Gaining and Maintaining Support for a SOC

Jim Goddard
Executive Director, Kaiser Permanente
Objectives

Agenda

1. Lessons learned
2. How to build interest
3. Producing tangible benefits
4. Building momentum
5. Communicating success
6. Expanding the ecosystem
7. Quantitative metrics
Lessons learned while building a SOC

- Investment is multi-year
- Agile development, not waterfall
- Mission must be focused
- Remember the triad of people, process and technology
- Seasoned leadership is essential
- Be visible
- Avoid silo’s
- Manage 24/7 expectations
Why support is so important

- Investment is for the long haul
- SOC is not self-reliant
- Expectations can be too easily misplaced
Common objections must be overcome

- Aren’t we already compliant?
- Will this guarantee against a breach?
- Can’t we just outsource this?
- Can we just purchase a tool?
- What is the ROI?

INVESTMENT DECISION PROCESS

LESSONS LEARNED
Crisis events whether internal or external often stimulate interest, but you have to take it home from there

UNCERTAINTY

- Explaining events in a way people understand
- Illustrating a solution
- Overcoming objections
Produce tangible benefits people “get”

1. Physical presence with visualization
2. Diverse skillsets
3. Actionable events, not data analysis
4. Rapid, high touch response
Physical design

- Map to how you work and collaborate
- NASA versus open design

- Open floor
- Incident Command Center
- Manager offices

- Interactive visualization
- Sound system
- Telepresence
- Clean images

- Biometrics
- Mantrap
- Secure network
- Dirty network
Make sure your organization has enough reach

Executive Leader

SOC Manager
- Threat intel analysts
- Kill chain analysts
- Policy engineers
- Team leaders

IR Manager
- Incident handlers
- Forensic specialists
- Investigators
- E-Discovery handlers
- Remediation engineers

Analytics Manager
- Use case engineers
- Data scientists
- Quality assurance analysts

Infrastructure
Build momentum with quick wins

Year 1
- Security & Event Management (SIEM)
- Flow data
- Security control data (e.g., malware)
- Threat intel & IOC detection
- Reference lists

Year 2
- Log data analytics
- Raw data capture
- IOC sweeps & quarantine
- Lateral movement
- Data visualization

Year 3
- Application level analysis
- Countermeasure automation
- Big data analytics
Startup use cases can get you more actionable events

Day 1 domains
Imposter domains
Threat & reputation feeds

Advanced Warning
Infiltration
Escalation
Exfiltration

Callbacks
IDS exploits
Domain name entropy

Internal scanning
Connection anomalies
User baselining

Volumetric analysis
Entropy analysis
Frequency analysis
Communicate wins that people will read

• Give up the techie talk and explain

• Make the communication accessible (no Powerpoint; simple text that looks good on a phone).

• Be brief (2-3 swipes on a phone). Executives don’t have time to figure out what you are trying to say.

• Give them what they want to know, not what you want to say.

• Never be late.
What you should try to communicate (with responsibility)

- Incident alerts and updates
- Countermeasure application
- Threat intelligence (formal and informal)
- Operational metrics
- Customer inquiries
Continue to expand your ecosystem

<table>
<thead>
<tr>
<th>INITIAL GROUPS TO CO-OPT:</th>
<th>LONGER TERM VALUE:</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Incident Response</td>
<td>✓ Infrastructure</td>
</tr>
<tr>
<td>✓ Legal</td>
<td>✓ Service Desk</td>
</tr>
<tr>
<td>✓ Compliance</td>
<td>✓ Architecture &amp; Strategy</td>
</tr>
<tr>
<td>✓ Senior executives</td>
<td>✓ Sales</td>
</tr>
</tbody>
</table>

ECOSYSTEM
Operational metrics will also help drive perception

<table>
<thead>
<tr>
<th>Area</th>
<th>Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detection</td>
<td>• Detected versus reported</td>
</tr>
<tr>
<td></td>
<td>• Correct designations for response</td>
</tr>
<tr>
<td></td>
<td>• Time to analyze and resolve</td>
</tr>
<tr>
<td></td>
<td>• False positives</td>
</tr>
<tr>
<td>Response</td>
<td>• Time to contain, by severity</td>
</tr>
<tr>
<td></td>
<td>• Indicators of compromise with actionable events</td>
</tr>
<tr>
<td>Remediation</td>
<td>• Time to remediate, by severity</td>
</tr>
<tr>
<td></td>
<td>• Repeat incidents</td>
</tr>
</tbody>
</table>
Questions?