Building a Security Operations Center

Randy Marchany
VA Tech IT Security Office and Lab
marchany@vt.edu
VT Cyber Security Strategy

- University has 3 main business processes
  - Academic, Administrative, Research
- Academic
  - Open access needed – THE ISP MODEL
- Administrative
  - Traditional corporate security model
- Research
  - Hybrid
    - Open access
    - Restricted research, e.g. ITAR

Must design a strategy that covers all 3 areas
CyberSecurity Operations Center

- Security Operations Center (SOC) term is being taken over by physical surveillance companies
- We’re building a Cyber Security Operations Center (CSOC) that doesn’t have any physical surveillance capability.
- It could be a component of a SOC in the future
(C)SOC vs. NOC

• Network Operations Center usually responsible for monitoring and maintaining the overall network infrastructure. Its primary function is to ensure uninterrupted network service.

• CSOC leverages security related network activity to refine security incidents response.

• CSOC and NOC should complement each other and work in tandem.
Continuous Monitoring

- Keeping someone from getting inside has failed miserably
- Firewalls are not effective PROTECTION devices.
  - They are effective DETECTION devices
- Change the strategy
  - Assume they are in so go hunt for the compromised hosts
  - Monitor outbound traffic
  - Prevent their command and control communication
  - Inbound monitors server side attacks; outbound monitors client side attacks
Why?

• The CSOC is a logical place to collect, analyze and distribute data collected to support our Defense in Depth Strategy
  • Detecting **Network Based** Attacks
  • Detecting **Host Based** Attacks
  • Eliminating Security **Vulnerabilities**
  • Supporting **Authorized Users**
  • Providing tools for **Minimizing Business Loss**
Why?

• We want to measure and report compliance with our IT policies, state/federal laws and regulations
  • FERPA, HIPAA, PCI, ITAR, GLB, SOX
  • State Data Breach Notification Laws
  • VT Policies
  • 7010 Policy for Securing Technology Resources and Services 1/22/2007
  • 7025 Safeguarding Nonpublic Customer Information 5/12/2004
  • 7035 Privacy Policy for Employees’ Electronic Communications 3/14/2005
  • 7040 Personal Credentials for Enterprise Electronic Services 4/01/2008
  • 7100 Administrative Data Management and Access Policy 4/01/2008
  • 7105 Policy for Protecting University Information in Digital Form 7/1/2008
  • 7200 University IT Security Program 6/12/2006
  • 7205 IT Infrastructure, Architecture and Ongoing Operations 6/12/2006
  • 7210 IT Project Management 6/12/2006
  • 7215 IT Accessibility 6/12/2006
Where?

- OS Syslog/event logs, IDS logs, IPS logs, PID logs, Firewall logs, Pen Test Logs, PCI, netflow
- CSOC needs to be able to analyze and display this data quickly
- Data resides on separate, distributed servers
- CSOC pulls data from these servers as needed
- CSOC lives in the IT Security Office & Lab
What?

- Provides real-time view of the VT network’s security status
- Provides info to assess risk, attacks, mitigation
- Provide data for network forensics
- Provides metrics
  - Executive
  - Operational
  - Incident
What?

• Event Generators (E boxes)
  • Any form of IDS sensor (firewalls, IPS, IDS, Snort, Active Directory servers, Remedy, vulnerability scanners, TACACS, application software

• Most are Polling Generators
  • Generate specific event data in response to a specific action
  • Example: IDS or firewall
What?

- Events Databases (D boxes)
  - Provide basic storage, search and correlation tools for events collected and sent to the CSOC
  - Vulnerability databases contain info about security breaches, etc.
What?

• Events Reactions (R boxes)
• SOC Console
  • Used for internal analysis
  • Real-time monitors (Snort, Base, IPS, Dshield)
  • Incident Handling
  • Service Now trouble ticket system
  • Location tools
  • Statistical analysis
• End User Portals
  • Multi level reporting for various target audiences
    • Sysadmin, management
What?

• Analysis Engines (A Boxes)
  • Helps ID Analyst determine if an incident has occurred, its spread, its impact, etc.

• Knowledge Base Engines (K boxes)
  • Store security configs of critical assets, tips/tricks and effective solutions to previous problems

• Reaction and Report Engines (R boxes)
  • Switches, routers, IPS and associated management tools
Intrusion vs. Extrusion

- Intrusion detection is the process of identifying unauthorized activity by inspecting inbound network traffic.
- Extrusion detection is the process of identifying unauthorized activity by inspecting outbound network traffic.
- Network forensics is the art of collecting, protecting, analyzing and presenting network traffic to support remediation or prosecution.

