Operational Enterprise Security

**Desert Schools Federal Credit Union**

**148 N. 48th Street Phoenix, AZ 85034**

**602.334.6000**

**3/23/2015**

Brent E. Chambers

There is an ever-growing need to continuously collect and analyze enterprise-wide security data in order to effectively manage information risk and prevent data breaches. Given the dynamic nature of modern threats, enterprise security operations should be able to quickly assess and gauge security posture in real-time. This document outlines the techniques, tactics, procedures and tools to further implement network and continuous security monitoring practices throughout the enterprise network.

Table of Contents (“Is this a ‘real’ table of contents?” –MM ‘15)

[Abstract: 3](#_Toc415574001)

[Introduction: 5](#_Toc415574002)

[Definitions: 6](#_Toc415574003)

[Asset Zones 7](#_Toc415574004)

[Defense Domains (OES Framework) 8](#_Toc415574005)

[Deployed Systems 8](#_Toc415574006)

[Enterprise Security Architecture Map 10](#_Toc415574007)

[Deployed Security System Descriptions 11](#_Toc415574008)

[Nessus 11](#_Toc415574009)

[Solar Winds Log and Event Manager (LEM) 12](#_Toc415574010)

[IBM Managed Security Services (MSS) 13](#_Toc415574011)

[RSA Data Loss Prevention Tool 14](#_Toc415574012)

[IDS Sensors 15](#_Toc415574013)

[FireEye 16](#_Toc415574014)

[Automation Task Table 18](#_Toc415574015)

[Security Templates and Documentation 19](#_Toc415574016)

[Proactive Security Operations 20](#_Toc415574017)

[Continuous Security Monitoring 21](#_Toc415574018)

[Network Security Monitoring 22](#_Toc415574019)

[NSM Tool Cannon: 24](#_Toc415574020)

[Daily Operations Reporting 25](#_Toc415574021)

[Weekly Operations Reporting 26](#_Toc415574022)

[Monthly Operations Reporting 27](#_Toc415574023)

[ISRAB Report (Quarterly) 28](#_Toc415574024)

[Enterprise Security Services 29](#_Toc415574025)

[In-Depth Tactics and Procedures 30](#_Toc415574026)

Abstract:

The ever-evolving security risk landscape requires a new approach to information security management. Traditional security management teams and practices in the enterprise are generally understaffed and fragmented, leading to visibility gaps and thus opportunities for targeted attacks and data breach. Due to the increasing complexity of modern IT environments, system compromise is inevitable whereas comprehensive management, critical monitoring and proactive assessments are necessary for not only developing an overall enterprise-wide view of risk and security posture, but to detect points-of-entry and unauthorized activity before it results in the loss of sensitive and/or critical data.

\\phx.dsfcu.local\engineering\Enterprise Services\Projects

Introduction:

Operational Enterprise Security (OES) is a metric and deliverable-driven program based around continuous security monitoring (CSM), network security monitoring (NSM) and repeatable security process delivery (RSPD) in and throughout the enterprise data network. Because the core components of network infiltration and data compromise can be simplified to unauthorized network communication and unauthorized program execution, specific operational tasks to detect points-of-entry and indicators of compromise (IOC) can be derived from CSM, NSM and RSPD.

Continuous Security Monitoring (CSM) is the proactive assessment of system integrity (data at rest: workstation and server log files, registry keys and system configurations) in order to identify static IOC’s. Network Security Monitoring (NSM) is the active analysis of real-time network communication (data in motion) to detect network-wide anomalies and malicious activity. In order to identify compromised systems that may lead to data breach or data loss, NSM practices promote the standardization of communication and configurations, constant advances in network visibility for anomaly detection, and application layer transmission analysis. Repeatable Security Process Delivery (RSPD) is the concept that all security operations tasks and procedures as well as offensive assignments and engagements should be documented procedurally, in order to be performed in a repeatable manner where results are generated and delivered through consistent means. In order to ensure consistent reporting and delivery, RSPD promotes the creation and use of document templates to maintain a level of cohesiveness when work is complete.

While the general implementation of OES practices is to defend enterprise network information systems, offensive assignments and engagements must be incorporated into operations to identify publicly available enterprise intelligence, publicly exploitable vulnerabilities and points of entry, enterprise network attack paths, as well as poorly deployed or misconfigured internal systems. The process and exploitation of information systems occurs through the concept of a “kill chain”. The kill chain defines each general step of an attack, from reconnaissance through delivery, to command and control and ultimately action, leading to exfiltration (data loss or theft).



The first steps of an attack kill chain can be actively identified by OES teams that implement offensive tactics to perform actions attackers would take to discover and detected by leaves behind or generates static and/or mobilized indicators of compromise. A large portion of IOC’s typically go unnoticed unless they are explicitly searched for and identified for analysis. Once an intruders intent and methodology are understood, system compromise can be detected before sequential steps in an attack can be carried out, ultimately thwarting an attack before data exfiltration. Effective CSM eliminates links in attack kill chains.

Definitions:

* 1. **Attack kill-chain:** the different stages of a planned cyber attack
  2. **DS Defense Domain:** One of 9 essential areas of defense
  3. **Enterprise Network:** A private network uses by a business to connect assets and share resources
  4. **Indicator of Compromise (IoC):** An artifact or event that indicates a computer intrusion
  5. **Kill-chain:** A pattern of transactional activities that are linked together in order for an act (usually malicious) takes place
  6. **Posture Report:** A deliverable that provides a snapshot of various Defense Domain metrics
  7. **Private Network:** A network segmented from the Internet
  8. **Public Network:** A generally accessible network for information and technology resources

