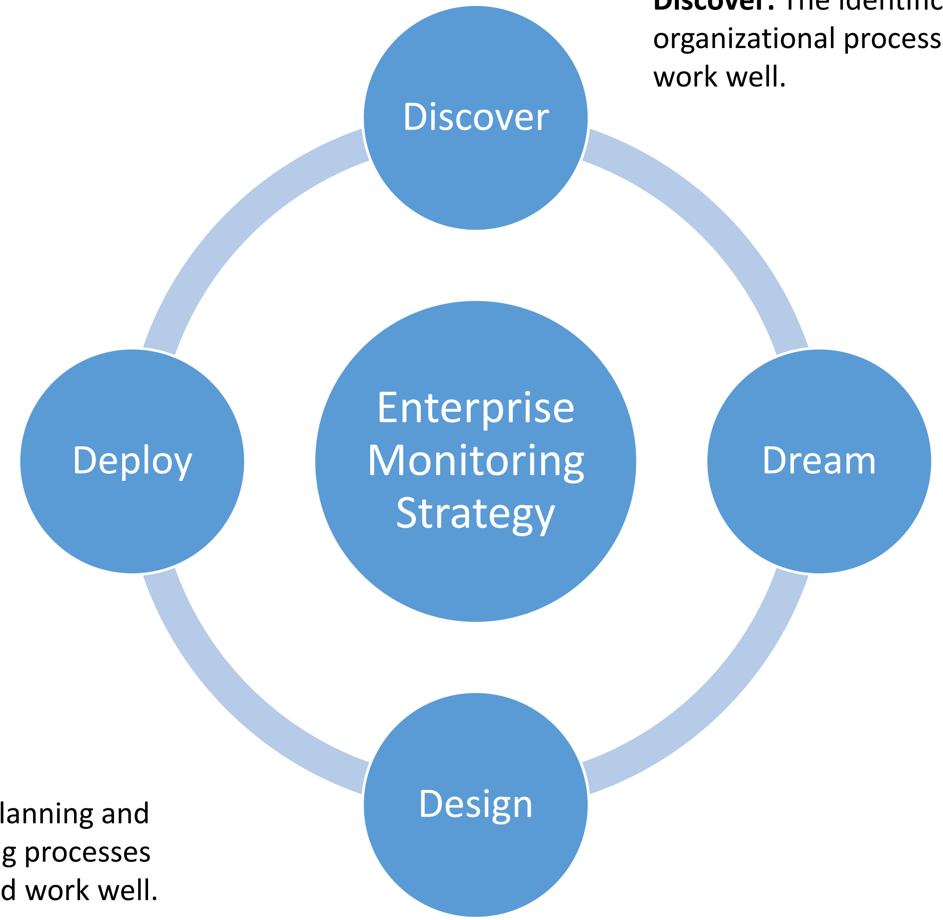
Useful for creating security monitoring use cases based on attack patterns

Defining a Shared Security Monitoring Vision

Appreciative Inquiry

- Appreciative inquiry attempts to use ways of asking questions and envisioning the future in order to foster positive relationships and build on the present potential of a given person, organization or situation.
- The aim is to build – or rebuild – organizations around what works, rather than trying to fix what doesn't.
- Helps establish cross-functional support and define the critical information requirements for enterprise monitoring (compliance, IT operations, privacy, fraud, security)

Appreciative Inquiry 4-D Process



Discover: The identification of organizational processes that work well.

Dream: The envisioning of processes that would work well in the future.

Design: Planning and prioritizing processes that would work well.

Deploy: The implementation (execution) of the proposed design.

Problem Solving vs. Appreciative Inquiry

Problem Solving	Appreciative Inquiry
Felt need, identification of problem(s)	Appreciating - valuing "the best of what is"
Analysis of causes	Envisioning what might be
Analysis of possible solutions	Engaging in dialogue about what should be
Action planning (treatment)	Innovating what will be

