"Chaos isn't a pit. Chaos is a ladder."
Security maturity – tales from the ladder

Customer experiences and maturity levels from around the nordic market

Gustav Rydmark
Security Architect
Atea Sweden
Prologue…

Who works there?

How do they work?

What tools do they use?
Stage 1: "The Ad Hoc Menace" – Limited sec work

<table>
<thead>
<tr>
<th>People</th>
<th>Organisation</th>
<th>General IT staff</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Skillset</td>
<td>Interested individuials</td>
</tr>
<tr>
<td></td>
<td>Culture</td>
<td>Isolated</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Process</th>
<th>Incident process</th>
<th>Improvised</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Schedule</td>
<td>Ad Hoc</td>
</tr>
<tr>
<td></td>
<td>Collaboration</td>
<td>Not set</td>
</tr>
<tr>
<td></td>
<td>Priority</td>
<td>Best effort</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Technology</th>
<th>Primary detection tool</th>
<th>Users &amp; external contacts</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Visibility scope</td>
<td>&quot;We have a firewall&quot;</td>
</tr>
<tr>
<td></td>
<td>Maintenance effort</td>
<td>Fire and forget</td>
</tr>
</tbody>
</table>
Stage 2: "A New Hope" – Ongoing sec work

**People**
- Organisation
- Skillset
- Culture
- Security group
- Vendor specific
- Within group or possibly in IT

**Process**
- Incident process
- Schedule
- Collaboration
- Priority
- Self built, partially documented
- 9-5
- Uncomfortable questions
- Category based

**Technology**
- Primary detection tool
- Visibility scope
- Maintenance effort
- SIEM alerts
- "We have a SIEM"
- Monthly effort
Stage 3: “Security Strikes Back” – Healthy sec work

**People**
- Organisation
- Skillset
- Culture

Security team + external
Security certs, analyst etc.
Pervasive throughout org.

**Process**
- Incident process
- Schedule
- Collaboration
- Priority

Standardized: ISO 27035/NIST or eq.
SLA, Defcons
Wide and appreciated
Risk based, asset context.

**Technology**
- Primary detection tool
- Visibility scope
- Maintenance effort

Realtime, workbench and Threat Intel
Own org and vertical + geo
Lessons learned, simulations, proactive
So, how can the rest of us help?

<table>
<thead>
<tr>
<th>People</th>
<th>Specialists</th>
<th>SOC</th>
<th>Advisors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process</td>
<td>Establishment</td>
<td>Cooperation &amp; metrics</td>
<td>Evaluation</td>
</tr>
<tr>
<td>Technology</td>
<td>Implementation</td>
<td>Detection &amp; maintenance</td>
<td>Investigation and IRT</td>
</tr>
</tbody>
</table>
Usually the saying goes "defenders only need to make one mistake" … We need to get to a place where our attackers are in the same position.

Favorite customer quote (so far) of 2019

Thanks everyone!

// Gustav Rydmark
gustav.rydmark@atea.se