Asset Zones

To uniquely identify enterprise network locations, separate homogenous assets into logical groups. Asset zones in the Desert Schools FCU enterprise network, as of Spring 2015, is topographically flat, consisting of four primary asset zones: Server, DMZ, User and Branch. These four primary asset zones can be further defined, however due to the overall reachability of all enterprise hosts and network segments, it is recommended that increased granularity coincide with actively implemented layer 2 or layer 3 network segmentation policies.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Server Asset Zone | DMZ Asset Zone | User Asset Zone | Branch Asset Zone |
| Description/Contents: | Backbone systems, production and failover servers, switches/blades, internal databases, core banking systems, some dev/qa systems | Perimeter systems (publicly reachable), DMZ middleware systems and databases, B2B nodes | Papago and Camelback Plaza workstations (LAN & Wireless) | Workstations and Servers on all branch office network segments |
| IP Range(s): | |  |  | | --- | --- | | 10.1.0.0/24  10.1.1.0/24  **10.1.2.0/24**  **10.1.3.0/24**  10.1.4.0/24  10.1.5.0/24  10.1.6.0/24  10.1.7.0/24 | 10.1.8.0/24  10.1.9.0/24  10.1.11.0/24  10.1.12.0/24  10.1.13.0/24  10.1.47.0/24  10.1.48.0/24  10.1.49.0/24 | | |  |  | | --- | --- | | Pub: 65.89.28.0/24  Pub: 207.224.246.0/24  **192.168.200.0/24**  192.168.100.0/24 | 192.168.150.0/24  192.168.175.0/24  192.168.75.0/24  192.168.50.0/24 | | |  |  | | --- | --- | | 10.1.101.0/24  10.1.111.0/24  10.1.121.0/24  10.1.131.0/24  10.1.141.0/24  10.1.151.0/24 | 10.1.161.0/24  10.1.171.0/24  10.1.150.0/24  10.1.15.0/24  10.1.16.0/24 | | 10.176.0.0/16  10.177.0.0/16  10.178.0.0/16  10.179.0.0/16 |
| Threats: | The Server zone contains critical business systems and databases which are considered high value and certainly worthwhile targets. The 10.1.2.0/24, and 10.1.3.0/24 network ranges are the primary segments for the majority of DSFCU critical servers and should be monitored for unauthorized and irregular access, unauthorized outbound communication, and unauthorized execution. Servers should share the same baseline configuration to aid in the detection of Indicators of Compromise. | The DMZ Asset zone contains standard public facing systems (Web, Mail, Name Server, VPN, etc.) that are constantly subjected to attacks from the public Internet. While attacks on the DMZ happen often, they are rarely successful. Public DMZ systems should be scanned constantly for new vulnerabilities. Middleware DMZ systems should be monitored for unauthorized and irregular logins, at the least. | Hosts in the User Asset zone are primarily workstations with users, respectively. Workstations and outdated/vulnerable client-side vulnerabilities are top targets for advanced attackers. Phishing attempts that rely on vulnerable client-side software will fail if software and systems are patched aggressively. Users also need persistent security education. | Similar to the User Asset zone, the Branch Asset zone primarily consists of workstations (at branches) with users.  Users at branches are just as susceptible to phishing attacks as users anywhere else on the network. |
| Notes: | * All traffic originating from the Server Asset Zone can be sniffed from the Papago Snort Sensor. * Interactive login activity on hosts in the Server Zone is relatively rare and should be reviewed on a continuous basis. * Servers have the ability to communicate outbound to the internet on all TCP ports besides 443 and 80. | * Public facing DMZ hosts with vulnerabilities should be top priority. * Traffic traversing DMZ segments should be audited and analyzed for clear-text communication. DMZ systems should not be communicating without encryption. | * The introduction of host-based firewall and application whitelisting will eliminate the majority of potential unauthorized execution. * The User Asset zone is an excellent starting point for proactive IoC detection (hunting). | * All Branch Asset zone network traffic can be sniffed from the Papago Snort sensor. |

Defense Domains (OES Framework)

The OES framework consists of the operationalization, data collection automation, management, administration, and reporting of 9 separate enterprise defense domains. The operationalization of each defense domain takes a top down approach that begins with a primary domain metric. Tools used for each domain are to be determined by overall OEM team platform familiarity and skill sets. The OES framework simplifies generating initial operational security metrics where gaps become visibility apparent and remediation or improvement work can be quickly assigned. Generating initial operational security metrics will also aid in overall domain anomaly detection as well as reporting upon and presenting enterprise security posture.

|  |  |  |
| --- | --- | --- |
| Domain | Description | Primary Domain Metric(s) |
| Vulnerability Management | The detection of vulnerabilities, misconfigurations and points of entry. | # of easily exploitable sys |
| Patch Management | The detection of missing and required patches. | % of unpatched systems |
| Event Management | The management of deployed systems producing system logs/events. | Uptime, Availability |
| Incident Management | The management of escalated indicators of compromise. | # of incidents, % resolved |
| Malware Detection | Proactive enterprise ‘hunting’ for unauthorized execution and comm | #,% of infected systems |
| Asset Management | The real-time awareness of deployed inventory, activity and access | #deployed sys, logins |
| Configuration Management | The continuous improvement and comparison of standardized configs | % baseline compliant |
| Network Management | The management of network traffic control. | # of unauthorized traffic |
| Information Management | The detection and management of sensitive data throughout the network | % of unauthorized sensitive data storage |

Deployed Systems

The following systems are mapped to the 9 DS Defense Domains. ISP Standards should be used to define audit and proactive assessment procedures in order to generate accurate posture reports.