Use Case Development

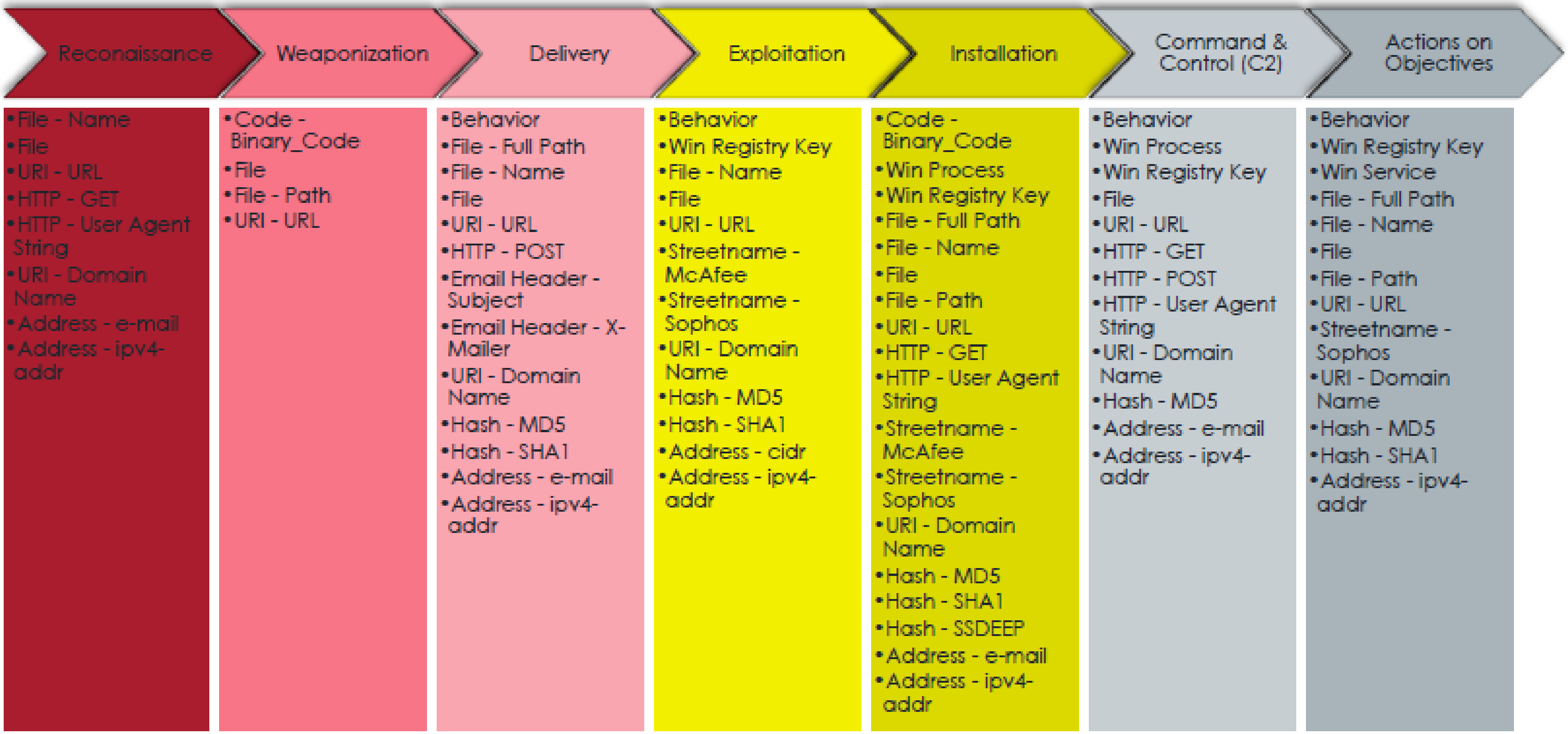
Use Case Characteristics

- Use case name
- Use case objective (assets protected, activity detected)
- Use case triggers (thresholds, attack vectors)
- Use case type (IT operations, cybersecurity, compliance)
- Event sources required
- Use case reporting/analysis solution (alert, search, stacking/risk rarity analysis, ad hoc report, scheduled report)
- Operational processes related to the use case (triggered reviews, associated playbook)
- Anticipated design cost
- Anticipated operational cost
- Test plan
- Priority

