Three Phases of Security
Security Analyst: Tools of the Trade

Patrick Lane, M.Ed., Security+, Network+, CISSP, MCSE
Senior Manager, Product Development
Product Manager for:
CompTIA Security+
CompTIA Cybersecurity Analyst (CSA+)
CompTIA Advanced Security Practitioner (CASP)
CompTIA Server+
1. Why have security analyst skills become so important?
2. What tools do security analysts use?
3. How does a SIEM work – unified security management?
4. How is threat intelligence integrated?
5. Real-world examples
   - Splunk: Database hack discovered
   - LogRhythm: Financial server hack discovered
   - AlienVault: Brute force attack discovered
Why have security analyst skills become so important?
• Wake up call for the IT security world
• Brought widespread attention to the “Advanced Persistent Threat”
• Demonstrated that traditional security tools, such as firewalls and anti-virus, do not alone protect networks
• Recent high profile attacks at Yahoo! and Democratic National Committee (DNC)
The Advanced Persistent Threat (APT)

Characteristics:

- Never stop
- Often highly coordinated / state sponsored
- Bad actors lurk on systems and networks
- Hard to detect
Lessons Learned

We must apply behavioral analytics to the IT security market to improve the overall state of IT security.

• We must focus on network behavior in an organization’s interior network
• We must identify network anomalies that indicate bad behavior

We must train IT security professionals security analyst skills, which include:

✓ Threat management
✓ Vulnerability management
✓ Cyber incident response
✓ Security and architecture tool sets
TOTAL NUMBER OF JOB POSTINGS:

Security Analyst Job Role

175% increase from 2012 to 2015. Data for U.S. only, but reflects an international need.

Source: Burning Glass Technologies Labor Insights, January 2016
Additional Indicators

The U.S. Bureau of Labor Statistics predicts that information security analysts will be the *fastest growing job category*, with 37% overall growth between 2012 and 2022.*

In an analysis of recent U.S. Bureau of Labor Statistics data, information security analysts saw an 8% bump in growth over the first three months of 2016. *That’s a new BLS record.**

8 in 10 managers indicate that IT security certifications are very valuable (38%) or valuable (42%) in terms of validating security-related knowledge/skills or evaluating job candidates.***

* CompTIA, Trends in Information Security 2015
** U.S. Bureau of Labor Statistics data
*** International Trends in Cybersecurity, CompTIA, 2016
(Quick Advertisement)

CompTIA Cybersecurity Analyst (CSA+) Certification
Developed to address the need for IT Security Analysts.

As attackers have learned to evade traditional signature-based solutions, an analytics-based approach has become extremely important. CSA+ applies behavioral analytics to the IT security market to improve the overall state of security.
2 What tools do security analysts use?
## Tools of the Trade – Open Source

<table>
<thead>
<tr>
<th>Open source software</th>
<th>Description</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireshark</td>
<td>Network protocol analyzer / packet capture tool</td>
<td><a href="https://www.wireshark.org">https://www.wireshark.org</a></td>
</tr>
<tr>
<td>Bro and/or Snort</td>
<td>Network intrusion detection systems (NIDS)</td>
<td><a href="https://www.bro.org">https://www.bro.org</a> <a href="https://www.snort.org">https://www.snort.org</a></td>
</tr>
</tbody>
</table>
Security Information and Event Management (SIEM) software

• All about logs
  – To constantly aggregate and analyze internal and external network logs
  – To quickly prevent breaches or perform incident response using these logs

• What does it address?
  – Threat management
  – Incident response
  – Compliance

• 80% of SIEMs are funded to close a compliance gap

• Security Operations Center (SOC)
  – Security Analyst, SOC Analyst, Vulnerability Analyst, Cybersecurity Specialist
  – Threat Intelligence Analyst, Security Engineer
<table>
<thead>
<tr>
<th>Vendor-specific software</th>
<th>Description</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manager</td>
<td>detection</td>
<td></td>
</tr>
<tr>
<td>AlienVault Unified Security Management (USM)</td>
<td>SIEM, threat</td>
<td><a href="https://www.alienvault.com/products">https://www.alienvault.com/products</a></td>
</tr>
</tbody>
</table>
## Tools of the Trade – Vendor Specific

<table>
<thead>
<tr>
<th>Vendor-specific software</th>
<th>Description</th>
<th>URL</th>
</tr>
</thead>
</table>
SIEM
Example
How does a SIEM work – unified security management?
OSSIM

• AlienVault Open Source SIEM (OSSIM) – free, but no support
• AlienVault USM is commercial version ($32K). What it does:
  – External Data Sources: applications and devices that generate events
  – Sensors: collect and normalize events
  – Server: conducts risk assessment, correlation directives and storage of events in an SQL database (SIEM)
  – Storage: events are digitally signed and time stamped in a massive storage system, usually NAS or SAN, called Logger, that includes an additional database for forensics.
  – Web Interface - provides a reporting system, metrics, reports, dashboards, ticketing system, vulnerability management system, real-time network information
Source: LogRhythm’s Unified Security Intelligence Platform
OSSIM Installation

• OSSIM .ISO image includes Linux Debian, OSSIM, and OSSIM agent software
  – AlienVault_OSSIM_64bits_5.3.2.iso (630 MB)

• Implement on virtual machine
• Needs power – AWS or Azure recommended
OSSIM Agents and Plug Ins