|  |  |  |  |
| --- | --- | --- | --- |
| Domain | Tools/Software | Operational Metric / Measurement | Standard Documentation |
| Vulnerability Management | Nessus | Which systems are remotely exploitable?  Which hosts/vulnerabilities should be targeted next? | [IT-ISP04 Vulnerability Management](https://wiki.desertschools.cure/wiki/it/Sec/_layouts/WordViewer.aspx?id=/wiki/it/Sec/Shared%20Documents/Information%20Security%20Policy%20ISP/ISP%20Supporting%20Standards/IT-ISP04%20Vulnerability%20Management%20Standard.doc&Source=https%3A%2F%2Fwiki%2Edesertschools%2Ecure%2Fwiki%2Fit%2FSec%2FShared%2520Documents%2FForms%2FAllItems%2Easpx%3FRootFolder%3D%252Fwiki%252Fit%252FSec%252FShared%2520Documents%252FInformation%2520Security%2520Policy%2520ISP%252FISP%2520Supporting%2520Standards&DefaultItemOpen=1&DefaultItemOpen=1) |
| Patch Management | SCCM, Nessus | Which systems are missing critical or security updates? | [IT-ISP05 Configuration Management](https://wiki.desertschools.cure/wiki/it/Sec/_layouts/WordViewer.aspx?id=/wiki/it/Sec/Shared%20Documents/Information%20Security%20Policy%20ISP/ISP%20Supporting%20Standards/IT-ISP05%20Configuration%20Management.docx&Source=https%3A%2F%2Fwiki%2Edesertschools%2Ecure%2Fwiki%2Fit%2FSec%2FShared%2520Documents%2FForms%2FAllItems%2Easpx%3FRootFolder%3D%252Fwiki%252Fit%252FSec%252FShared%2520Documents%252FInformation%2520Security%2520Policy%2520ISP%252FISP%2520Supporting%2520Standards&DefaultItemOpen=1&DefaultItemOpen=1) |
| Event Management | LEM, MSS | Which systems are not configured for centralized log collection?  How are Events of the same group responded to?  What is the process for promoting events to alerts, and alerts to ISERTFR notifications? | [IT-ISP07 Incident Response Standard](https://wiki.desertschools.cure/wiki/it/Sec/_layouts/WordViewer.aspx?id=/wiki/it/Sec/Shared%20Documents/Information%20Security%20Policy%20ISP/ISP%20Supporting%20Standards/IT-ISP07%20Incident%20Response%20Standard.docx&Source=https%3A%2F%2Fwiki%2Edesertschools%2Ecure%2Fwiki%2Fit%2FSec%2FShared%2520Documents%2FForms%2FAllItems%2Easpx%3FRootFolder%3D%252Fwiki%252Fit%252FSec%252FShared%2520Documents%252FInformation%2520Security%2520Policy%2520ISP%252FISP%2520Supporting%2520Standards&DefaultItemOpen=1&DefaultItemOpen=1)  [IT-ISP07.1 Incident Handling Procedures](https://wiki.desertschools.cure/wiki/it/Sec/_layouts/WordViewer.aspx?id=/wiki/it/Sec/Shared%20Documents/Information%20Security%20Policy%20ISP/ISP%20Supporting%20Standards/IT-ISP07.1%20Incident%20Handling%20Procedures.docx&Source=https%3A%2F%2Fwiki%2Edesertschools%2Ecure%2Fwiki%2Fit%2FSec%2FShared%2520Documents%2FForms%2FAllItems%2Easpx%3FRootFolder%3D%252Fwiki%252Fit%252FSec%252FShared%2520Documents%252FInformation%2520Security%2520Policy%2520ISP%252FISP%2520Supporting%2520Standards&DefaultItemOpen=1&DefaultItemOpen=1)  [IT-ISP07.2 Incident Response Procedures](https://wiki.desertschools.cure/wiki/it/Sec/_layouts/WordViewer.aspx?id=/wiki/it/Sec/Shared%20Documents/Information%20Security%20Policy%20ISP/ISP%20Supporting%20Standards/IT-ISP07.2%20Incident%20Response%20Procedures.doc&Source=https%3A%2F%2Fwiki%2Edesertschools%2Ecure%2Fwiki%2Fit%2FSec%2FShared%2520Documents%2FForms%2FAllItems%2Easpx%3FRootFolder%3D%252Fwiki%252Fit%252FSec%252FShared%2520Documents%252FInformation%2520Security%2520Policy%2520ISP%252FISP%2520Supporting%2520Standards&DefaultItemOpen=1&DefaultItemOpen=1) |
| Incident Management |  | How many incidents were reported in X amount of time?  How many reported incidents are resolved?  …still in progress?  How many incident reports were drafted in X amount of time? |
| Malware Detection | Sophos, FireEye | Which systems do not have Anti-Virus detection deployed?  Which systems do not have up-to-date AV signatures? | [IT-ISP05 Configuration Management](https://wiki.desertschools.cure/wiki/it/Sec/_layouts/WordViewer.aspx?id=/wiki/it/Sec/Shared%20Documents/Information%20Security%20Policy%20ISP/ISP%20Supporting%20Standards/IT-ISP05%20Configuration%20Management.docx&Source=https%3A%2F%2Fwiki%2Edesertschools%2Ecure%2Fwiki%2Fit%2FSec%2FShared%2520Documents%2FForms%2FAllItems%2Easpx%3FRootFolder%3D%252Fwiki%252Fit%252FSec%252FShared%2520Documents%252FInformation%2520Security%2520Policy%2520ISP%252FISP%2520Supporting%2520Standards&DefaultItemOpen=1&DefaultItemOpen=1) |
| Asset Management | Express Metrix, Nessus | Are all deployed systems and assets authorized?  How many systems/live nodes are live in the XYZ asset zone? | [IT-ISP03 Mobile Computing Device Standard](https://wiki.desertschools.cure/wiki/it/Sec/_layouts/WordViewer.aspx?id=/wiki/it/Sec/Shared%20Documents/Information%20Security%20Policy%20ISP/ISP%20Supporting%20Standards/IT-ISP03%20Mobile%20Computing%20Device%20Standard.docx&Source=https%3A%2F%2Fwiki%2Edesertschools%2Ecure%2Fwiki%2Fit%2FSec%2FShared%2520Documents%2FForms%2FAllItems%2Easpx%3FRootFolder%3D%252Fwiki%252Fit%252FSec%252FShared%2520Documents%252FInformation%2520Security%2520Policy%2520ISP%252FISP%2520Supporting%2520Standards&DefaultItemOpen=1&DefaultItemOpen=1) |
| Configuration Management | Nessus | Which systems violate/deviate from configuration standards?  Which systems have default configurations deployed?  Which systems have modify registry | Autostart settings?  Which systems have non-configured or default settings? | [IT-ISP05 Configuration Management](https://wiki.desertschools.cure/wiki/it/Sec/_layouts/WordViewer.aspx?id=/wiki/it/Sec/Shared%20Documents/Information%20Security%20Policy%20ISP/ISP%20Supporting%20Standards/IT-ISP05%20Configuration%20Management.docx&Source=https%3A%2F%2Fwiki%2Edesertschools%2Ecure%2Fwiki%2Fit%2FSec%2FShared%2520Documents%2FForms%2FAllItems%2Easpx%3FRootFolder%3D%252Fwiki%252Fit%252FSec%252FShared%2520Documents%252FInformation%2520Security%2520Policy%2520ISP%252FISP%2520Supporting%2520Standards&DefaultItemOpen=1&DefaultItemOpen=1)  [IT-ISP22 System Security Assessment](https://wiki.desertschools.cure/wiki/it/Sec/_layouts/WordViewer.aspx?id=/wiki/it/Sec/Shared%20Documents/Information%20Security%20Policy%20ISP/ISP%20Supporting%20Standards/IT-ISP22%20System%20Security%20Assessment%20Standard.docx&Source=https%3A%2F%2Fwiki%2Edesertschools%2Ecure%2Fwiki%2Fit%2FSec%2FShared%2520Documents%2FForms%2FAllItems%2Easpx%3FRootFolder%3D%252Fwiki%252Fit%252FSec%252FShared%2520Documents%252FInformation%2520Security%2520Policy%2520ISP%252FISP%2520Supporting%2520Standards&DefaultItemOpen=1&DefaultItemOpen=1)  [IT-ISP06 Password Standard](https://wiki.desertschools.cure/wiki/it/Sec/_layouts/WordViewer.aspx?id=/wiki/it/Sec/Shared%20Documents/Information%20Security%20Policy%20ISP/ISP%20Supporting%20Standards/IT-ISP06%20Password%20Standard.docx&Source=https%3A%2F%2Fwiki%2Edesertschools%2Ecure%2Fwiki%2Fit%2FSec%2FShared%2520Documents%2FForms%2FAllItems%2Easpx%3FRootFolder%3D%252Fwiki%252Fit%252FSec%252FShared%2520Documents%252FInformation%2520Security%2520Policy%2520ISP%252FISP%2520Supporting%2520Standards&DefaultItemOpen=1&DefaultItemOpen=1)  [IT-ISP16.1 Vendor Remote Access](https://wiki.desertschools.cure/wiki/it/Sec/_layouts/WordViewer.aspx?id=/wiki/it/Sec/Shared%20Documents/Information%20Security%20Policy%20ISP/ISP%20Supporting%20Standards/IT-ISP16.1%20Vendor%20Remote%20Access%20Procedures.docx&Source=https%3A%2F%2Fwiki%2Edesertschools%2Ecure%2Fwiki%2Fit%2FSec%2FShared%2520Documents%2FForms%2FAllItems%2Easpx%3FRootFolder%3D%252Fwiki%252Fit%252FSec%252FShared%2520Documents%252FInformation%2520Security%2520Policy%2520ISP%252FISP%2520Supporting%2520Standards&DefaultItemOpen=1&DefaultItemOpen=1) |
| Network Management | SCCM  Nessus  SCOM | Which systems are generating unauthorized communication?  Which systems are transmitting sensitive data in clear text?  Which systems violate internal network security standards? | [IT-ISP021 Perimeter Security](https://wiki.desertschools.cure/wiki/it/Sec/_layouts/WordViewer.aspx?id=/wiki/it/Sec/Shared%20Documents/Information%20Security%20Policy%20ISP/ISP%20Supporting%20Standards/IT-ISP21%20Perimeter%20Security%20Standard.docx&Source=https%3A%2F%2Fwiki%2Edesertschools%2Ecure%2Fwiki%2Fit%2FSec%2FShared%2520Documents%2FForms%2FAllItems%2Easpx%3FRootFolder%3D%252Fwiki%252Fit%252FSec%252FShared%2520Documents%252FInformation%2520Security%2520Policy%2520ISP%252FISP%2520Supporting%2520Standards&DefaultItemOpen=1&DefaultItemOpen=1)  [IT-ISP021.1 Information Transmission](https://wiki.desertschools.cure/wiki/it/Sec/_layouts/WordViewer.aspx?id=/wiki/it/Sec/Shared%20Documents/Information%20Security%20Policy%20ISP/ISP%20Supporting%20Standards/IT-ISP21.1%20Information%20Transmission%20Standard.docx&Source=https%3A%2F%2Fwiki%2Edesertschools%2Ecure%2Fwiki%2Fit%2FSec%2FShared%2520Documents%2FForms%2FAllItems%2Easpx%3FRootFolder%3D%252Fwiki%252Fit%252FSec%252FShared%2520Documents%252FInformation%2520Security%2520Policy%2520ISP%252FISP%2520Supporting%2520Standards&DefaultItemOpen=1&DefaultItemOpen=1) |
| Information Management | RSA DLP | Which servers house sensitive information?  Which workstations house sensitive information?  Which locations (asset zones) on the network are most volatile?  Which | DLP Standard, Guidelines, Procedures |