Event Source Characteristics

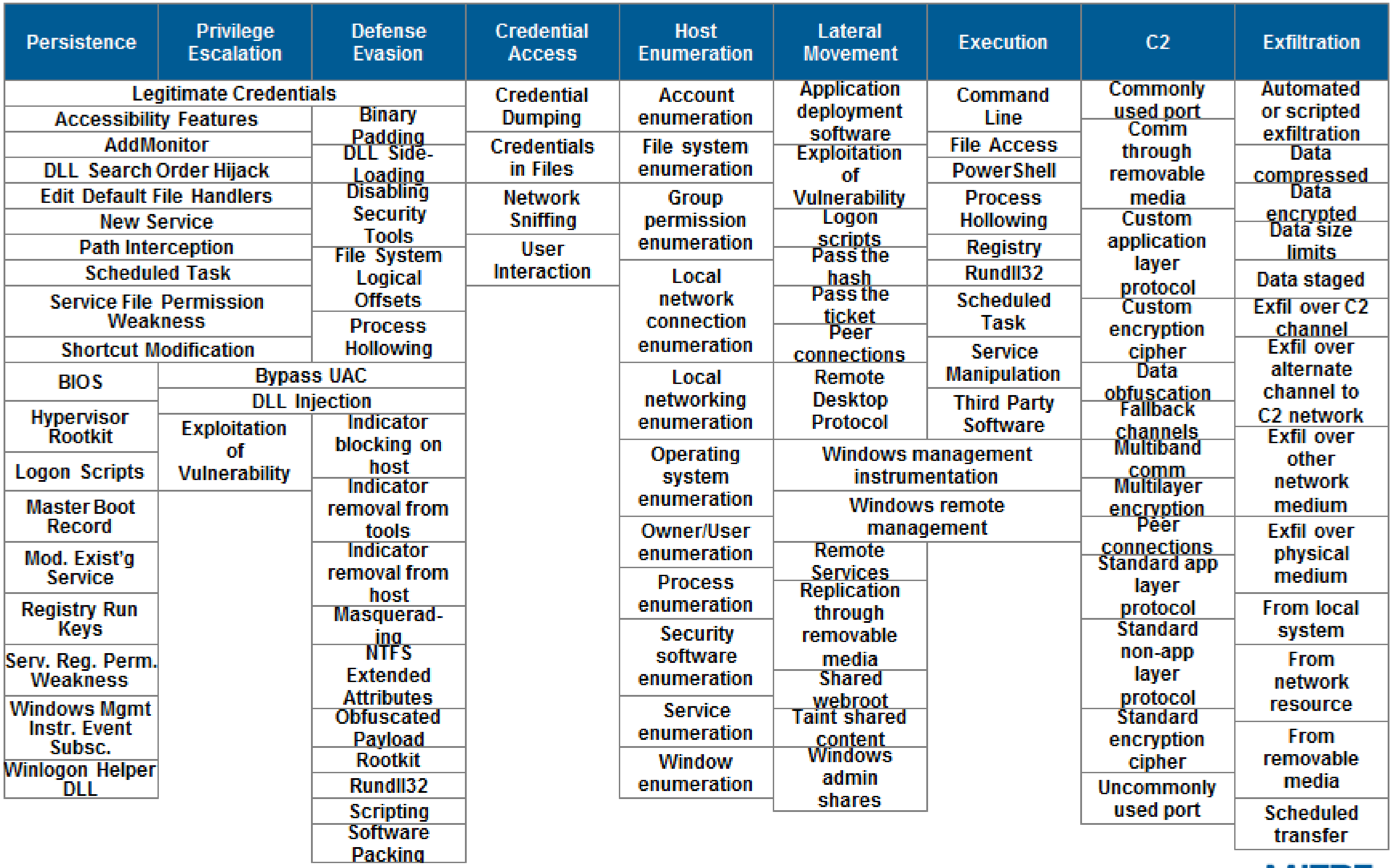
- Event source name
- Event source description
- Event source type (application, IT operations, cybersecurity, compliance)
- Event source data type (alert - full content data)
- Event source fields
- Event source retention requirement (days - months)
- Anticipated event source storage requirement (EPS, GB,TB,PB)
- Event source integration type (syslog, CEF, API)
- Event source logging configurations required
- Priority

