BUILDING A SECURITY OPERATION CENTER (SOC)

ACI-BIT Vancouver, BC.

Los Angeles World Airports

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 compliancy 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?

Selecting Effective Security Solutions

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

- **Logge**r – 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:

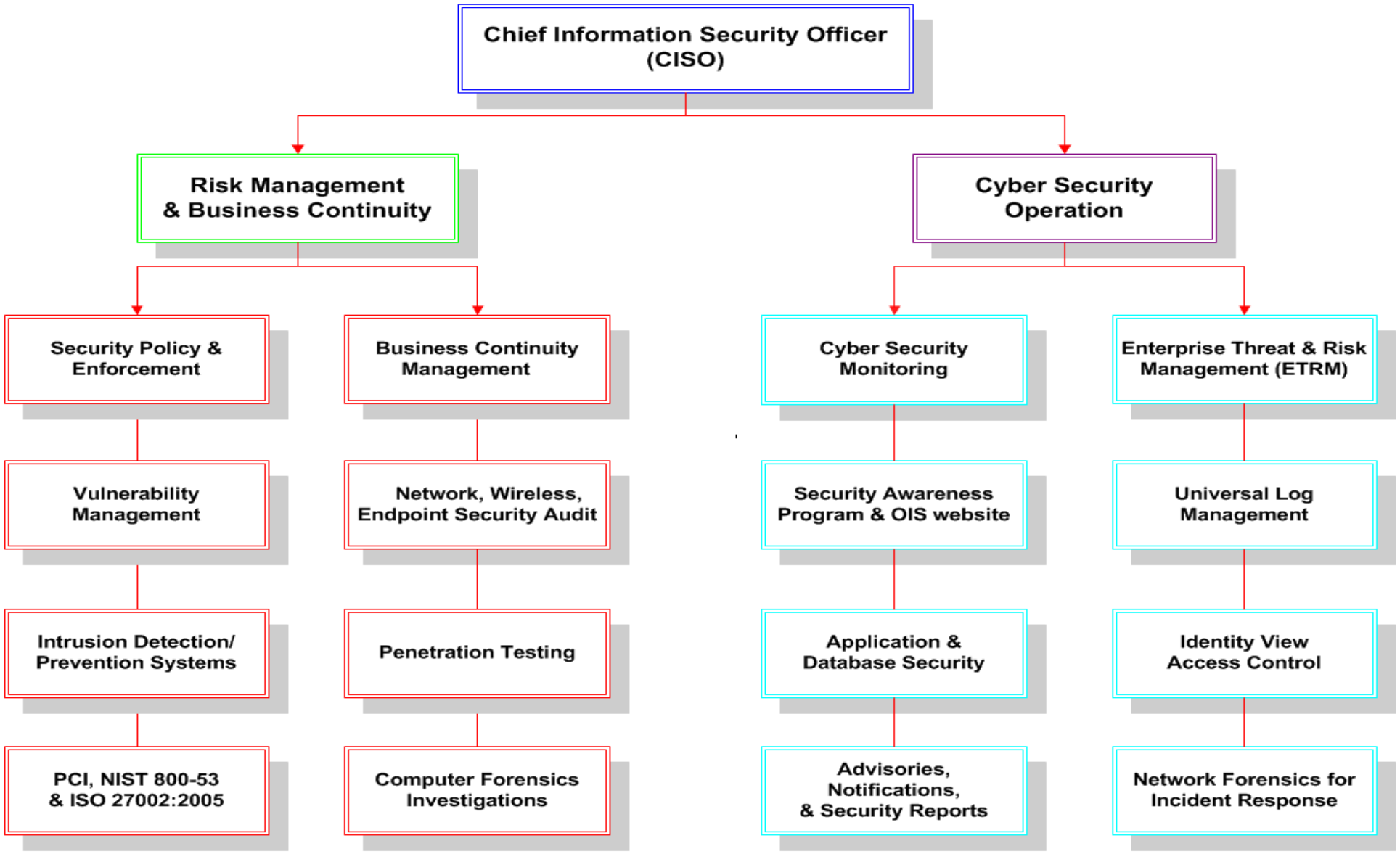
- Select real-time security dashboards for notification.
- Develop incident response processes and procedures.
- Select critical security alerts to notify your team 24 x 7.
- Send syslog and security events from firewalls, routers, netflow, IPS, applications, and operating systems to the SOC for monitoring.
- 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:

