TECH TALKS: SUPPORTING THE REMOTE WORKFORCE

Aggregating, Analyzing, Alerting on VPN & Firewall Logs
Panelists today

Host: Brad Six
Technical Product Evangelist

Guest Speaker: Nick Carstensen
Security & Integrations Product Manager

- Enter comments anytime via Q&A Window at the bottom
- Recording of today’s Tech Talk will be e-mailed to you next week
VPN & FIREWALL LOGS ARE TRICKY

Why are people not monitoring them?

- Vendors have different formats of logs
- Each version can change the format
- Configuration of device can be challenging
  - What Level to Log? (Info, Verbose, Debug)
- How to get logs? (Syslog, OPSEC-LEA)
- Concerns on volume of logs.
- They are confusing

Sample Checkpoint Log

31Oct2016 10:00:00 allow 192.168.1.2 eth2-01.111
src:192.168.1.2;dst:193.212.4.120;proto:tcp;app_name:Google Keep;app_desc:Google Keep is a note-taking service. Google Keep allows to write notes and color code them, to take pictures and record your voice. Supported from: R75.40.;app_id:60460461;app_category:Business Applications;matched_category:Business Applications;app_properties:SSL Protocol, Very Low Risk, Business Applications;app_risk:1;app_rule_id:{0EF98E02-F296-4AAB-AB87-F618F933362F};app_rule_name:default-ut;web_client_type:Other: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko;app_sig_id:60460461:6;resource:http://clients4.google.com/invalidation/lcs/request;proxy_src_ip:removed-ip;bytes:2357;sent_bytes:1984;received_bytes:373;browse_time:0:00:01;Suppressed logs:1;Referrer_self_uid:{58170810-0000-0000-8496-39100C0000C0};user:fjernet;src_user_name:fjernet;snid:51bfa9cd;product:Application Control;service:80;s_port:38975;product_family:Network
## TIPS & TRICKS

Setting yourself up for success

- **Schema, Parsing, Normalizing, Pipeline Rules, Enrichment**
- **Indexing, Streams, Retention & Archiving**
- **Prebuilt Dashboards and Investigation Templates**
- **Threat Intelligence and SOC Displays**

### Stage 0
Contains 1 rule
Messages satisfying at least one rule in this stage, will continue to the next stage.
Throughput: 0 msg/s

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
<th>Throughput</th>
<th>Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>pSensor.FirewallFiltering - Parse base data</td>
<td>pSensor.FirewallFiltering - Parse base data</td>
<td>0 msg/s</td>
<td>0 errors (0 total)</td>
</tr>
</tbody>
</table>

### Stage 1
Contains 1 rule
Messages satisfying at least one rule in this stage, will continue to the next stage.
Throughput: 0 msg/s

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
<th>Throughput</th>
<th>Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>pSensor.FirewallFiltering - Parse IPv6 data</td>
<td>pSensor.FirewallFiltering - Parse IPv6 data</td>
<td>0 msg/s</td>
<td>0 errors (0 total)</td>
</tr>
</tbody>
</table>

### Stage 2
Contains 2 rules
Messages satisfying at least one rule in this stage, will continue to the next stage.
Throughput: 0 msg/s

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
<th>Throughput</th>
<th>Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>pSensor.FirewallFiltering - Parse CIDR and TCP data</td>
<td>pSensor.FirewallFiltering - Parse CIDR and TCP data</td>
<td>0 msg/s</td>
<td>0 errors (0 total)</td>
</tr>
<tr>
<td>pSensor.FirewallFiltering - Parse ICMP data</td>
<td>pSensor.FirewallFiltering - Parse ICMP data</td>
<td>0 msg/s</td>
<td>0 errors (0 total)</td>
</tr>
</tbody>
</table>

### Stage 3
Contains 1 rule
Messages satisfying at least one rule in this stage, will continue to the next stage.
Throughput: 0 msg/s

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
<th>Throughput</th>
<th>Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify if src_addr and/or dst_addr are both Internal or external</td>
<td>Identify if src_addr and/or dst_addr are both Internal or external</td>
<td>0 msg/s</td>
<td>0 errors (0 total)</td>
</tr>
</tbody>
</table>

### Stage 4
Contains 4 rules
Messages satisfying at least one rule in this stage, will continue to the next stage.
Throughput: 0 msg/s

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
<th>Throughput</th>
<th>Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Intelligence Lookups for dst_addr</td>
<td>Threat Intelligence Lookups for dst_addr</td>
<td>0 msg/s</td>
<td>0 errors (0 total)</td>
</tr>
<tr>
<td>Threat Intelligence Lookups for src_addr</td>
<td>Threat Intelligence Lookups for src_addr</td>
<td>0 msg/s</td>
<td>0 errors (0 total)</td>
</tr>
<tr>
<td>pSensor.CasP Lookup dst_addr</td>
<td>pSensor.CasP Lookup dst_addr</td>
<td>0 msg/s</td>
<td>0 errors (0 total)</td>
</tr>
<tr>
<td>pSensor.CasP Lookup src_addr</td>
<td>pSensor.CasP Lookup src_addr</td>
<td>0 msg/s</td>
<td>0 errors (0 total)</td>
</tr>
</tbody>
</table>

### Stage 5
Contains 1 rule
There are no further stages in this pipeline. Once rules in this stage are applied, the pipeline will have finished processing.
Throughput: 0 msg/s

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
<th>Throughput</th>
<th>Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>pSensor.FirewallFiltering - Build summary message</td>
<td>pSensor.FirewallFiltering - Build summary message</td>
<td>0 msg/s</td>
<td>0 errors (0 total)</td>
</tr>
</tbody>
</table>
UNUSUAL LOGONS

Alert on suspicious activity

- Geolocation, Time of Day, Frequency
- The unusual has become usual and the usual, unusual
- Balance alert rules granularity with quantity
1. Not all FW, VPN vendors build in good license monitoring, management

2. What happens when you hit your licensing limit?

3. You have full control over when to alert: 80%? 90%? 98%? - depends on

4. Have an action plan in place
ARCHIVING

Save it for later

- Fighting fires? Give yourself visibility when it’s time to look back
- Search of archived data will be a little slower, but less expensive storage
- Look for odd traffic patterns
- Report on Who logged in over the entire time
- Notice any changes not alerted on?
QUESTIONS?
● TechTalks@graylog.com

FOLLOW US
● Twitter: @graylog2
● Linkedin: Graylog
● Reddit: /r/graylog/
BUT WAIT, THERE’S MORE!

30 April - Top 5 Authentication Dashboards You Should Be Monitoring Right Now
7 May - Monitoring For Insider Threats In Turbulent Times
14 May - Collaborating To Improve Availability, Root Cause Analysis
21 May - Threat Hunting Techniques For Today’s Biggest Threats

SPECIAL PRICING ON 10GB & 20GB PACKAGES WITH JUMP START SERVICES