Bianco's Enterprise Security Monitoring Detection Attributes



Reconnaissance	Weaponization	Delivery	Exploitation	Installation	Command & Control (C2)	Actions on Objectives
• File - Name • File • URI - URL • HTTP - GET • HTTP - User Agent String • URI - Domain Name • Address - e-mail • Address - ipv4-addr	• Code - Binary_Code • File • File - Path • URI - URL	• Behavior • File - Full Path • File - Name • File • URI - URL • HTTP - POST • Email Header - Subject • Email Header - X-Mailer • URI - Domain Name • Hash - MD5 • Hash - SHA1 • Address - e-mail • Address - ipv4-addr	• Behavior • Win Registry Key • File - Name • File • URI - URL • Streetname - McAfee • Streetname - Sophos • URI - Domain Name • Hash - MD5 • Hash - SHA1 • Address - cidr • Address - ipv4-addr	• Code - Binary_Code • Win Process • Win Registry Key • File - Full Path • File - Name • File • File - Path • URI - URL • HTTP - GET • HTTP - User Agent String • Streetname - McAfee • Streetname - Sophos • URI - Domain Name • Hash - MD5 • Hash - SHA1 • Hash - SSDEEP • Address - e-mail • Address - ipv4-addr	• Behavior • Win Process • Win Registry Key • File • URI - URL • HTTP - GET • HTTP - POST • HTTP - User Agent String • URI - Domain Name • Hash - MD5 • Address - e-mail • Address - ipv4-addr	• Behavior • Win Registry Key • Win Service • File - Full Path • File - Name • File • File - Path • URI - URL • Streetname - Sophos • URI - Domain Name • Hash - MD5 • Hash - SHA1 • Address - ipv4-addr

