Presented by: Peter Häufel

SIEM MODERNIZATION – THE SMARTER WAY
• 62% would change their SOC
• 79% report old tech as being an issue
• 47% report too many alerts as a major concern
Security Management Process with Legacy SIEM

<table>
<thead>
<tr>
<th>Collection</th>
<th>Detection</th>
<th>Investigation</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingest Logs</td>
<td>Centralize in SIEM</td>
<td>Get Alert</td>
<td>Build Timeline</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Gather Evidence</td>
<td>Respond to Attack</td>
</tr>
</tbody>
</table>
Legacy SIEMs Cause Challenges at Each Step

<table>
<thead>
<tr>
<th>Collection</th>
<th>Detection</th>
<th>Investigation</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingest Logs</td>
<td>Centralize in SIEM</td>
<td>Get Alert</td>
<td>Build Timeline</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Gather Evidence</td>
<td>Respond to Attack</td>
</tr>
</tbody>
</table>

**PROBLEMS**

- Excessive Logging Costs
- Can’t Catch Unknown Threats
- Missing Distributed Attacks
- Manual Investigation
- Manual, Incomplete Response
Solving Security Management Challenges

**Collection**
- Ingest Logs
- Centralize in SIEM

**Detection**
- Get Alert
- Gather Evidence

**Investigation**
- Build Timeline
- Respond to Attack

**Response**

**PROBLEMS**
- Excessive Logging Costs
- Can’t Catch Unknown Threats
- Missing Distributed Attacks
- Manual Investigation
- Manual, Incomplete Response

**EXABEAM SOLUTION**
- Unlimited Logging with a Flat Price
- Behavioral Analysis (UEBA)
- Lateral Movement Tracking
- Automatically Created Incident Timelines
- Automated Incident Response (SOAR)
Smart Timelines Follow Lateral Movement throughout Attacks

Lateral movement without Smart Timelines

Part of the attack is undetected due to changes in
• IP Addresses
• Credentials
• Devices

Lateral movement with Smart Timelines

By tracking state changes, Exabeam Smart Timelines can attribute this activity using different credentials back to Barbara.
Logs Don’t Contain Data Needed to Recreate an Attack

Analysts must manually connect-the-dots, or risk missing parts of an attack

<table>
<thead>
<tr>
<th>Log 1</th>
<th>Log 2</th>
<th>Log 3</th>
<th>Log 4</th>
<th>Log 5</th>
<th>Log 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Log 1 Icon]</td>
<td>![Log 2 Icon]</td>
<td>![Log 3 Icon]</td>
<td>![Log 4 Icon]</td>
<td>![Log 5 Icon]</td>
<td>![Log 6 Icon]</td>
</tr>
<tr>
<td>Barry</td>
<td>?</td>
<td>Barry</td>
<td>Barry</td>
<td>Barry</td>
<td>?</td>
</tr>
<tr>
<td>![Device_1 Icon]</td>
<td>![Device_1 Icon]</td>
<td>![Device_1 Icon]</td>
<td>![Device_1 Icon]</td>
<td>![Device_2 Icon]</td>
<td>![Device_2 Icon]</td>
</tr>
</tbody>
</table>
| 142.1.12.68 | 142.1.12.68 | 37.4.1.23 | 37.4.1.23 | }
Smart Timelines stich together log data in real time to fill in the holes, from:

- Millions of logs
- Thousands of users and machines
- IP addresses that change constantly

Other SIEM Vendors

Only Exabeam
Gartner Magic Quadrant for Security Information and Event Management

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Exabeam.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.
Market and Industry Reception

250+ Enterprise Customers

Select Awards & Recognition

BARCLAYS
Royal Bank of Scotland
DISCOVER
Freddie Mac

UNITED
Delta
Caltrans
MTA Metropolitan Transportation Authority

Louisiana
Anthem
Cigna
Cincinnati Children's

Anadarko Petroleum Corporation
DUKE ENERGY
First Solar
Black Hills Corporation

P&G
Levi's
Under Armour
Safeway
GAP

THOMSON REUTERS
eBay
Verizon Telematics
NTT DATA

Gartner
COOL VENDOR

Gartner Peer Insights Customers' Choice 2018

Inc. 5000 #12 2018

WSJ Tech Companies to Watch 2018

Forbes Cloud 100 Rising Stars

exabeam
Conclusion

• Saving money with predictable license model
• Detect unknown attacks with machine learning and data science
• Smart Timelines™ reduces response time – minutes vs. hours per incident!
• Automate and orchestrate responses
• Saving money massively in operational costs
• Augmentation or replacement/greenfield possible

The Smarter SIEM™