TECH TALKS: SUPPORTING THE REMOTE WORKFORCE

Top 5 Authentication Dashboards
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
14 DAY TRENDING FOR ALERT TUNING

**TRENDS CAN BREAK THE HAYSTACK AND FIND A NEEDLE**

Logon Activity Over Time by Outcome (14d)
YOUR WORKERS ARE REMOTE, BUT ARE THEY “THAT” REMOTE
TROUBLESHOOTING ACCOUNT LOCKOUTS

FIND OUT WHERE THE ACCOUNT WAS LOCKED OUT

- Successful Access Attempts (24h) = 0
- Failed Access Attempts (24h) = 28
- Logon Count Over Time by Logon Type (24h)
- User Authentication and Access Logs (24h)
- User Logon Count by Source, Outcome (24h)
- Login Destinations by Count, Outcome (24h)
TROUBLESHOOTING ACCOUNT LOCKOUTS

FIND OUT WHERE THE ACCOUNT WAS LOCKED OUT

---

**User Logon Count by Source, Outcome (24h)**

<table>
<thead>
<tr>
<th>user_name</th>
<th>source_ip</th>
<th>Count</th>
<th>failure Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>testuser01</td>
<td>::1</td>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>100.15.248.116</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>testuser03</td>
<td>::1</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>100.15.248.116</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>testuser02</td>
<td>::1</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>100.15.248.116</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>testuser04</td>
<td>100.15.248.116</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>testuser05</td>
<td>100.15.248.116</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>testuser00</td>
<td>::1</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>testuser06</td>
<td>100.15.248.116</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
ADMIN MONITORING DASHBOARD

MONITOR THE ADMINISTRATORS ACTIVITY

Event Logs Cleared by User

Scheduled Tasks by User

Top 10 EventID's By User

Domain Groups Created by User

Domain Policy Changed by User

Users Added to Admin Groups
## COMPANY ASSETS VS. BYOD

### NOT ALL DEVICES ARE LOGGED EQUAL

#### Logon Destination Totals by Outcome (24h)

<table>
<thead>
<tr>
<th>destination_reference</th>
<th>Count</th>
<th>success Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRAYLOGLABDC1.grayloglab.local</td>
<td>3353</td>
<td>3353</td>
</tr>
<tr>
<td>JUMPBOX</td>
<td>71</td>
<td>71</td>
</tr>
<tr>
<td>GRAYLOGMEMBER1.grayloglab.local</td>
<td>64</td>
<td>64</td>
</tr>
</tbody>
</table>

#### Source Devices

<table>
<thead>
<tr>
<th>source</th>
<th>count0</th>
</tr>
</thead>
<tbody>
<tr>
<td>graylog_32</td>
<td>2038359</td>
</tr>
<tr>
<td>desktop-k09cipp</td>
<td>5120</td>
</tr>
<tr>
<td>knight</td>
<td>140</td>
</tr>
<tr>
<td>52.53.211.151</td>
<td>100</td>
</tr>
</tbody>
</table>
What is the Security Content Pack?

AUTHENTICATION MODULE IN BETA NOW - WANT TO JOIN?

Zipped up and ready to deploy inside your Graylog application, the content pack will include security-related:

- Dashboards
- Processing & data enrichment rules
- Search templates with input parameters
- Alerts
- Reports
- Look up tables
- Sidecar
- And more…
QUESTIONS?
● TechTalks@graylog.com

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

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