MITRE ATT&CK Matrix

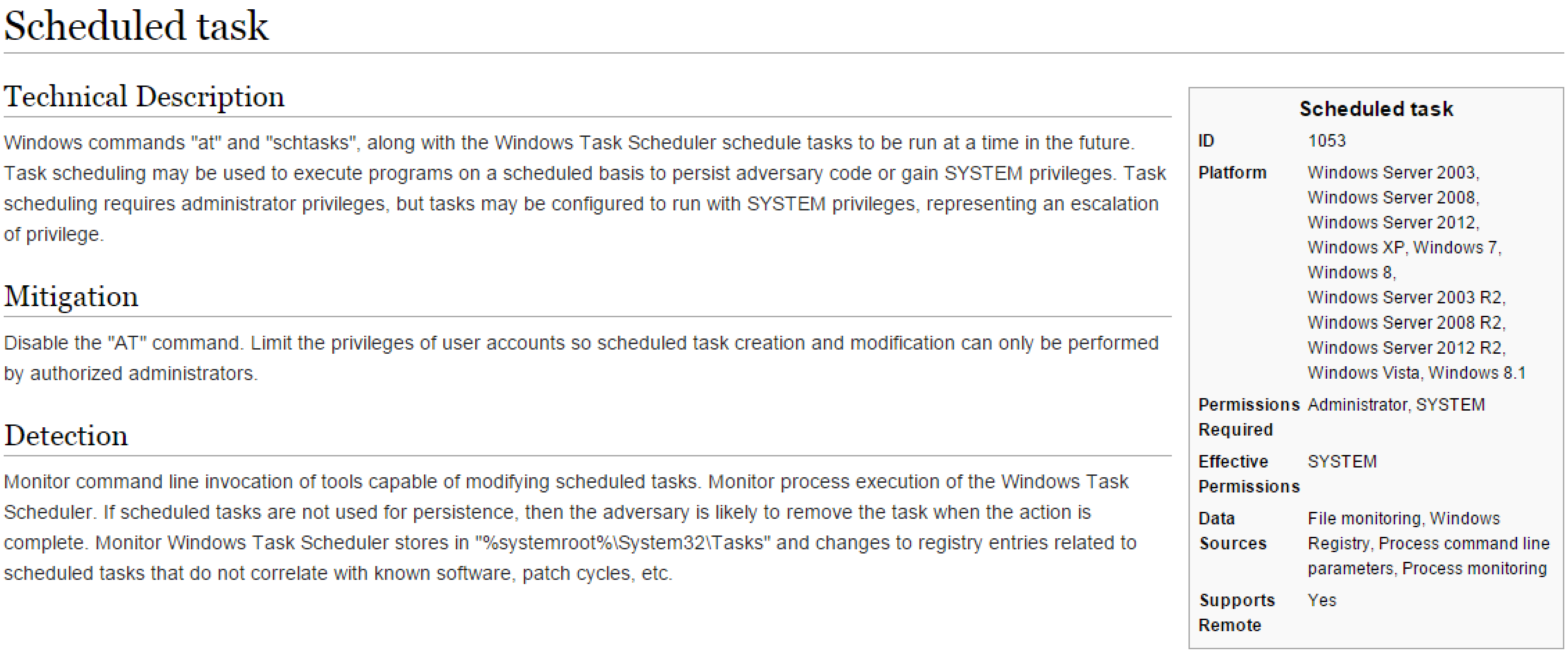


Persistence	Privilege Escalation	Defense Evasion	Credential Access	Host Enumeration	Lateral Movement	Execution	C2	Exfiltration
Legitimate Credentials			Credential Dumping	Account enumeration	Application deployment software	Command Line	Commonly used port	Automated or scripted exfiltration
Accessibility Features		Binary Padding	Credentials in Files	File system enumeration	Exploitation of Vulnerability	File Access	Comm through removable media	Data compressed
AddMonitor		DLL Side-Loading	Network Sniffing	Group permission enumeration	Logon scripts	PowerShell	Custom application layer protocol	Data encrypted
DLL Search Order Hijack		Disabling Security Tools	User Interaction	Local network connection enumeration	Pass the hash	Process Hollowing	Custom encryption cipher	Data size limits
Edit Default File Handlers		File System Logical Offsets		Local networking enumeration	Pass the ticket	Registry	Data obfuscation	Data staged
New Service		Process Hollowing		Operating system enumeration	Peer connections	Rundll32	Fallback channels	Exfil over C2 channel
Path Interception				Owner/User enumeration	Remote Desktop Protocol	Scheduled Task	Multiband comm	Exfil over alternate channel to C2 network
Scheduled Task				Process enumeration		Service Manipulation	Multilayer encryption	Exfil over other network medium
Service File Permission Weakness				Security software enumeration		Third Party Software	Peer connections	Exfil over physical medium
Shortcut Modification				Service enumeration	Windows management instrumentation		Standard app layer protocol	From local system
BIOS	Bypass UAC			Window enumeration	Windows remote management		Standard non-app layer protocol	From network resource
Hypervisor Rootkit	DLL Injection				Remote Services		Standard encryption cipher	From removable media
Logon Scripts	Exploitation of Vulnerability	Indicator blocking on host			Replication through removable media		Uncommonly used port	Scheduled transfer
Master Boot Record		Indicator removal from tools			Shared webroot			
Mod. Exist'g Service		Indicator removal from host			Taint shared content			
Registry Run Keys		Masquerading			Windows admin shares			
Serv. Reg. Perm. Weakness		NTFS Extended Attributes						
Windows Mgmt Instr. Event Subsc.		Obfuscated Payload						
Winlogon Helper DLL		Rootkit						
		Rundll32						
		Scripting						
		Software Packing						

Approved for Public Release; Distribution Unlimited. Case Number 15-1288

MITRE

MITRE ATT&CK Lateral Movement



Scheduled task

Technical Description

Windows commands "at" and "schtasks", along with the Windows Task Scheduler schedule tasks to be run at a time in the future. Task scheduling may be used to execute programs on a scheduled basis to persist adversary code or gain SYSTEM privileges. Task scheduling requires administrator privileges, but tasks may be configured to run with SYSTEM privileges, representing an escalation of privilege.

Mitigation

Disable the "AT" command. Limit the privileges of user accounts so scheduled task creation and modification can only be performed by authorized administrators.

Detection

Monitor command line invocation of tools capable of modifying scheduled tasks. Monitor process execution of the Windows Task Scheduler. If scheduled tasks are not used for persistence, then the adversary is likely to remove the task when the action is complete. Monitor Windows Task Scheduler stores in "%systemroot%\System32\Tasks" and changes to registry entries related to scheduled tasks that do not correlate with known software, patch cycles, etc.

Scheduled task

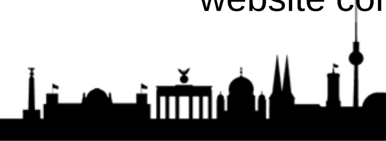
ID	1053
Platform	Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1
Permissions Required	Administrator, SYSTEM
Effective Permissions	SYSTEM
Data Sources	File monitoring, Windows Registry, Process command line parameters, Process monitoring
Supports Remote	Yes

Key Event Sources

- Network flow records (egress router/firewall flow data)
- DNS logs
- VPN (session, RDP, OWA, Citrix) logs
- LDAP logs
- Windows logs (Active Directory, process creation, PowerShell, SysMon, WMI)
- Web proxy logs
- Network/web application firewall logs
- DHCP logs
- IDS/IPS alerts
- AV alerts
- DLP alerts
- SMTP logs
- Apache/IIS web server logs
- Unix/Linux syslog
- System management logs
- Cloud service provider logs
- Ad hoc/rolling full packet captures at network choke points

