Three easy ways to enhance security monitoring

Vijay Gupta, Sr. Software Designer

#HPProtect
Agenda

Security issues
Security monitoring
HP Solutions
Security issues

Resources

User

Roles and privileges

Sensitive information
Security monitoring

HP ArcSight ESM

HP ArcSight Connector
# Security monitoring

## Security events in ESM

<table>
<thead>
<tr>
<th>End Time</th>
<th>Name</th>
<th>Source Address</th>
<th>Source Host Name</th>
<th>Destination Addr</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 Sep 2012 13:49:46 PDT</td>
<td>CF FW In Action:accept Service nname Rule:5 (Sec ...</td>
<td>10.0.20.21</td>
<td>w2ksj101.sj1.west.arcnet.c...</td>
<td>206.98.142.116</td>
</tr>
<tr>
<td>3 Sep 2012 13:38:12 PDT</td>
<td>CF FW In Action:accept Service nname Rule:5 (Sec ...</td>
<td>10.0.20.21</td>
<td>w2ksj101.sj1.west.arcnet.c...</td>
<td>199.248.65.119</td>
</tr>
<tr>
<td>3 Sep 2012 13:30:12 PDT</td>
<td>CF FW In Action:accept Service nname Rule:5 (Sec ...</td>
<td>10.0.20.21</td>
<td>w2ksj101.sj1.west.arcnet.c...</td>
<td>199.248.65.119</td>
</tr>
<tr>
<td>3 Sep 2012 13:38:11 PDT</td>
<td>CF FW In Action:accept Service ftp Rule:5 (Sec Log)</td>
<td>10.0.20.21</td>
<td>w2ksj101.sj1.west.arcnet.c...</td>
<td>199.248.65.119</td>
</tr>
<tr>
<td>3 Sep 2012 13:38:11 PDT</td>
<td>CF FW In Action:accept Service ftp Rule:5 (Sec Log)</td>
<td>10.0.20.21</td>
<td>w2ksj101.sj1.west.arcnet.c...</td>
<td>199.248.65.119</td>
</tr>
<tr>
<td>3 Sep 2012 13:38:11 PDT</td>
<td>CF FW In Action:accept Service time-udp Rule:5 (Sec ...</td>
<td>10.0.20.21</td>
<td>w2ksj101.sj1.west.arcnet.c...</td>
<td>192.168.111.9</td>
</tr>
<tr>
<td>3 Sep 2012 13:38:11 PDT</td>
<td>CF FW In Action:accept Service nmp-udp Rule:5 (Sec ...</td>
<td>10.0.20.21</td>
<td>w2ksj101.sj1.west.arcnet.c...</td>
<td>192.168.111.9</td>
</tr>
<tr>
<td>3 Sep 2012 13:38:11 PDT</td>
<td>SQL injection</td>
<td>10.0.20.21</td>
<td>w2ksj101.sj1.west.arcnet.c...</td>
<td>10.10.10.10</td>
</tr>
<tr>
<td>3 Sep 2012 13:38:11 PDT</td>
<td>XSS Attempt</td>
<td>10.0.20.21</td>
<td>w2ksj101.sj1.west.arcnet.c...</td>
<td>10.10.10.10</td>
</tr>
<tr>
<td>3 Sep 2012 13:38:11 PDT</td>
<td>SQL injection</td>
<td>10.0.20.21</td>
<td>w2ksj101.sj1.west.arcnet.c...</td>
<td>16.10.10.20</td>
</tr>
<tr>
<td>3 Sep 2012 13:38:10 PDT</td>
<td>CF FW In Action:accept Service time-udp Rule:5 (Sec ...</td>
<td>10.0.20.21</td>
<td>w2ksj101.sj1.west.arcnet.c...</td>
<td>192.168.111.9</td>
</tr>
<tr>
<td>3 Sep 2012 13:38:10 PDT</td>
<td>CF FW In Action:accept Service time-udp Rule:5 (Sec ...</td>
<td>10.0.20.21</td>
<td>w2ksj101.sj1.west.arcnet.c...</td>
<td>192.168.111.9</td>
</tr>
<tr>
<td>3 Sep 2012 13:38:06 PDT</td>
<td>CF FW In Action:accept Service nname Rule:5 (Sec ...</td>
<td>10.0.20.21</td>
<td>w2ksj101.sj1.west.arcnet.c...</td>
<td>206.98.142.116</td>
</tr>
<tr>
<td>3 Sep 2012 13:38:06 PDT</td>
<td>CF FW In Action:accept Service nname Rule:5 (Sec ...</td>
<td>10.0.20.21</td>
<td>w2ksj101.sj1.west.arcnet.c...</td>
<td>206.98.142.116</td>
</tr>
<tr>
<td>3 Sep 2012 13:38:06 PDT</td>
<td>CF FW In Action:accept Service nname Rule:5 (Sec ...</td>
<td>10.0.20.21</td>
<td>w2ksj101.sj1.west.arcnet.c...</td>
<td>199.248.65.119</td>
</tr>
<tr>
<td>3 Sep 2012 13:38:06 PDT</td>
<td>CF FW In Action:accept Service nname Rule:5 (Sec ...</td>
<td>10.0.20.21</td>
<td>w2ksj101.sj1.west.arcnet.c...</td>
<td>199.248.65.119</td>
</tr>
<tr>
<td>3 Sep 2012 13:38:06 PDT</td>
<td>USB insert</td>
<td>10.0.20.21</td>
<td>w2ksj101.sj1.west.arcnet.c...</td>
<td>199.248.65.119</td>
</tr>
</tbody>
</table>
A typical security event:
User john.doe accessed a (top secret) file