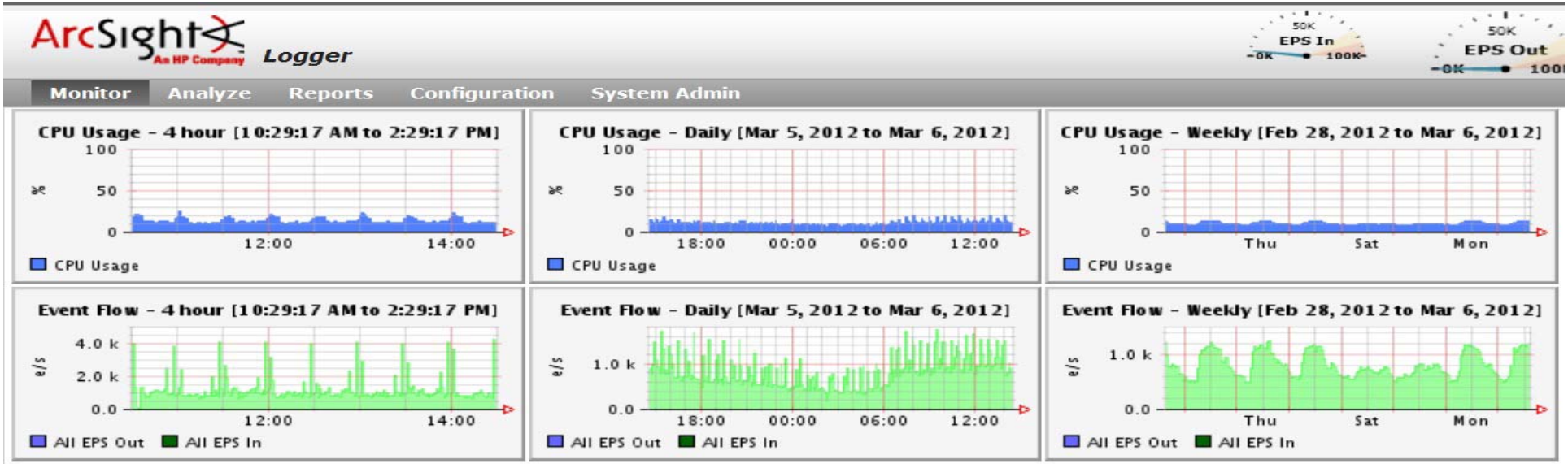
- Define specific tasks assigned to the SOC – e.g. detecting attacks from internet, monitoring compliance, detecting insider threats, incident response/forensic analysis, vulnerability review, etc
- Selecting SOC analysts experienced in networks, servers, and applications troubleshooting and intrusion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