Sample Use Cases for Detection and Response

- Analyze outbound network traffic to identify compromised systems or exfiltration for a given time period (IP addresses, ports, protocols, bytes transferred, duration, system location)
- Determine which system was assigned a DHCP-issued IP address for a given time period
- Analyze DNS activity to determine which internal systems resolved a particular domain name
- Search authentication logs to determine whether a specific source IP address or username was used
- Analyze VPN, OWA, RDP, and Citrix logs to identify anomalous login activity by geolocation for a given time period
- Analyze authentication logs for anomalous privileged account activity across internal network
- Search for a specific threat indicator across all systems (MD5 hash, path, filenames, extensions, registry keys, scheduled tasks, dual-use admin tools, password dumpers, RAR files)
- Determine whether a particular service was installed and started on any Windows system in the environment
- Analyze SMTP gateway logs to identify rarely seen email domains
- Analyze web proxy logs to determine which systems may have been exposed to malicious website content



Measuring Security Monitoring Effectiveness

Capability Maturity Model Benefits

- Efficient means for assessing and benchmarking performance in an inverted pyramid format for leadership
- Effective for expressing a body of knowledge of best/contextual practices
- Identify gaps and devise improvement plans

SLWG CMM

- In 2012, the U.S. Department of Energy (DOE) and the National Electric Sector Cybersecurity Organization (NESCO) convened a "Security Logging Working Group" (SLWG) to suggest recommended capabilities for security logging.
- SLWG used a six level Capability Maturity Model (CMM) to express an organization's ability to effectively collect and analyze data that might be security significant.
- The SLWG CMM was eventually integrated into the DOE Cybersecurity Capability Maturity Models (C2M2), but remains a very useful model

SLWG CMM Critical Aspects

- **Prerequisite:** defines capabilities that are required to be in place before an organization can start assessment at a particular maturity level.
- **Activity:** provides details on the required activity of the organization in order to affect the desired outcome within the process domain.
- **Integration:** describes the required relationships between the process domain and other external and internal organizational processes.
- **Process:** describes the required documentation of uniform work steps, standards, and policy required for a given maturity level.
- **Staff:** provides details on the required capabilities of staff and other personnel performing activities related to the process domain.
- **Tools:** describes the maturity level of tools and systems used in the execution of the process domain activities.
- **Training:** evaluates the presence and maturity of a training program relevant to the process domain.

SLWG Security Logging CMM Level 0

- **CMM Level 0** (Not Performed)
- **Prerequisite:** None.
- **Activity:** New systems are not configured to log activity. Logging configurations are not consistent and no predefined logging configurations exist. Log analysis/aggregation systems do not exist. Log information is not dependable.
- **Integration:** Logging is not integrated with other business processes.
- **Process:** There are no policies to identify scope and storage of log data. There are no defined processes or standards to ensure consistent logging. The server or device provisioning process does not include log configuration.
- **Staff:** No staff members are dedicated to the logging function.
- **Tools:** No log analysis or log aggregation systems exist. Log tools are not supported by IT. No hardware is dedicated for logging.
- **Training:** Training programs do not exist.

SLWG Security Logging CMM Level 5

- **CMM Level 5** (Continuously Improving)
- **Prerequisite:** All requirements from CMM Levels 1 through 4 must be met.
- **Activity:** An established lifecycle for enhancements to system logging configuration exists. Centralized Integrated logging extends beyond security requirements and collects operational, flow, and activity logs for holistic view of the environment. Log messages are archived and access to log messages is controlled. Logging data is available to all analysts with a need to know.
- **Integration:** Measures of program effectiveness are documented and regularly tested. Tests of related business and security processes include logging as a component. External data sources are regularly reviewed and tested for integration with the logging function. Where appropriate, event data is shared with other business departments.
- **Process:** Efficacy of logging is validated by internal audit and reviewed by top management. Compliance against the log policy is reported regularly. Policies governing access to logging data are documented and regularly audited for compliance. Results of the audits are documented and fed back as proposed improvements to the program.
- **Staff:** Staff redundancy exists to ensure uninterrupted availability of logging components and infrastructure.
- **Tools:** Appropriate storage for long-term retention of logs is in place. Logging solution is a system with high availability requirements and full IT support, including clearly defined Service Level Agreements (SLAs). Tools for logging are reviewed and refined in response to feedback and effectiveness.
- **Training:** Training is uniform across staff members. Even if completed by different analysts, logging configurations for the same type of system or same classification of devices will yield similar (if not exact) results. The training program is documented and integrated into staff performance goals.