Enterprise Security Architecture Map

Deployed Security System Descriptions

## Nessus

|  |  |
| --- | --- |
| **Security Solution:** | **Nessus Vulnerability Detection Engine** |
| **Description:** | Licensed vulnerability detection solution used to scan internal hosts and devices for vulnerabilities, bugs and misconfigurations. |
| **Standard(s):**   1. Nessus signatures are updated to the latest signature release prior to scanning assets 2. Nessus vulnerability engine will be updated within a week of a new version release 3. Only authorized personnel may access Nessus | |
| **Associated Policy Violations:**   1. Unauthorized software installations on production servers 2. Outdated / vulnerable software installations on production servers 3. Outdated / vulnerable software installations on workstations 4. Default configurations deployed to production servers or network devices | |
| **Current Tool Use:** | * Scanning business unit assets, entire asset zones, network segments and individual workstations vulnerabilities, bugs, misconfigurations and default configurations * Frequently updated network asset inventory * Used to generate attack paths through the enterprise network |
| **Solution Agenda:** | 1. Authenticated vulnerability scanning to identify vulnerabilities, bugs, and default configurations as well as:    1. Credentialed Patch Audits    2. Windows Malware Scans    3. PCI Quarterly Scans    4. Network Vulnerability Scans for PCI    5. Advanced Policy Inspection and Configuration Auditing |
| **Link:** | <https://10.1.2.203:8834/> |
| **Notes:** | Credentials stored in Network Password Manager? |

## Solar Winds Log and Event Manager (LEM)

|  |  |
| --- | --- |
| **Security Solution:** | **SolarWinds LEM SIEM** |
| **Description:** | Licensed centralized log collection system that supports windows, unix and syslog data collection. |
| **Standard(s):**   1. Sensitive servers and hosts are configured to forward their security logs to the SIEM solution. 2. All network devices are configured to forward their syslog events to the SIEM solution. 3. IT Security Operations reserves the right to manage and maintain LEM agent deployment SLAs on a 24/7 basis. 4. Changes to standard security audit policies require a change control review process 5. Centralized log management logs are kept for a minimum of 60 days. | |
| **Associated Policy Violations:**   1. … | |
| **Current Tool Use:** | * Malware and Intrusion Detection w/ alerting |
| **Solution Agenda:** | 1. Maintain availability (98%) 2. Ensure signatures are the most recent 3. Track and respond to all alerts |
| **Link:** | <https://ppr-lem01:8443/lem/> |
| **Notes:** | The LEM has serious availability issues. Oftentimes when the WebUI fails to render, the system requires a reboot. To do this, log into the LEM appliance [ssh:\\10.1.2.28:32022] , enter the Restart Device commands:   |  |  |  |  | | --- | --- | --- | --- | | Restart manager service | Restart Database | Restart Device | Reset WebUI Admin account | | 1. Login to CMC 2. Cmc> manager 3. Cmc> restart | 1. Login to CMC 2. Cmc> manager 3. Cmc> dbrestart | 1. Login to CMC 2. Cmc> appliance 3. Cmc> reboot | 1. Login to CMC 2. Cmc> manager 3. Cmc> reset admin |   Credentials stored in password manager? |

It is overwhelming to simply turn on auditing and feed all of content into a centralized manager like the LEM. It becomes an incredibly arduous task to then sift through the mountains of event data and determine what is normal and anomalous. When redesigning the requirements and procedures of Event Management, consider configuring each component of the Event Management Architecture through thorough action and event testing. Incorporate offensive techniques into the detection of malicious activity and document all activity that was configured as an alert. This list of configured alerts will apply to the asset type that was tested; a process that can be configured for each asset type. (e.g. Network Switches, Windows 7 Workstations, Windows Server 2012, etc.)