(c) Marchany 2015
CM Security Principles

- Some intruders are smarter than you
- Many intruders are unpredictable
- Prevention eventually fails
- Defensible networks can be watched; they are monitored
- Defensible networks limit an intruder’s freedom to maneuver; they are controlled
- Defensible networks offer a minimum number of services and client-side applications; they are minimized
- Defensible networks can be kept current

- source: Extrusion Detection, R. Betjlich

(c) Marchany 2015
CM/SOC Implementation

- FireEyes
- Stonesoft
- Snort
- ITSO/Syslog
- Eventlog
- FW Logs
- Netflow/ARGUS
- VT Security Operations Center Data Flow
  4/29/14
  Color Codes:
  Blue – VT Network Sensors
  Red – RLAN only
  Purple – VT Network, NOVA and RLAN
  Green – disk storage
  Orange – ITSO “Silos”
  Yellow – Analysis Engines

- Netflow/ARGUS
- NAS
- Backups
- Stuples
- Projected

- NAS
- SIEM
- Central DISK FARM (proposed)
- HADOOP Cluster (Test)

- BRO (Future)
- Vulnerability Scanners
- Vulnerability Scanners DB
- Netscan
- Netscan DB

~50K events/day for most sensors
~65GB/day

(c) Marchany 2015
SOC Challenges

• Funding 😊
  • Commercial/Freeware + Infrastructure + Staff Salaries

• Training
  • 1st level needs specialized training
  • Not just point & clickers

• Process
  • Find the data, get access to the data
  • Help Desk Trouble Ticket process

• Technology
  • Backbone speeds, MPLS, IPV6
  • Sensor placement – inline or span port
ElasticSearch, Logstash, and Kibana

This is a test deployment of ELK for collecting and analyzing logs setup by the IT Security Office.

Dashboards:

- Logstash - Default Logstash Dashboard (Currently all Syslog)
- SSH Failures Dashboard - Dashboard describing information about SSH login failures
- SSH Login Activity - SSH Login Success and Failures
- Argus Dashboard - A simple dashboard displaying netflow/argus logs
- Apache Logs - A dashboard showing Apache logs
- Basic Windows Event Log - A basic logstash dashboard showing windows event log data
- Windows Event Log Logins - A dashboard showing successful and unsuccessful login attempts to the Windows servers.
- RLAN Firewall - Logs from the RLAN Firewall
- NAT - Dashboard detailing the NAT translations coming from the ASAs.
- Snort Dashboard - Dashboard showing Snort IDS alerts in the database
- DHCP Logs - Dashboard for logs from the DHCP servers
- Juniper Logs - Basic logs (primarily Junos Pulse) coming from Juniper machines.
- Radius Logs - Wireless and VPN
- General Security Dashboard - Dashboard showing various security-centric views of network traffic
- Marvel - Click "Developer Demo" to see performance and status of the ElasticSearch cluster
Netscan System