SLWG Security Monitoring CMM Level 0

- **CMM Level 0** (Not Performed)
- **Prerequisite:** None.
- **Activity:** Organization's monitoring efforts are ad hoc, not coordinated, and not planned.
- **Integration:** Monitoring is not integrated with other business or security processes, or is not included in/aligned with the organization's incident response plan.
- **Process:** Systems and processes for consistent analysis of data do not exist or are not formalized/standardized.
- **Staff:** Staff members are not dedicated to monitoring function; monitoring is a secondary duty.
- **Tools:** Tools for monitoring are not standardized.
- **Training:** Training programs are informal or do not exist.

SLWG Security Monitoring CMM Level 5

- **CMM Level 5** (Continuously Improving)
- **Prerequisite:** All requirements from CMM Levels 1 through 4 must be met.
- **Activity:** Monitoring is performed around the clock by trained professionals (as evidenced by certification and training programs).
- **Integration:** Monitoring program is recognized and regularly tested as a key component of organization's incident response plans and other relevant business/security processes. Results of testing are fed back as proposed improvements to the program. Measures of program effectiveness are documented and regularly tested.
- **Process:** Concurrent, integrated monitoring of multiple sources is performed, with correlation and aggregation of data with appropriate application of institutional knowledge. Ability to perform ad hoc queries and advanced correlative analysis (both in terms of resources and capability), and to migrate these queries/analyses into regular monitoring cycles within a reasonable period, exists.
- **Staff:** Staff redundancy exists to ensure continuous monitoring. Peer review of analysis prior to release is formalized and encouraged.
- **Tools:** Tools to support monitoring are reviewed and refined in response to feedback and effectiveness.
- **Training:** Training is uniform across monitoring resources. Analysis of the same data by different analysts will yield similar (if not exact) results. Training program is documented and integrated into staff performance goals.

Commonly Observed Security Monitoring Profiles

- Organizations are resource constrained to leverage either open source or commercial solutions
- Organizations are reaching functional/cost limits of commercial solutions they have invested in, but lack resources to use open source solutions
- Organizations are building security monitoring capabilities using open source solutions due to the functional limits/cost of commercial offerings

Conclusion

- Be proactive about taking stock of **all** factors that impact logging and security monitoring strategy
- Emphasize cross-functional, shared vision use cases; constantly measure progress operationally and technically
- Consider participating in the FIRST Network Monitoring and Metrics SIGs to collaborate on security monitoring practices as a global community

Questions?

References

- [CSA CCM] Cloud Security Alliance Cloud Controls Matrix. Retrieved from https://cloudsecurityalliance.org/research/ccm.
- [Appreciative Inquiry] https://en.wikipedia.org/?title=Appreciative_inquiry
- [ISO/IEC 27001:2013] International Organization for Standardization. (2013). Information security management systems (ISO/IEC 27001:2013).
- [NIST SP800-53] National Institute of Standards and Technology, Joint Task Force Transformation Initiative. (2013). Security and Privacy Controls for Federal Information Systems and Organizations (NIST Special Publication 800-53, revision 4)
- [PCI DSS] PCI SSC Data Security Standard v3.1. (2015). Retrieved from https://www.pcisecuritystandards.org/security_standards/documents.php?document=pci_dss_v2-0#pci_dss_v2-0.
- [CCS CSC] Council on CyberSecurity Critical Security Controls. (2014). Retrieved from http://www.counciloncybersecurity.org/critical-controls/.
- [MITRE ATT&CK] MITRE Adversarial Tactics, Techniques, and Common Knowledge. (2014). Retrieved from https://attack.mitre.org.
- [NSM] Practice Of Network Security Monitoring. Understanding Incident Detection and Response by Richard Bejtlich. (2013). Retrieved from http://www.nostarch.com/nsm.
- [ESM] Enterprise Security Monitoring: Comprehensive Intel-Driven Detection. (2014). Retrieved from https://www.first.org/resources/papers/conference2014/first_2014_-_bianco-_david_-_enterprise_security_monitoring_20140610.pdf.
- [NESCO Logging] Bromberger, S., & Maschino, C. (2012). Security logging in the utility sector: Roadmap to improved maturity. National Electric Sector Cybersecurity Organization, Southern California Edison. Retrieved from https://www.bromberger.com/pubs/SecurityLoggingCMM1.0.pdf.