## IBM Managed Security Services (MSS)

|  |  |
| --- | --- |
| **Security Solution:** | **IBM Portal (MSS)** |
| Description: | Publicly accessible portal where DS Firewall and DS Cisco IPS system logs can be viewed, searched, and reported upon. MSS is a SOC service provided by IBM that aims to assist companies and organizations with threat intelligence and detection. |
| Standard(s):   1. SOC Alerts generated by IBM MSS are investigated based on Incident Response procedures to determine if the Alert is a false positive, false negative or an indicator of compromise. | |
| Associated Policy Violations:   1. Unauthorized network communication 2. Unauthorized network activity | |
| Current Tool Use: | * Firewall log searching for authorized and unauthorized communication * Network IDS event analysis and searching for unauthorized activity * Network communication report generation that is supplied to numerous scripts for custom reporting * Maintaining DMZ asset inventory |
| Solution Agenda: | 1. Ensure all monitored devices maintain an SL of 98% availability 2. Ensure alerts and notification are tuned to maximum efficiency 3. Track and respond to all alerts 4. Investigate external attacks to the public facing internet and ensure actors are tracked and indexed for threat context 5. Automate the generation of reports to advance internal threat intelligence |
| Link: | <https://portal.mss.iss.net/mss/login.mss> |
| Notes: | Credentials stored in password manager? |

## RSA Data Loss Prevention Tool

|  |  |
| --- | --- |
| **Security Solution:** | **RSA Data Loss Prevention Tool** |
| Description: | Enterprise-level regular expression engine with a robust content database used to identify sensitive and confidential information (at rest). |
| Standard(s):   1. User/administrative access to the RSA DLP tool must consist of a provisioning process 2. Only authorized personnel may access the RSA DLP tool | |
| Associated Policy Violations:   1. Unauthorized sensitive data storage | |
| Current Tool Use: | * Scanning business unit assets, entire asset zones, network segments and individual workstations for sensitive (CCN, SSN) content. * Database of secure files and content throughout the enterprise |
| Solution Agenda: | 1. Sensitive and confidential data that is discovered is either:    1. Protected with encryption (RMS)    2. Locked down via access control (NTLM Permissions)    3. Relocated to a secure, controlled environment    4. Deleted 2. To standardize data sensitivity risk rating levels via Content, Context and Quantity. |
| Links: | <https://pi-dlpem01/login.html> |
| Notes: | The DLP system is currently managed and supported by Jason Lutz.  Credentials stored in password manager? |

## IDS Sensors

|  |  |
| --- | --- |
| **Security Solution:** | **Papago and Annex Sensors** |
| **Description:** | Open source IDS sensors installed to identify anomalous and malicious network activity |
| **Standard(s):**   1. When critical events are triggered by IDS sensors, an investigation will be conducted to determine if the alert is a false positive, false negative or an indicator of compromise. 2. IDS sensors should be maintained at a monthly availability of 98%. 3. IDS sensors shall track and store network communication data for up to 30 days. 4. IDS signatures are updated daily. 5. Only authorized personnel may access IDS sensors (via Shell or UI) | |
| **Associated Policy Violations:**   1. Unauthorized network traffic or communication | |
| **Current Tool Use:** | * Intrusion detection w/o fine-tuned alerting * Network and network data statistics * Packet tracing and sniffing for host and incident investigations |
| **Solution Agenda:** | 1. Maintain availability (98%) 2. Ensure signatures are the most recent 3. Track and respond to all alerts |
| **Links:** | Annex: <https://10.100.3.21>    Papago: <https://10.1.3.21> |
| **Notes:** | Both Snort sensors are built on the linux platform CentOS.  Credentials stored in password manager? |

## FireEye

|  |  |
| --- | --- |
| **Security Solution:** | **FireEye Sensor** |
| **Description:** | Licensed network device that monitors web requests and malware callback signatures. Can duplicate a callback or download and execute it inside a virtual machine to identify threats. |
| **Standard(s):**   1. Critical events triggered by FireEye detection devices will be investigated based on malware investigation procedures to determine if the Alert is a false positive, false negative or an indicator of compromise. | |
| **Associated Policy Violations:**   1. Unauthorized network traffic or communication 2. Unauthorized program execution | |
| **Current Tool Use:** | * Malware and Intrusion Detection w/ alerting * Network and network data statistics * Packet tracing and sniffing for host and incident investigations * Generating malware execution signatures for investigation |
| **Solution Agenda:** | 1. Maintain availability (98%) 2. Ensure signatures are the most recent 3. Track and respond to all alerts |
| **Link:** | <https://10.1.48.45/login/login> |
| **Notes:** | When analyzing FireEye alerts, keep in mind that FireEye is spanned, so it sees requests that originate from workstations as well as the request that the Sophos proxy makes if  in fact it doesn’t block the request.  Typically, a user/workstation will make the initial request, which has to go through the Proxy due to network policy.  If Sophos is being a good little proxy, it will block the request and we won’t see a FireEye alert from the proxy.  This process is illustrated below:  Credentials stored in password manager?      Ultimately, it cannot be determined that AV picked up on the download and took action, then it is necessary to investigate further, using the signature that FireEye triggered upon for investigative starting points. |

Automation Task Table

The ability to generate posture updates and critical metrics quickly is the corner stone of operational reporting. At moment’s notice, the data and logs of deployed security systems should be immediately accessible. Custom libraries and API’s are typically required to develop techniques to query, structure and present the data for decision making. The following is a chart of standard security system query requirements. See (link: [Operative Security Software](http://www.brentchambers.net/oss.html)) for assistance with developing interactive applications for the visualization, reporting and measurement of operational security data.

|  |  |  |  |
| --- | --- | --- | --- |
| **Tool** | **Capabilities** | **Policy Violations** | **Needed** |
| Annex Sensor | [+] Annex Network Visibility / Intrusion Detection and Alerting [+] Packet Sniffing | Unauthorized network activity | Technique to list the last X amount of alerts fired. Technique to quickly sniff/trace network traffic (dss.py) Technique to export to serve up pcap files |
| Papago Sensor (needs a rebuild) | [+] Papago Network Visibility / Intrusion Detection and Alerting [+] Packet Sniffing | Unauthorized network activity | Technique to list the last X amount of alerts fired. Technique to quickly sniff/trace network traffic (dss.py) Technique to export to serve up pcap files |
| FireEye Sensor | [+] Malicious communication detection (App, L4, L3) [+] Malware Detection / Virtualized Analysis | Unauthorized network activity Unauthorized execution |  |
| LEM SEIM | [+] Real-time system syslog monitoring [+] Real-time alerting [+] SEIM Reporting [+] Customizable situational awareness dashboard | [Various] | To improve agent deployment % to above 90% To quickly list deployed agents and compare them to inventory results |
| IBM Portal | [+] External threat analysis [+] Cisco IPS Logging [+] External Vulnerability Scanning | Unauthorized network activity Unauthorized external access attempts | To improve agent deployment % to above 90% To quickly list deployed agents and compare them to inventory results Automatically retrieve generated reports for mss.py processing |
| Firewall / ACL | [+] Primary network access control [+] Traffic auditing [+] Traffic control | Unauthorized outbound connections | Technique to list the connection builds granted per host |
| RSA DLP | [+] Identifying data types  [+] Identifying sensitive data | Unauthorized data storage | Method to quickly assess where sensitive data is, the nature of it, and its context. |
| Nessus Scanner | [+] Vulnerability discovery [+] System auditing [+] PCI Auditing | Unauthorized services Outdated software installations | Technique to quickly group business systems, their vulnerabilities, and a formula to rate relative risk. |

