Building a Security Operation Center

• Agenda:
  ➢ Auditing Your Network Environment
  ➢ Selecting Effective Security Solutions
  ➢ Building A Security Operation Center
  ➢ Forming A Security Team
  ➢ Samples of Real-Time Dashboards
Auditing Your Network Environment

To start off the security program, we need to assess the risks of your current network environment by asking the following questions:

- Are there vulnerabilities that exist in your applications, servers, and network devices?
- Security Awareness program?
  - Recommend SANS ‘Securing the Human’
- Defined Security Policies for data classification, firewall, wireless policy, computer use policy, etc?
- Do you log all critical systems for compliance and monitoring purposes?
Auditing Your Network Environment

To start off the security program, we need to assess the risks of your current network environment by asking the following questions:

- Any there security controls such as access control, malware defenses, application security, date loss prevention, incident response, etc.? 
  - Which security controls are lacking in your internal networks?
  - Which security controls are lacking at your edge internet perimeters?
- Do you practice layered security in your network architecture?
  - Avoid utilizing a single solution for firewalls, IPS, remote access, etc.
- Do you have a single point of entry and exit from your internal network to internet?
To have an effective security operations, selection of best-of-breed security products is essential. Included are:

- **Logger** – a centralized logger that logs critical systems security events
- **Endpoint Protection** – antivirus, antispyware, application control, firewall/IPS
- **Vulnerability Scanner** – scanning workstations and servers vulnerabilities
- **Network Advisor** - analyze network devices configurations for vulnerabilities
Selecting Effective Security Solutions

To have an effective security operations, selection of best-of-breed security products is essential. Included are:

- **Applications Firewall** - provides controls over applications, users, and any type of network traffic including threats
- **Intrusion Prevention Systems** – detect and block security hackings and intrusions
- **Penetration Testing** – tool that runs vulnerable exploits against your systems
- **Enterprise Security Management** – analyzes, correlates, and detect security events through log records to find the critical incidents.
Building A Security Operation Center

Building a successful SOC requires the following approach:

- Select real-time security dashboards for notification.
- Develop incident response processes and procedures.
- Select critical security alerts to notify your team 24 x 7.
- Send syslog and security events from firewalls, routers, netflow, IPS, applications, and operating systems to the SOC for monitoring.
- Staffing plans for 24 hours rotation OR using MSSP for 24 x 7 monitoring plus 8 x 5 local monitoring for insider and internet threats.
Building A Security Operation Center

Building a successful SOC requires the following approach:

- Define specific tasks assigned to the SOC – e.g. detecting attacks from internet, monitoring compliance, detecting insider threats, incident response/forensic analysis, vulnerability review, etc.
- Selecting SOC analysts experienced in networks, servers, and applications troubleshooting and intrusion analysis skills.
- Requires SOC analysts to be trained with Information Security, Intrusion Detection in Depth, TCP/IP, Network Forensics, etc.
Forming a Security Team

Chief Information Security Officer (CISO)

Risk Management & Business Continuity
- Security Policy & Enforcement
- Vulnerability Management
- Intrusion Detection/Prevention Systems
- PCI, NIST 800-53 & ISO 27002:2005
- Business Continuity Management
- Network, Wireless, Endpoint Security Audit
- Penetration Testing
- Computer Forensics Investigations

Cyber Security Operation
- Cyber Security Monitoring
- Security Awareness Program & OIS website
- Application & Database Security
- Advisories, Notifications, & Security Reports
- Enterprise Threat & Risk Management (ETRM)
- Universal Log Management
- Identity View Access Control
- Network Forensics for Incident Response

