Contextualizing Your Logs

Why and How?

#OReillySecurity
DEFENSE is DIFFICULT
Without context, a piece of information is just a dot. It floats in your brain with a lot of other dots and doesn't mean a damn thing. Knowledge is information-in-context ... connecting the dots.

- Michael Ventura

#OReillySecurity
99 Problems and a log ain’t 1

IPS
Proxy
FW

Web Application
Web Server

Threat Intel Feeds
(N/H)IDS

Netflow
AV

EDR

User Info
DB

I’m here for the logs
Analyst: First Person View
Signal to Noise

Signal-to-noise ratio is defined as the ratio of the power of a signal (meaningful information) and the power of background noise (unwanted signal)

\[ \text{SNR} = \frac{P_{\text{signal}}}{P_{\text{noise}}}, \]
Benefits of Context

• Builds in Institutional knowledge
• Smarter alerts
• Help triage alerts
• Speed up analysis

#OReillySecurity
# What Kind of Context?

<table>
<thead>
<tr>
<th>Type</th>
<th>Value</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>What area of the network does it represent?</td>
<td>Dept. of Transportation Proxy IP</td>
</tr>
<tr>
<td>Host</td>
<td>What kind of host is this?</td>
<td>Workstation Server Mobile device Data Leakage case #222</td>
</tr>
<tr>
<td>User</td>
<td>Who is this user?</td>
<td>Admin HUG Contractor This user is on the “leavers” list</td>
</tr>
</tbody>
</table>
Context Down the Stack

Alert: Attack-Apache Struts
Tag: IIS Server

email: ceo@biz.com
Tag: HUG

Alert: PUP
Tag: 22 alerts today

IP: 1.2.3.4
Tag: OWA Server

URL: myurl.com
Tag: Ref: Case#223

EVT Logs
user: phillips
hostname: win7dst
Tag: Admin

Alert: Process Injected
Hostname: winsrv89
Tag: Critical Server

#OReillySecurity
Splunk: Tags & Event types

Tags...

• annotate your search results
• can be applied to event types
• can be used to identify different event types within a single data source.
• can be used to track abstract field values (e.g. IP addresses, ID numbers)

Event types...

• are a categorization system to help you make sense of your data.
• let you sift through huge amounts of data, find similar patterns, and create alerts and reports.
• help normalize unfamiliar data

#OReillySecurity
Building in Context

Prior Policy Violation

Event types ➔ Prior Policy Violation

Search string:
index=* customer_name="Hayden Holman"

Tag(s):
prior_policy_violation

Event Actions

<table>
<thead>
<tr>
<th>Type</th>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>host</td>
<td>fileserver</td>
<td></td>
</tr>
<tr>
<td>source</td>
<td>/var/log/fileserver.log</td>
<td></td>
</tr>
<tr>
<td>sourcetype</td>
<td>ri:pas:file</td>
<td></td>
</tr>
<tr>
<td>command</td>
<td>getattrib</td>
<td></td>
</tr>
<tr>
<td>customer_name</td>
<td>Hayden Holman</td>
<td></td>
</tr>
<tr>
<td>department</td>
<td>Research</td>
<td></td>
</tr>
<tr>
<td>department_group</td>
<td>Education</td>
<td></td>
</tr>
<tr>
<td>eventtype</td>
<td>ri:pas:file (audit_change_pas)</td>
<td></td>
</tr>
</tbody>
</table>

#OReillySecurity
Building in Context

#OReillySecurity
Smarter Analysis

<table>
<thead>
<tr>
<th>src_ip</th>
<th>tag</th>
<th>user_id</th>
<th>department</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.51.210.42</td>
<td>audit</td>
<td>jbell</td>
<td>Marketing</td>
</tr>
<tr>
<td></td>
<td>buildingA</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>change</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>pas</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>read</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>src_ip</th>
<th>tag</th>
<th>user_id</th>
<th>department</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.51.210.42</td>
<td>audit</td>
<td>sallen</td>
<td>Marketing</td>
</tr>
<tr>
<td></td>
<td>buildingA</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>change</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>pas</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>read</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#OReillySecurity
Faster Triaging

#OReillySecurity
BYOT (Bring Your Own Tags)
loggin' off

#OReillySecurity