Forming a Security Team



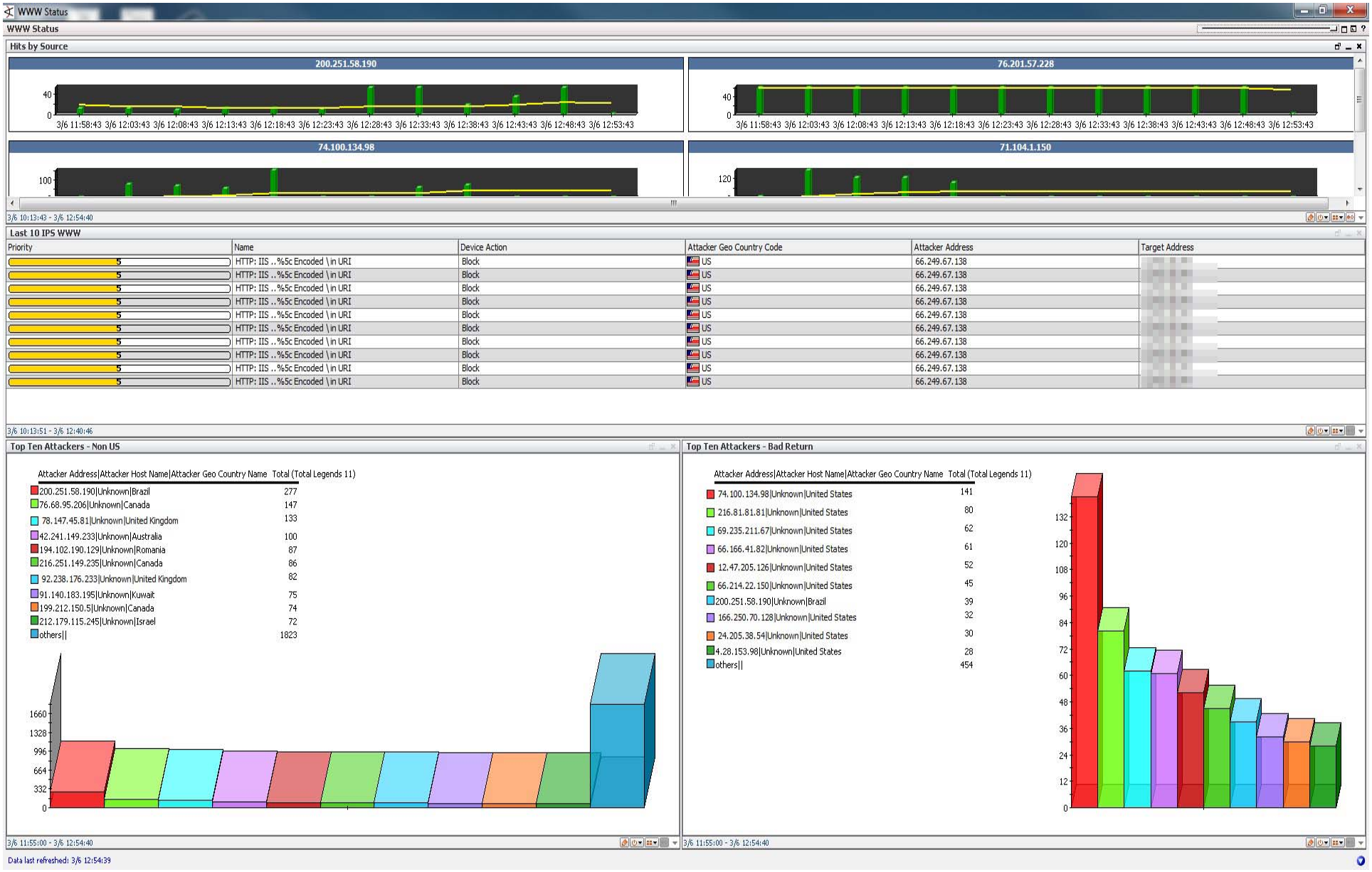
Designed by Bob Cheong
Version: 3.0

A Centralized Logger

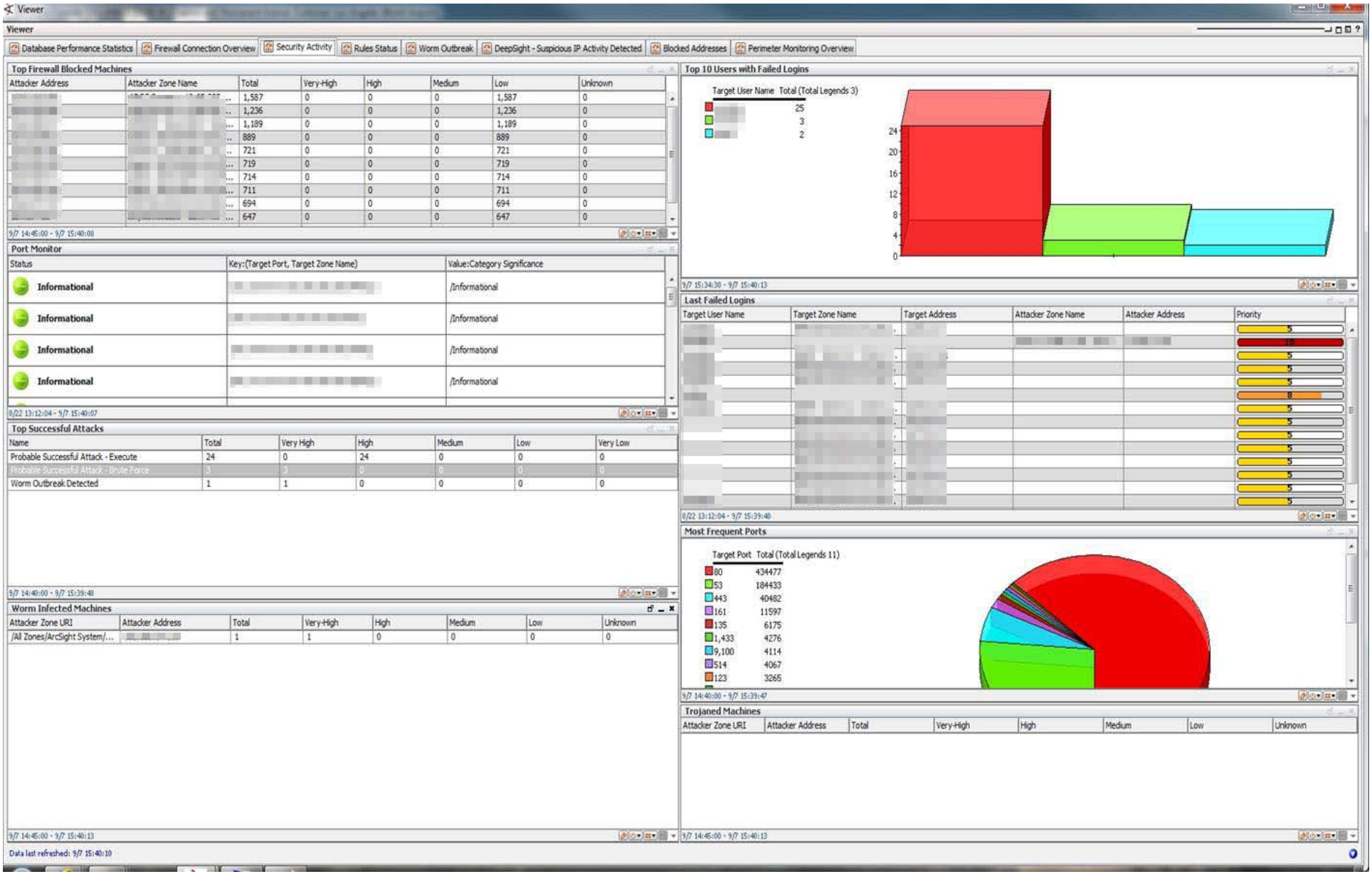


Receiver	Current EPS	Current Bytes/Second	Maximum EPS	Total Events
BCPSGF- Proxy	3,090 e/s	5,733,434 B/s	4,730 e/s	799,647,988 Events
MDHCPF-MS DHCP	0 e/s	0 B/s	4,255 e/s	15,047,446 Events
MDHCPF-MS DHCP-Badging	0 e/s	108 B/s	30 e/s	79,142 Events
MEMTLF-MS Exchange	9 e/s	10,175 B/s	4,650 e/s	39,155,435 Events
MIMSrF-	10 e/s	12,485 B/s	1,140 e/s	991,998 Events
MIMSrF-WWW	0 e/s	0 B/s	8,188 e/s	141,383,357 Events
MNSMDB- IPS	0 e/s	0 B/s	12 e/s	76,038 Events
MWELU-MS Domain Controller	30 e/s	35,466 B/s	3,602 e/s	1,410,917,182 Events
MWELU-MS Domain Controller-Badging	1 e/s	1,951 B/s	980 e/s	35,128,584 Events
SD- Syslog-TBIT	0 e/s	0 B/s	3,733 e/s	690,306,992 Events
SD- Firewall ScreenOS Syslog-TBIT	220 e/s	424,382 B/s	1,181 e/s	1,273,401,399 Events
SD- Syslog	550 e/s	879,399 B/s	4,130 e/s	3,668,138,250 Events
SD-Routers	0 e/s	0 B/s	56 e/s	1,856,927 Events
SEPDB- AV	0 e/s	724 B/s	317 e/s	4,827,598 Events
TSSE- IPS	0 e/s	265 B/s	5,300 e/s	4,171,457 Events
SD- ASA	0 e/s	0 B/s	100 e/s	2,109,665 Events
SD- ACS	0 e/s	272 B/s	57 e/s	7,491,267 Events
SD- SSL VPN	0 e/s	105 B/s	50 e/s	416,181 Events
SD- -Badging	0 e/s	0 B/s	1,520 e/s	510,812 Events