- SIEMs work best in a large organization with multiple network devices, such as firewalls, IDS/IPS, anti-virus, web servers, etc.
- To collect logs from hosts
  - Install agents, such as OSSEC (Linux) and Snare (Windows)
- To connect data-sources to OSSIM server
  - Install plug-ins (XML-based configuration file) at data source
  - Plug-ins integrated into many security tools:
    - CheckPoint, Cisco, Citrix, Exchange, IIS, Syslog, Wmi, Nessus, Anti-virus (Sophos, Symantec, McAfee, Avast), OSSEC, Snare
    - Apache, Snort, Ntop, Nmap, OpenVAS, P0f, Pads, Arpwatch, OSSEC, Osiris, Nagios, OCS, Kismet
Correlation

• Separates SIEM from IDS/IPS using intelligence
• Reduces false positives
• Calculates multiple input events and alarms into a more manageable number of events to address
• Cross Correlation
  – Works only with events that have defined destination IP addresses
  – Checks IP address in database to determine any vulnerabilities
  – Changes the reliability value of the event, which is used to calculate risk
  – Removes a lot of alarms
Correlation (cont’d)

• Correlation Directive
  – Generates an alarm by following rules
  – Rules written in XML (there can be thousands – most preconfigured)
  – Analyze multiple events and decide whether to raise an alarm or not
    • E.g., multiple login attempts into a web server using SSH
  – Capable of identifying zero-day attacks, since it uses rules based on behavior
Risk Calculation

- OSSIM data management:
  - Raw logs
  - Events
  - Alarms
  - Tickets
- Raw logs are sent to OSSIM server and normalized
- The logs become events
- Alarms are raised when the risk value of event is $\geq 1$ on a scale to 10.
  
  \[
  \text{RISK OF THE EVENT} = \frac{\text{ASSET VALUE}(0-5) \times \text{PRIORITY}(0-5) \times \text{RELIABILITY}(0-10)}{25}
  \]
- Tickets are manually or automatically created in OSSIM after reviewing alarms. Assigned to appropriate personnel.
Reporting

- Highly scalable
- Easy to use
- Schedule reports and e-mail
How is threat intelligence integrated?
Threat Intelligence

Unified Security Management

- Assess the Network
  - Find devices on your network, what’s installed on them, & vulnerabilities

- Find Threats
  - Detect active threats & exploits on your network

- Respond to Incidents
  - Analyze the threat & learn how to remediate

Open Threat Exchange

- Investigate & Collaborate
  - Automatically share anonymous threat information with the OTX community

Measure & Improve

Source: https://www.alienvault.com/products
5 Real world examples
LogRhythm: Financial Server Hack Discovered
Top Common Event:
- File Monitoring Event - Access
- User Account Attribute Modified
- Account Added To Group
- User Account Deleted
- Policy Enabled - System
- User Logon
- Initialize Object Failure
- User Account Created
- Account Enabled
- General Web Access

Top Classification:
- Access Success
- Access Grant
- Account Modified
- Account Deleted
- Policy
- Authentication Success
- Access Failure
- Account Created
- Account

Top User (Impacted):
- Steven Jacobs: 8,000

Top Host (Origin):
- us-finsvr001*: 9,000

Top URL:
- http://www.drop...

Temporary User:
- us-finsvr001 accessed

Dropbox accessed
Splunk: Database Hack Discovered
Critical database server access attempts.

Series of random brute force attacks to cloud web server 01-07

The attack carried out in 2 different intervals, 8 min after the initial first series of attacks.

<table>
<thead>
<tr>
<th>_time</th>
<th>src</th>
<th>dest</th>
<th>user</th>
<th>COMMENTTEXT</th>
<th>SQLTEXT</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016-11-03 08:33:12</td>
<td>10.1.21.153</td>
<td>DATABASE-001</td>
<td>hax0r</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2016-11-03 08:32:48</td>
<td>10.1.21.153</td>
<td>DATABASE-001</td>
<td>hax0r</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2016-11-03 08:32:40</td>
<td>10.1.21.153</td>
<td>DATABASE-001</td>
<td>ORACLE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2016-11-03 08:31:50</td>
<td>10.1.21.153</td>
<td>DATABASE-001</td>
<td>ORACLE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

> Privilege user activities and multiple user activities

> Various privilege change SQL and access to sensitive info

<table>
<thead>
<tr>
<th>SQL</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SELECT * FROM cust_info.svc;</td>
<td></td>
</tr>
<tr>
<td>UPDATE SET perm.app_svc_defin = allow WHERE id.app_svc_defin = hax0r;</td>
<td></td>
</tr>
<tr>
<td>GRANT privileges ON app_svc_defin TO user hax0r;</td>
<td></td>
</tr>
<tr>
<td>SELECT * FROM ALL_USERS;</td>
<td></td>
</tr>
</tbody>
</table>

> Successful long activities followed by failed login
AlienVault: 
Bruteforce attack discovered
Alarm Details List

DELIVERY & ATTACK: BRUTEFORCE AUTHENTICATION
ATTACK PATTERN: EXTERNAL TO INTERNAL ONE-TO-ONE

OPEN & CLOSED ALARMS
TOTAL EVENTS: 7
DURATION: 4 SECS
ELAPSED TIME: 2 HOURS

Source: https://www.alienvault.com/products
Thank You

Questions?