- Who is john.doe?
- Which department does he work in?
- What is he authorized to do?
Actor Model Import Connectors

Import user profiles (Actors) into ESM

- Profiles along with accounts and roles
- Various sources like Active Directory, Oracle IDM, and many other databases
- Real time updates for new, removed, or changed profiles
### Actor Model Import Connectors

Import user profiles (Actors) into ESM

<table>
<thead>
<tr>
<th>Name</th>
<th>Attacker Address</th>
<th>role</th>
<th>status</th>
<th>identity</th>
<th>Manager</th>
<th>Attacker Port</th>
<th>Target Address</th>
<th>Target Host Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>sqlplus login</td>
<td>10.1.1.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4535</td>
<td>192.168.10.10</td>
<td>finance.arcsgight.com</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Attacker Address</th>
<th>role</th>
<th>status</th>
<th>identity</th>
<th>Manager</th>
<th>Attacker Port</th>
<th>Target Address</th>
<th>Target Host Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>sqlplus login</td>
<td>10.1.1.1</td>
<td>Consultant</td>
<td>Inactive</td>
<td>Morris Hicks</td>
<td>John Doe</td>
<td>4535</td>
<td>192.168.10.10</td>
<td>finance.arcsgight.com</td>
</tr>
</tbody>
</table>
Security event

A typical security event with Actors:
User john.doe accessed a (top secret) file

• Who is john.doe? Senior Architect
• Which department does he work in? Government Initiatives
• What is he authorized to do? Access top secret files
Security issues

Roles and privileges

Resources

User

Sensitive information
Security issues

Roles and privileges

User

Resources

Sensitive information
Security event

A typical security event:
User john.doe accessed a (top secret) file located at 10.0.26.9

• Where is this host located?
• What kind of data is present on this host?
• Are there any system/application vulnerabilities?
Asset Model Import Connectors

Import asset information into ESM

- Information like host name, IP address, MAC address
- Assign location, network zone, categories, vulnerabilities
- Real time updates for new, removed and changed asset information
Security event

A typical security event with Assets:
User john.doe accessed a (top secret) file located at 10.0.26.9

- Where is this host located? Headquarters
- What kind of data is present on this host? NASA's mission to Mars
- Are there any system/application vulnerabilities? None
Security issues

Roles and privileges

User

Resources

Sensitive information
Security issues

Roles and privileges

Resources

User

Sensitive information
Security event

A typical security event:
User john.doe accessed a (top secret) file located at 10.0.26.9 from xxx.78.195.166

- Where does it come from?
- Do we know anything about it?
- Is there any threat?
Model Import Connector for RepSM

RepSM = Reputation Security Monitor

Import RepDV data into ESM
Reputation Digital Vaccine

Or RepDV

Internet reputation data feed from HP TippingPoint

• Provides security intelligence feed
• Categorizes IP addresses and domains
• Calculates severity
Model Import Connector for RepSM

RepSM = Reputation Security Monitor

Import RepDV data into ESM

• Malicious IP addresses, domains
• Threat type, threat score
• Real time updates
Security Event

A typical security event with RepSM:
User john.doe accessed a (top secret) file located at 10.0.26.9 from xxx.78.195.166

• Where does it come from? **External**
• Do we know anything about it? **Threat type ‘Abuse and Misuse’**
• Is there a threat? **Threat score 80%**
Security issues

Enhanced

Resources

User

Roles and privileges

Denied!

Sensitive information
For more information

Attend these sessions
- TB3295, Network modeling: A real world example
- TB3262, Catching malicious insiders through behavioral analytics

Visit these demos
- HP ArcSight ESM Demo Station
- HP ArcSight Threat Central Demo Station

After the event
- Contact your sales rep
- Visit the https://protect724.hp.com/community/events/protect-conference

Your feedback is important to us. Please take a few minutes to complete the session survey.
Please give me your feedback

**Session** TT3070  **Speaker** Vijay Gupta

Please fill out a survey.

Hand it to the door monitor on your way out.

Thank you for providing your feedback, which helps us enhance content for future events.
Thank you