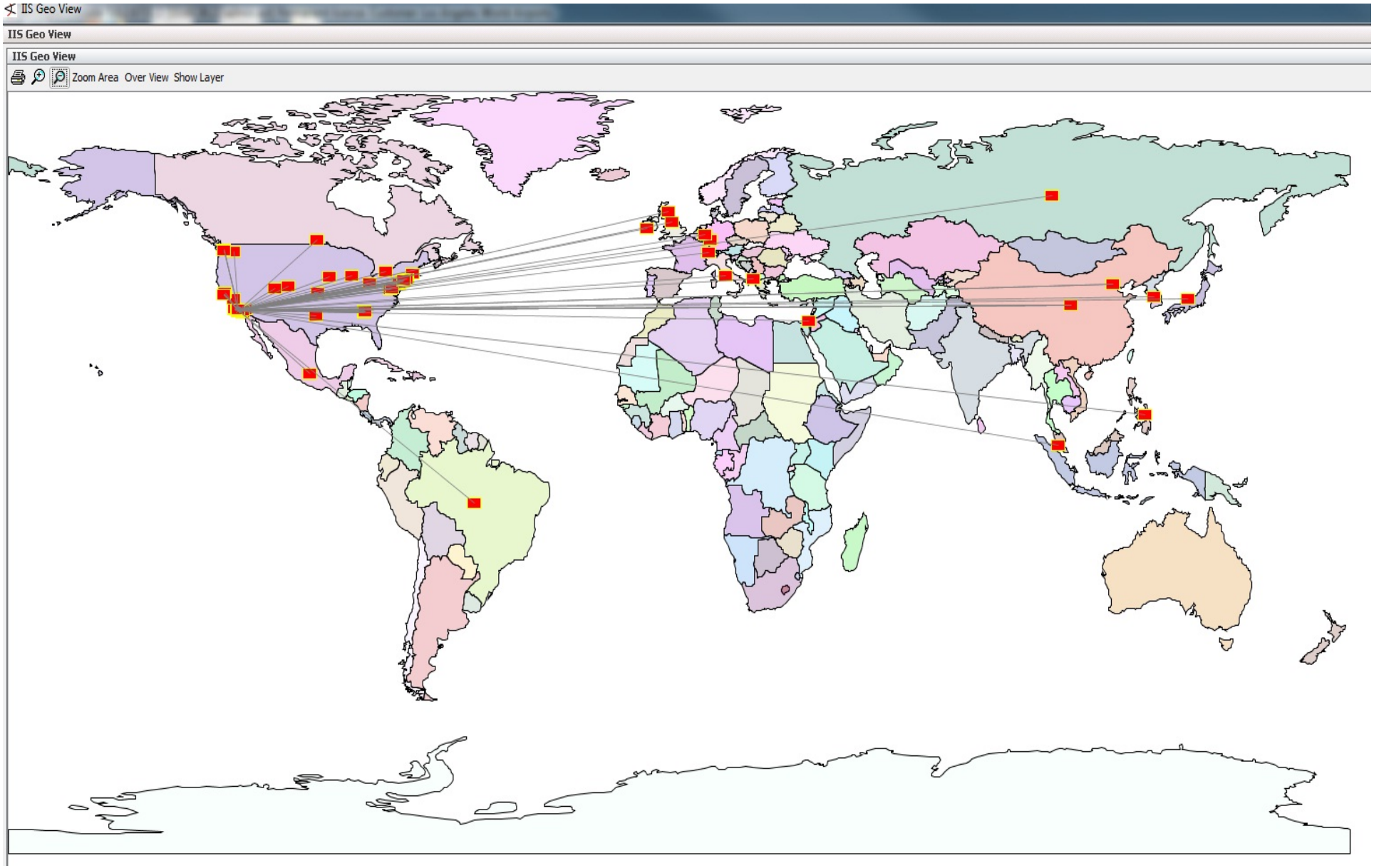
Security Monitoring Console



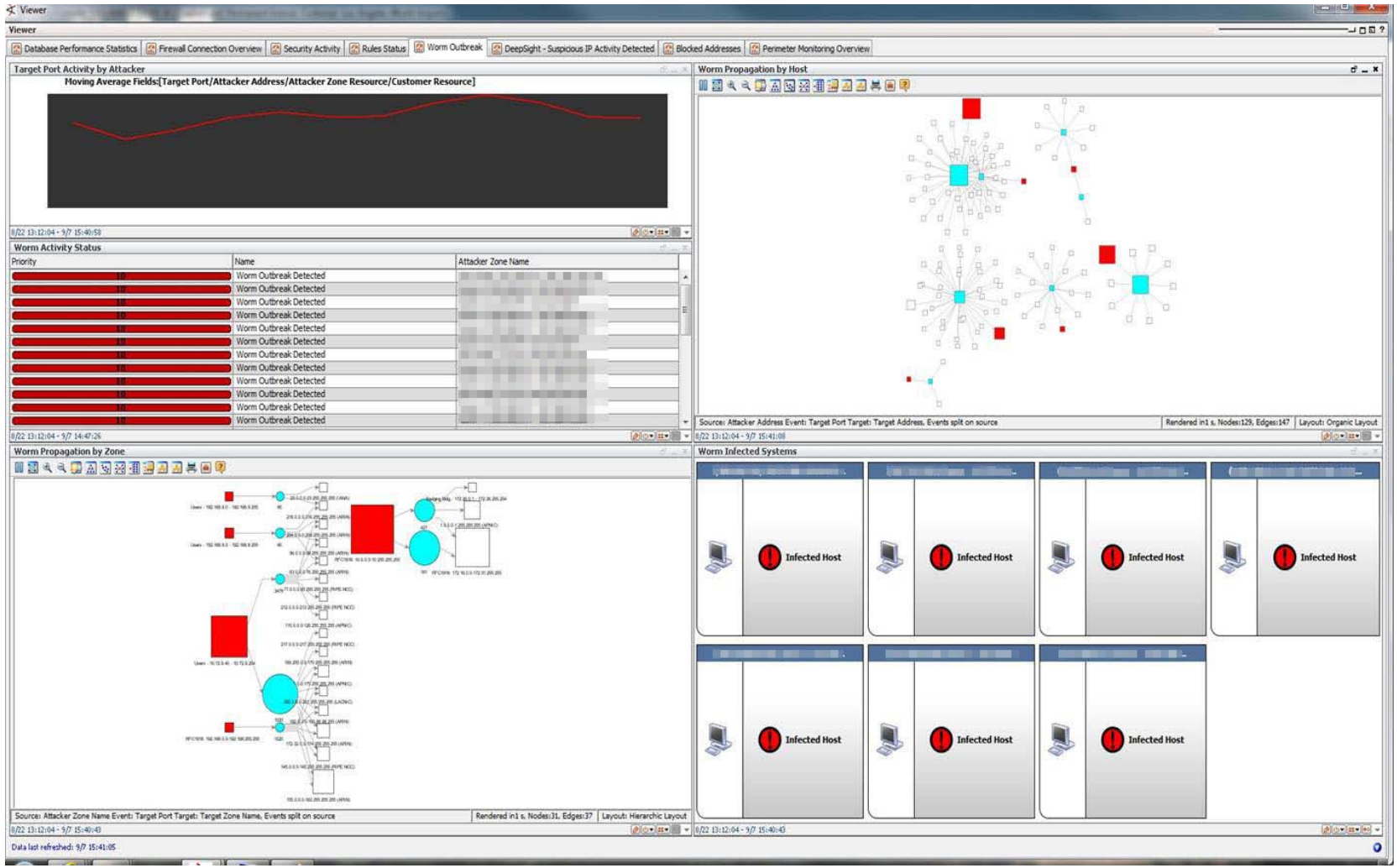
Security Monitoring Console