<table>
<thead>
<tr>
<th>Service</th>
<th>Hosts</th>
<th>Charts</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP</td>
<td></td>
<td>□ □ □</td>
<td>1462</td>
</tr>
<tr>
<td>SSH</td>
<td></td>
<td>□ □ □</td>
<td>3464</td>
</tr>
<tr>
<td>Telnet</td>
<td></td>
<td>□ □ □</td>
<td>1128</td>
</tr>
<tr>
<td>SMTP</td>
<td></td>
<td>□ □ □</td>
<td>1083</td>
</tr>
<tr>
<td>DNS</td>
<td></td>
<td>□ □ □</td>
<td>571</td>
</tr>
<tr>
<td>HTTP</td>
<td></td>
<td>□ □ □</td>
<td>3482</td>
</tr>
<tr>
<td>POP3</td>
<td></td>
<td>□ □ □</td>
<td>420</td>
</tr>
<tr>
<td>MS-EFS</td>
<td></td>
<td>□ □ □</td>
<td>4253</td>
</tr>
<tr>
<td>NetBIOS</td>
<td></td>
<td>□ □ □</td>
<td>3342</td>
</tr>
<tr>
<td>IMAP</td>
<td></td>
<td>□ □ □</td>
<td>429</td>
</tr>
<tr>
<td>LDAP</td>
<td></td>
<td>□ □ □</td>
<td>530</td>
</tr>
<tr>
<td>HTTP SSL</td>
<td></td>
<td>□ □ □</td>
<td>2884</td>
</tr>
<tr>
<td>MicroSoft-DSS</td>
<td></td>
<td>□ □ □</td>
<td>3469</td>
</tr>
<tr>
<td>AppleTalk</td>
<td></td>
<td>□ □ □</td>
<td>587</td>
</tr>
<tr>
<td>LDAP SSL</td>
<td></td>
<td>□ □ □</td>
<td>507</td>
</tr>
<tr>
<td>IMAP SSL</td>
<td></td>
<td>□ □ □</td>
<td>472</td>
</tr>
<tr>
<td>POP3 SSL</td>
<td></td>
<td>□ □ □</td>
<td>432</td>
</tr>
<tr>
<td>MS-SQL</td>
<td></td>
<td>□ □ □</td>
<td>434</td>
</tr>
<tr>
<td>Oracle</td>
<td></td>
<td>□ □ □</td>
<td>390</td>
</tr>
<tr>
<td>ORASRV</td>
<td></td>
<td>□ □ □</td>
<td>382</td>
</tr>
<tr>
<td>NFS</td>
<td></td>
<td>□ □ □</td>
<td>599</td>
</tr>
<tr>
<td>Squid</td>
<td></td>
<td>□ □ □</td>
<td>391</td>
</tr>
<tr>
<td>MySQL</td>
<td></td>
<td>□ □ □</td>
<td>495</td>
</tr>
<tr>
<td>RDF</td>
<td></td>
<td>□ □ □</td>
<td>2533</td>
</tr>
<tr>
<td>FileMaker</td>
<td></td>
<td>□ □ □</td>
<td>394</td>
</tr>
<tr>
<td>Postgres</td>
<td></td>
<td>□ □ □</td>
<td>401</td>
</tr>
<tr>
<td>VNC</td>
<td></td>
<td>□ □ □</td>
<td>1546</td>
</tr>
<tr>
<td>TOR Relay or Cisco XRemote</td>
<td></td>
<td>□ □ □</td>
<td>403</td>
</tr>
<tr>
<td>DB2</td>
<td></td>
<td>□ □ □</td>
<td>394</td>
</tr>
</tbody>
</table>
Distributed Intrusion Detection System

Virginia Tech DShield

Records Added

Last Month: 12,441,646  Last Week: 3,347,949  Today: 864,122

As of November 04, 2008 09:13 pm GMT

Target Map  Attacker Map

Most Attacked: 128.173.8.62  Most Attacked Port: 1900
Top Destination Ports - By Connection

Apr 01, 2015 to Apr 15, 2015 - ITSO Argus Data

Connections

Port Number

- 80: 18999
- 53: 13961
- 443: 13534
- 123: 7215
- 22: 3318
- 993: 1312
- 25: 1253
- 137: 878
- 445: 847
- 8080: 807
### Top Source & Destination Countries - By Connection

April 01, 2015 to April 15, 2015 - ITSO Argus Data

<table>
<thead>
<tr>
<th>Country Code</th>
<th>Country Name</th>
<th>Source Count</th>
<th>Destination Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>CN</td>
<td>China</td>
<td>8743</td>
<td>2137</td>
</tr>
<tr>
<td>US</td>
<td>United States</td>
<td>66071</td>
<td>88660</td>
</tr>
</tbody>
</table>
## ASSETS

<table>
<thead>
<tr>
<th>Asset Name</th>
<th>IP Address</th>
<th>Application</th>
<th>Asset Type</th>
<th>Location</th>
<th>Criticality</th>
</tr>
</thead>
<tbody>
<tr>
<td>vt.edu</td>
<td>198.82.173.1</td>
<td>Vendor Maintenance, Tuition Remission for Graduate School, Travel Reimbursement, Student Accounts, Sponsored Programs, Purchasing (SciQuest, eVA), Processing to report to the state, Payment Gateway (Infinet), General Accounting, Fund Management, Fixed Assets and Inventory Control, Effort Reporting, Cash Receipts, Budgeting, Banner Student Accounts, Receivable Accounts Payable, Travel Reimbursement, Student Accounts, Sponsored Programs, Purchasing (SciQuest, eVA), Processing to report to the state, Payment Gateway (Infinet)</td>
<td>Production Linux Server</td>
<td>AISB</td>
<td>4.29</td>
</tr>
</tbody>
</table>
Futures

• There are commercial tools that do all of this
• They cost lots of $$$
• We don’t have lots of $$$
• Had to grow our own
• Improves our skill set, proactive and reactive capabilities
• We can better evaluate commercial products because of our experience
Reference

• Reference paper “Security Operation Center Concepts & Implementation” by Renaud Bidou

• We used this as our blueprint
Contact Information

- Randy Marchany
- VA Tech IT Security Office & Lab
- 1300 Torgersen Hall
- Blacksburg, VA 24060
- 540-231-9523
- marchany@vt.edu
- http://security.vt.edu
- Twitter: @randymarchany
- Randymarchany.blogspot.com