LogRhythm Presentation for Joint Technology Committee

Presented by: James Carder, CISO / Vice President of LogRhythm Labs
Sara Avery, Sr. Customer Success Manager
48 year resident of CO, WheatRidge Farmer, CSU Grad, Co-Founder Women in Security / ISSA SIG. Passion Project to get more Women into Security

June 17th, 2019
• Founded in 2003
• America headquarters based in Boulder, CO. Additional offices in EMEA, APJ.
• Over 600 employees worldwide. Majority of employees are out of Boulder, CO.
• More than 3,000 customers
• Numerous patents granted and pending
• Strong community involvement – software for students, WIS
• Technology Integrations with other Colorado Companies
• Majority ownership by Thoma Bravo, a growth-focused PE firm
• Product has been pre-built for organizations to reach faster ROI and Return on Investment
LogRhythm is the Platform to run the Next Gen SOC – Faster detection and Faster Response

The heart of Security Operation Center (SOC) mission is to execute the following programs:

- Threat monitoring
- Threat hunting
- Threat investigation
- Incident response

“The SOC is a team, not a facility.”

Gartner: How to Plan, Design, Operate and Evolve a SOC
<table>
<thead>
<tr>
<th>IT / OT Environment Challenges</th>
<th>Threat Landscape Challenges</th>
<th>Operational Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital Disruption</td>
<td>Expanding Attack Surface</td>
<td>Alarm Fatigue</td>
</tr>
<tr>
<td>Perimeter erosion</td>
<td>Motivated Threat Actors</td>
<td>Cost of Operation</td>
</tr>
<tr>
<td>Volume of Data</td>
<td>Cybercrime Supply Chain</td>
<td>Workflow Efficiency</td>
</tr>
</tbody>
</table>
Before LogRhythm......swivel chair approach.
This BEST approach is – Single Next Gen SIEM Platform

- Advanced Correlation
- Log Management
- UEBA
- Security Automation Orchestration
- Network Monitoring & Forensics
- Endpoint Behavior Analytics
- Network Behavior Analytics
Innovation track record

2005
- Log Management Foundation
- Unified SIEM and Log Management
- Endpoint Forensics (SysMon)

2007
- Content Delivery Foundation (KB)
- Patent: Log Data Processing (MPE)

2010
- Machine-Analytics Foundation (AI Engine)
- Automation Foundation (SmartResponse)
- Patent: Stream-based Analytics (AI Engine)

2012
- Behavior Analytics (AI Engine)

2014
- Network Forensics (NetMon)

2016
- Elasticsearch Backend
- Case Management

2018
- LogRhythm UEBA
- LogRhythm 7.4 (Playbooks)
- NextGen UI/UX (Web Console)
- Analytics-as-a-service (CloudAI)

2018
- Patent: Log Data Processing (MPE)
- Patent: Stream-based Analytics (AI Engine)

LogRhythm 7.4 (Playbooks)
Why LogRhythm

- Security Focus
- Innovation Track Record
- Platform Scalability and Flexibility
- Broad Regulatory Compliance
- Customer Success –