Security Templates and Documentation

The InfoSec wiki is the primary repository for completed deliverables. When work requires documentation, it should be stored in the appropriate child folder of the InfoSec Security Operations wiki page. The following is a chart that details operational work that generally requires a deliverable for completion.

|  |  |  |
| --- | --- | --- |
| **Deliverable** | **Description** | **Templates** |
| Technical Assessments   * Risk Assessments * Technical Risk Assessments * Vulnerability Research * Quick System Scan and Analysis | Technical assessments are generally performed as a part of a security review, although they don’t have to be. A technical assessment may be requested by a PM, an engineer and can be performed proactively with the approval of Management. Proactive technical assessments may also be conducted when performing specific research (e.g. newly disclosed vulnerability analysis). | [Vulnerability\_Research\_Template.doc](https://wiki.desertschools.cure/wiki/it/Sec/_layouts/WordViewer.aspx?id=/wiki/it/Sec/Shared%20Documents/Security%20Operations/Security%20Templates%20and%20Documentation/Vulnerability_Research_Template.docx&Source=https%3A%2F%2Fwiki%2Edesertschools%2Ecure%2Fwiki%2Fit%2FSec%2FShared%2520Documents%2FForms%2FAllItems%2Easpx%3FRootFolder%3D%252Fwiki%252Fit%252FSec%252FShared%2520Documents%252FSecurity%2520Operations%252FSecurity%2520Templates%2520and%2520Documentation%26InitialTabId%3DRibbon%252EDocument%26VisibilityContext%3DWSSTabPersistence&DefaultItemOpen=1&DefaultItemOpen=1)  Risk\_Assessment\_Template.doc  Security\_Status\_Report\_Template.doc |
| Standards, Procedures and Guidelines | IT Security Standards, Procedures and Guidelines are needed when defining how a system or technology is to be used throughout the enterprise. The wiki folder provides guidelines and templates for developing technology requirements and standards. | [Standard\_Document\_Template.doc](https://wiki.desertschools.cure/wiki/it/Sec/_layouts/WordViewer.aspx?id=/wiki/it/Sec/Shared%20Documents/Security%20Operations/Security%20Templates%20and%20Documentation/Standard_Document_Template.docx&Source=https%3A%2F%2Fwiki%2Edesertschools%2Ecure%2Fwiki%2Fit%2FSec%2FShared%2520Documents%2FForms%2FAllItems%2Easpx%3FRootFolder%3D%252Fwiki%252Fit%252FSec%252FShared%2520Documents%252FSecurity%2520Operations%252FSecurity%2520Templates%2520and%2520Documentation%26InitialTabId%3DRibbon%252EDocument%26VisibilityContext%3DWSSTabPersistence&DefaultItemOpen=1&DefaultItemOpen=1)  Procedure\_Document\_Template.doc  Guideline\_Document\_Template.doc |
| Red Team Operations | When offensive work is performed on information assets, steps should be tracked and documentation should be made to account for all activity that took place on the enterprise network. | See folder |
| Blue Team Operations | Comprised of network defense and continuous monitoring documentation and reporting. Wiki location contains DS\_Defense tools, outlines, procedures, guidelines, efforts, tasks and tactics. | DS Defense SOC Outline  DS\_SOC Tool Descriptions  IT-ISPXX Security Operations Standard  IT-ISPXX Security Operations Procedure |
| Incident Reports | Incident reports are created to document violations of policy, data loss or potential data loss and confirmed security incidents. | [Incident\_Report\_Template.doc](https://wiki.desertschools.cure/wiki/it/Sec/_layouts/WordViewer.aspx?id=/wiki/it/Sec/Shared%20Documents/Security%20Operations/Security%20Templates%20and%20Documentation/Incident%20Report%20Template.docx&Source=https%3A%2F%2Fwiki%2Edesertschools%2Ecure%2Fwiki%2Fit%2FSec%2FShared%2520Documents%2FForms%2FAllItems%2Easpx%3FRootFolder%3D%252Fwiki%252Fit%252FSec%252FShared%2520Documents%252FSecurity%2520Operations%252FSecurity%2520Templates%2520and%2520Documentation%26InitialTabId%3DRibbon%252EDocument%26VisibilityContext%3DWSSTabPersistence&DefaultItemOpen=1&DefaultItemOpen=1) (OLD) |
| Data Loss Prevention |  | Data\_Sensitivity\_Report\_Template.doc (NEW) |
| Daily Operations | Deployed Security Systems require daily content and report analysis. The procedures included in this folder should be followed on a daily to semi-daily basis. | Daily\_Operations\_Workbook.xls (NEW) |

Proactive Security Operations

The InfoSec wiki is the primary repository for completed deliverables. When work requires documentation, it should be stored in the appropriate child folder of the InfoSec Security Operations wiki page.

**For each Defense Domain:**

|  |  |  |
| --- | --- | --- |
| Continuous Analysis Steps Per Domain | | Deliverable |
| Step 1 | Locate the source of security data and develop a technique to extract the raw data necessary to perform analysis (file) | Data File (CSV, XML, XLS, Txt) |
| Step 2 | Determine useful/valuable metrics that can be derived from the data. | Data Structure  […, …, …] |
| Step 3 | Automate the collection of data and design a multi-dimensional data structure to organize like fields and items. | Program Design Program/Script (\*.py) |
| Step 4 | Develop an interactive UI to query the data structure with a relative rotation factor of at least 3. | Access Class / API  UI Interface |
| Step 5 | Develop a process and frequency for automating data collection and querying the data structure for situational intelligence. | Ex. Scan X Ranges every 5 Min |
| Step 6 | Populate a data store for trending and historical analysis (Database) | MySQL, MSSQL, POSTGRE, etc |

## Continuous Security Monitoring

Continuous Security Monitoring (CSM) consists of proactively assessing the integrity of security related data at rest; workstation and server log files, registry keys, and system configurations.

How to develop a Continuous Security Monitoring system.