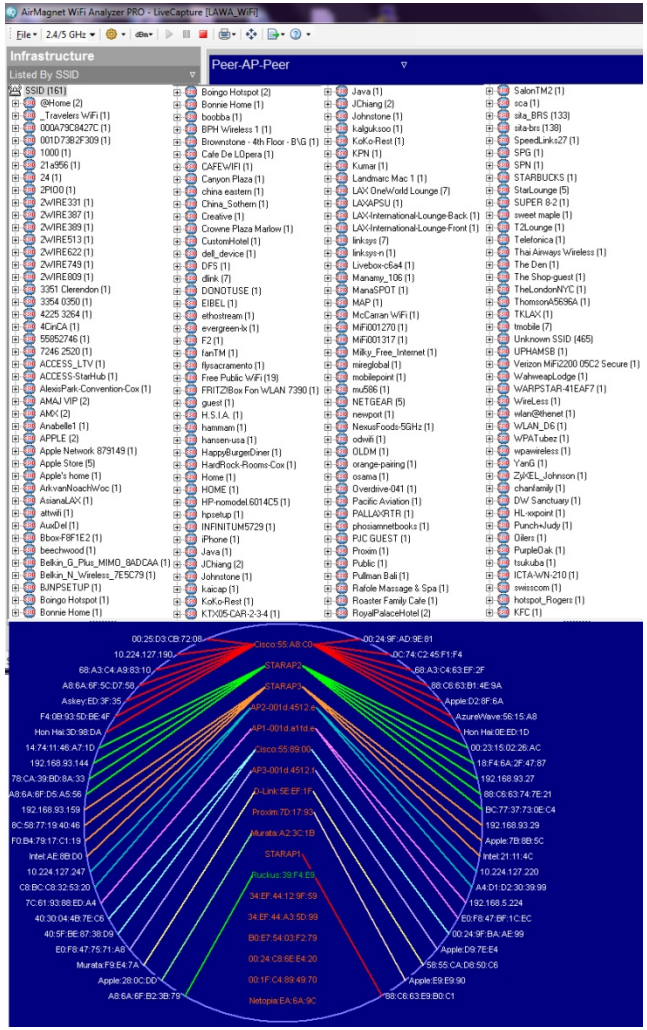
Global Access to LAWA.ORG



Detecting Malwares – viruses, bots, worms, trojans, rootkits, etc



Detecting Wireless Rogue Access Points



MS-ISAC – Multi-State Information Sharing & Analysis Center

LAWA Security Operation Center

Questions?