Designed by Bob Cheong
Version: 3.0
A Centralized Logger

<table>
<thead>
<tr>
<th>Receiver</th>
<th>Current EPS</th>
<th>Current Bytes/Second</th>
<th>Maximum EPS</th>
<th>Total Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCPSGF Proxy</td>
<td>3,090 c/s</td>
<td>5,733,434 B/s</td>
<td>4,730 c/s</td>
<td>799,647,988 Events</td>
</tr>
<tr>
<td>MDHCPE-MS DHCP</td>
<td>0 e/s</td>
<td>0 B/s</td>
<td>4,255 e/s</td>
<td>15,047,446 Events</td>
</tr>
<tr>
<td>MDHCPE-MS DHCP-Badging</td>
<td>0 e/s</td>
<td>108 B/s</td>
<td>30 e/s</td>
<td>15,142 Events</td>
</tr>
<tr>
<td>MEMTLE-MS Exchange</td>
<td>9 e/s</td>
<td>10,175 B/s</td>
<td>4,650 e/s</td>
<td>39,155,435 Events</td>
</tr>
<tr>
<td>MIMSrf-FTP</td>
<td>10 e/s</td>
<td>12,485 B/s</td>
<td>1,140 e/s</td>
<td>991,998 Events</td>
</tr>
<tr>
<td>MIMSrf-WWW</td>
<td>0 e/s</td>
<td>0 B/s</td>
<td>6,188 e/s</td>
<td>141,383,357 Events</td>
</tr>
<tr>
<td>MNSMDB-EMS IPS</td>
<td>0 e/s</td>
<td>0 B/s</td>
<td>12 e/s</td>
<td>76,038 Events</td>
</tr>
<tr>
<td>MWELM-MS Domain Controller</td>
<td>30 e/s</td>
<td>35,466 B/s</td>
<td>3,602 e/s</td>
<td>1,410,917,182 Events</td>
</tr>
<tr>
<td>MWELM-MS Domain Controller-Badging</td>
<td>1 e/s</td>
<td>1,951 B/s</td>
<td>980 e/s</td>
<td>35,128,584 Events</td>
</tr>
<tr>
<td>SD-Firewall ScreenOS Syslog-TBIT</td>
<td>0 e/s</td>
<td>0 B/s</td>
<td>3,733 e/s</td>
<td>690,306,992 Events</td>
</tr>
<tr>
<td>SD-Firewall ScreenOS Syslog-TBIT</td>
<td>220 c/s</td>
<td>424,382 B/s</td>
<td>1,181 c/s</td>
<td>1,273,401,399 Events</td>
</tr>
<tr>
<td>SD-Syslog</td>
<td>550 e/s</td>
<td>879,399 B/s</td>
<td>4,130 e/s</td>
<td>3,668,138,250 Events</td>
</tr>
<tr>
<td>SD-Syslog</td>
<td>550 e/s</td>
<td>879,399 B/s</td>
<td>4,130 e/s</td>
<td>3,668,138,250 Events</td>
</tr>
<tr>
<td>SD-Router</td>
<td>0 e/s</td>
<td>0 B/s</td>
<td>56 e/s</td>
<td>1,856,927 Events</td>
</tr>
<tr>
<td>SEPBD-EMS IPS</td>
<td>0 e/s</td>
<td>724 B/s</td>
<td>317 e/s</td>
<td>4,827,598 Events</td>
</tr>
<tr>
<td>TSSE-EMS IPS</td>
<td>0 e/s</td>
<td>265 B/s</td>
<td>5,300 e/s</td>
<td>4,171,457 Events</td>
</tr>
<tr>
<td>SD-ASA</td>
<td>0 e/s</td>
<td>0 B/s</td>
<td>100 e/s</td>
<td>2,109,665 Events</td>
</tr>
<tr>
<td>SD-ACS</td>
<td>0 e/s</td>
<td>272 B/s</td>
<td>57 e/s</td>
<td>7,491,267 Events</td>
</tr>
<tr>
<td>SD-SSL VPN</td>
<td>0 e/s</td>
<td>105 B/s</td>
<td>50 e/s</td>
<td>416,181 Events</td>
</tr>
<tr>
<td>SD-SSL Badging</td>
<td>0 e/s</td>
<td>0 B/s</td>
<td>1,520 e/s</td>
<td>510,812 Events</td>
</tr>
</tbody>
</table>
Security Monitoring Console
Security Monitoring Console
Global Access to LAWA.ORG
Detecting Malwares – viruses, bots, worms, trojans, rootkits, etc
Detecting Wireless Rogue Access Points
The Digital Dashboard was developed by the MS-ISAC as a central resource to provide valuable, real-time data regarding the current cyber security environment. The Dashboard features a variety of sources, including cyber attack information, cyber alert threat levels, and the latest advisories and news to assist organizations in their cyber security efforts. Comments can be directed to info@msisac.org.
LAWA Security Operation Center
Questions?