1. Developing and Evaluating Baseline Configurations
2. **Host Discovery and Inventory**
3. Hunting and Reconnaissance
   1. Detecting Malicious User-Agent Strings
      1. Capture all user agent strings over the network
      2. Ignore anything containing Mozilla, Opera, or Microsoft-CryptoAPI
      3. Sort from least common to most common
      4. Inspect the rarest User-Agent Strings and identify the source
4. Execution Propagation Detection
   1. E-mail attachments
   2. Downloads via HTTP/HTTPS
   3. Downloads via TFTP/FTP
   4. Download via DNS
   5. Download via SMB
   6. Download via whatever is allowed outbound
   7. Pivoted distribution from compromised host
   8. Removable media
5. Administrative Accounts
6. Tools
7. Hunting and Recon
   1. Recon: Building a targeted wordlist, employee list, email list, org chart from publicly available information
   2. Mapping: Using a multitude of techniques to identify potentially unpublished hostnames:
      1. Zone Transfer
      2. DNS Tricks
      3. Direct and Reflected host sweeps
      4. Search engines
      5. Bruteforce

## Network Security Monitoring

Network Security Monitoring consists of collecting and analyzing security related data in motion; network packets and data derived from network packets. The practice of Network Security Monitoring should result in a variety of reports when conducted:

1. **Continuous Host Discovery and Inventory**
   1. Maintain an inventory of all nodes on the network where logical groupings and security posture assessments can be performed at a moment’s notice:
      1. Desktops / Servers
      2. Routers / Switches
      3. Printers
      4. VoIP Devices
      5. Building Automation
      6. Physical Security Devices
      7. Other devices that talk TCP/IP

The operational goal and focus for continuous host discovery and inventory is not to merely collect a list of deployed hosts and nodes, but to develop a technique for persistent

1. **Network Traffic Analysis**
   1. Implementing HTTP User Agent Monitoring
      1. User-Agent blacklists/blocklists for known bad User-Agent strings (in Sophos)
      2. Determine what is normal
   2. Detecting Specific Anomalies
      1. Look for names of EXE’s, DLL’s, directories, usernames, DNS names, and function calls
      2. Search for one-character Windows EXE names (i.e. “w.exe”)
      3. Detecting Client-> Client EXE flow
      4. Detecting ICMP echo requests / response payloads that contain a lot of data
2. **Outbound Communication Report should answer the following questions:**
   1. How much data is sent outbound?
   2. Who sends the data?
      1. IPs/Hostnames
   3. Where is the data going?
   4. When is the data sent?
   5. Isolate and analyze data that goes to a foreign country
   6. Graph outbound connections based on destination ports
3. **Exploring Honeypots**
   1. Internal honeypots could be placed on specific VLANs for the detection of adversarial post-exploitation activity. Internal honeypots can also be used to detect rogue insiders. Honeypots and their general concepts can be used in the following scenarios:
      1. HoneyUsers / HoneyAdmins: The creation of accounts with names suggesting elevated privileges
      2. HoneyShares / HoneyFiles: Shares and files meant to entice an adversary that are closely monitored and alerted on any type of access
      3. HoneyDB / Honeytales: Databases and tables named to indicate passwords or sensitive info
      4. HoneyRobots.txt: An internal robots.txt on internal web servers where legit spiders/crawlers will not likely exist

|  |  |  |
| --- | --- | --- |
| **SYSTEM** | **USER** | **PASSWORD** |
| Nessus | admin | penelope77 |
| LEM | admin | MovingToMars#!5 |
| MSS |  |  |
| RSA |  | J.Lutz |
| IDS Papago | admin | MovingToMars#!5 |
| IDS Annex | admin | aftercataracts21! | MovingToMars#!5 |
| FireEye | admin | MovingToMars#!5 |

# NSM Tool Cannon:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Continuous Analysis Steps Per Domain | | | | | General Use(s) |
| Wireshark | Graphical, industry standard tool for capturing and analyzing network traffic. | | | | Extracting PCAP files from deployed sensors and analyzing them in WireShark |
| Example(s):  View strange GET requests with the following filters:   * http.request.method * frame contains <string> | | | | | |
| Strings | | Unix/Linux utility that will print the printable character sequences that are at least 4 characters long. Outrageously useful for extracting readable information from binary content (i.e. clear-text network transmissions, binary files, etc.) | | Extracting User-Agent strings, DNS requests, and clear-text network transmissions | |
|  | | **Example(s):**  ***Enumerate User-Agents from a pcap file:***   * $ strings filename.pcap | grep “User-Agent” | | | |
| Tcpdump/windump | | Packet capture utilities that mimic Wireshark’s functionality. TCPdump is typically native to Linux based systems while Windump is 3rd party and should be downloaded from [here.](https://www.winpcap.org/windump/install/bin/windump_3_9_5/WinDump.exe) |  | | |
|  | | **Example(s):**  ***Enumerate DNS Lookups:***   * $ tcpdump -i eth1 -n -XX udp port 53 and not dst net 10.0.0.0/8 | grep -I A?   ***Enumerate public/direct DNS Lookups with a defined string:***   * $ tcpdump -i eth1 -nXX udp port 53 and dst net 10.1.2.0/24 | grep -I A? | grep -v .phx.dsfcu.local | grep brent | | | |
| Tshark | | Command-line equivalent to wireshark: captures packet data, reads from capture files and uses the same capture expression filters. |  | | |
|  | | **Example(s):**  ***Extract User-Agent strings from pcaps:***   * $ tshark –nr /user-agent.pcap –R ‘htto.user\_agent” –Tfileds –e http.user\_agent | | | |
| Bro | | Network security monitor that provides a comprehensive platform for network traffic analysis and semantic security monitoring at scale. Can also be used to carve files out of pcaps. |  | | |
|  | | **Example(s):**  **Extract files from packet capture data:**  $ bro –r <capture.pcap> /opt/bro/share/bro/file-extraction/extract.bro | | | |
| ngrep | | Ngrep is a variation of the utility grep only it targets the network layer. Ngrep is a pcap-aware tool that will allow you to specify regular expressions to match against data payloads of packets. It currently recognizes TCP, UDP, and ICMP across Ethernet, PPP, SLIP, FDDI, and null interfaces. |  | | |

## Daily Operations Reporting

The following outline details the minimum requirements for a sample daily security operations reporting.

* + - * + Review Alerts generated in the last 12 hours
        + Indicators of compromise
    1. Run Egress Report – Last 24 Hours
       1. Generate long-tail egress report for different asset groups
    2. Long-tail URL GET Analysis – Last 24 Hours
    3. Long-tail DNS resolution analysis – Last 24 Hours
    4. A/V Quarantine actions taken
       - * Unauthorized account usage
    5. Server Login Report – Last 24 Hours
    6. Administrative Account Usage - Last 24 Hours
    7. Root Level Account Usage
       - * Policy and standard violations
    8. Status of ***# of policy violations configured for detection / # of detectable policy violations derived from ISP standards***

When reports are run, a reportable metric is generated and should be added to a trending system, included in a report of a larger scope, and/or escalated for further review.

# 

## Weekly Operations Reporting

The following outline details the minimum requirements for a sample weekly security operations reporting.

* + - * + Review Alerts generated in the last 12 hours

# 

## Monthly Operations Reporting

The following outline details the minimum requirements for a sample monthly security operations reporting.

* + - * + Review Alerts generated in the last 12 hours

## ISRAB Report (Quarterly)

The following outline details the minimum requirements for a quarterly (ISRAB) security operations reporting.

* + - * + Review Alerts generated in the last 12 hours

Enterprise Security Services

Service Requests are general work requests that the operations team receives as service tickets. It’s common that various departments in IT and throughout the business are not familiar with general security requests due to the infancy of security operations in the enterprise. Because of this, initial security assessments, engagements and investigations should be performed proactively. Security Architecture must be defined to a level where network, data, workstation and server locations can be easily specified, correlated, and cross-referenced in order to target levels of the network from the user layer down to the hardware.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Security Service Requests** | **Input** | **Output** | **Ref/Link** | **Tools** |
| **Security Reviews**  (To quantifiably assess the level of risk a project | * + - * + PR or SME provided system architecture diagram         + Populated security assessment questionnaire | Security Review Template (DREAD Model Based) | Link  Link |  |
| **Security Tests**  (To quickly assess a target for easy points of entry or attack.) | * + - * + A new or changing asset connected to the enterprise network and a general scope of what is to be tested | Security Test Results (often informal) |  | Kali Linux Bundle |
| **Web Application Assessments**  (To obtain access or data from a backend system using flaws in the web application or server). | * + - * + A web application or web location and a specific scope of what is and is not off-limits to the engagement. | Web Application Pen Test Report |  | Kali Linux Bundle |
| **System Data Sensitivity Report**  **(**Goal: To identify any and all sensitive data that is stored throughout the enterprise. | * + - * + DLP scan results (Bulk and Targeted) | System Data Sensitivity Report  Traffic Profile  AV Profile  Sensitive Info Profile  Vulnerability Scan |  |  |
| **Business System Pen Test**  (Goal: to target the business system with the intent of retrieving sensitive information) | * + - * + Business system architectural diagram         + Scope of what is to be tested and what is off-limits | Business System Penetration Test Executive Report  Business System Penetration Test Detailed Report |  | Kali Linux Bundle |
| **Web Traffic Analysis**  (Goal: Identify web requests with high entropy, analyze traffic for clear text transmission, extract binary files from HTTP transmission, etc.) | * + - * + Source Host or Domain AND/OR         + Destination Host or Domain | Web Traffic Analysis Report  Packet Capture if requested |  | Sophos UI  TCPdump/IDS |
| **Malware/Forensic Analysis**  (Goal: verify if unauthorized access or unauthorized execution occurred. Timeline the events of a system compromise) | * + - * + Live response results         + FireEye reports         + File System / Memory Analysis | Malware Analysis Report  OR  Incident – System Compromise |  | SIFT Workstation  FireEye UI |
| **Standard and Policy Writing**  (Draft a security standard, procedure, diagram or guideline) | * + - * + General requirements and consensus for a project, a new technology or technology change. | IT-ISP Standard  IT-ISP Procedure  IT-ISP Guidelines |  | Security Brain |
| **Network Traffic Analysis**  (Goal: Trace and analyze network and socket communication.  Produce a packet capture file (pcap) for X amount of time (or X amount of packets) | * + - * + Packet Capture File (.PCAP)         + Live SPAN port Trace | Network Traffic Analysis Report | Link | TCPdump  WINdump  WireShark |
| **Host Investigations**  (Goal: Locally or Remotely access a host in order to perform live response analysis on its running configuration, user names, startup folders/keys, network connections, etc.) | * + - * + Live response results | Host Investigation Report | Link | Wmic\_lr\_remote.cmd  Wmic\_lr\_local.cmd |
| **ISRAB Reporting**  (Generate standard quarterly ISRAB numbers)[ | * + - * + Vulnerability Statistics         + Patch Statistics         + FINAC Breach Reports         + Vuln Status | Excel charts and graphics for pasting into the ISRAB template. |  | Israb\_vulns.exe  Israb\_patches.exe |

## In-Depth Tactics and Procedures

The following sections will provide both offensive and defensive procedures.

1. **Windows Process Analysis Procedures**
   1. Investigate Image Names:
      1. Legit Process?
      2. Spelled correctly?
      3. Matches system context?
   2. Investigate Full Path names.
      1. Appropriate path for system executable?
      2. Running from a user or temp directory?
   3. Identify parent process
      1. Is the parent process expected?
   4. Was the process launched with any strange arguments?
   5. Identify process start time.
      1. Was the process started at boot time?
      2. Was it started near the time of the known attack?
   6. Identify SID.
      1. Does the SID make sense?
      2. Why would a process use a user account SID?

|  |
| --- |
| **Windows System Analysis TIPS** |
| 1. Most SYSTEM binaries from \windows\system32. Deviations are cause for concern. |
| 1. Standard System processes don’t typically use USER SIDs. Question the deviations. |
| 1. System processes with no parent process path are questionable. |
| 1. Memory acquisition tools look evil because they load drivers and access raw memory |
| 1. Services are typically a child of services.exe |
| 1. Similar processes should start around the same time (svchost.exe) |

1. **PENTRN Competency Quiz**

|  |  |  |
| --- | --- | --- |
| Skill Level | Technique | Sample Syntax |
|  | Perform a TCP traceroute? | Windows: tracert host  Linux: traceroute host |
|  | Identify CMS systems / frameworks? |  |
|  | Bruteforce a MSSQL server? |  |
|  | Perform a zone transfer? |  |
|  | Forward DNS brute force? |  |
|  | Reverse DNS brute force |  |
|  |  |  |
|  | Pull ARP frames from the network |  |
|  | Sniff just a network range |  |
|  | Sniff traffic associated with just one host |  |
|  | Exploit a NULL sessions on Windows? |  |
|  | Perform an ARP spoof |  |
|  | Poison a local network segment |  |
|  | Perform DNS poison on the local segment |  |

1. **Zero Day Economics**
2. How long will it take to patch?
3. How hard is it to exploit?
4. How many other people want it?

These questions influence behavior in the information technology space. Newly disclosed vulnerabilities tend to send those that have implemented or adopted the vulnerable technology, into a patch or temporary mitigation frenzy.

Zero day and malware economics can also influence global markets by

* + - * + financially affecting large IT companies when vulnerabilities are disclosed,
        + impacting a sector or industry that is heavily reliant on vulnerable technology
        + generating enormous amounts of revenue for cyber criminals

1. Windows XP Sethc Backdoor
2. Standard Post-Exploitation Procedures