Welcome to SANS ICS Europe 2019 Summit & Training

#SANSICSEUROPE
SANS 2019 State of OT/ICS Cybersecurity Survey & Whitepaper

Co-authors: Barb Filkins and Doug Wylie
Advisor: Jason Dely

www.sans.org/reading-room/whitepapers/analyst/
Respondents Details

Survey Demographics

• 338 respondents (IT, OT + hybrid roles)
• Across ICS (Discrete, Process, SCADA, BAS)
• Over 45% spend >50% time on OT/ICS cybersecurity

"More than 40% of respondents are using cloud-based services for OT-based system functions."

**Survey Results (Q35)**
- 78% systems have an external connection.

**Interpretation**
- The OT/ICS logical layer is becoming more important than physical layer in systems.
- Edges & boundaries are moving, and assets are becoming virtual(ized).
Initial Attack Vectors for OT/ICS Incidents

Survey Results (Q21 and Q22)

Event >> Incident >> Attack

Key Actors by Initial Attack Vectors (Point of Entry) for OT/ICS Incidents

- Employees & Service Providers
- Malicious Hackers
- Non-malicious & Malicious Actors

Organized Crime
Malicious Hackers
Service Providers, Consultants…

Employees & Service Providers

- Activists, activist organizations, backdoors
- Competitors
- Current employees

Physical access (USB stick, direct access to equipment)
Remote access (bypassing intended architecture)
Trusted remote access (through intended architecture)
Service maintenance and consulting (configuration changes)
Supply chain (i.e., altered/modified hardware or software; software/hardware updates and patches; maintenance tools/equipment)

High-risk vs. Low-risk Event >> Incident >> Attack

©2019 SANS Institute | www.sans.org
Companies Rely More on Trained Staff.

“A shared budget between IT and OT is diminishing.”

<table>
<thead>
<tr>
<th>Organization Controlling Budget</th>
<th>2017</th>
<th>2019</th>
<th>% Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operations</td>
<td>30.8%</td>
<td>48.7%</td>
<td>+17.9%</td>
</tr>
<tr>
<td>Enterprise IT</td>
<td>17.1%</td>
<td>31.6%</td>
<td>+14.5%</td>
</tr>
<tr>
<td>Shared budget between IT/OT</td>
<td>38.5%</td>
<td>29.4%</td>
<td>-9.1%</td>
</tr>
</tbody>
</table>

**Survey Results (Q46)**

**Interpretation**

The decrease in the shared budget may slow IT/OT convergence, but clarify risk ownership.

While IT & OT budgets appear to be separating, internal resource investments are increasing.
People Are a Key Enabler; Security Is the Common Thread.

### Table 7. Sources of Intelligence 2017 to 2019

<table>
<thead>
<tr>
<th>Source of Intelligence</th>
<th>2017</th>
<th>2019</th>
<th>% Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>We rely on our trained staff to know when to search out events.</td>
<td>37.8%</td>
<td>60.4%</td>
<td>+22.6%</td>
</tr>
<tr>
<td>We use third-party intelligence provided by our security vendors.</td>
<td>53.8%</td>
<td>51.8%</td>
<td>-2.0%</td>
</tr>
<tr>
<td>We work closely with government agencies to ensure up-to-date intelligence is available.</td>
<td>38.7%</td>
<td>44.7%</td>
<td>+6.0%</td>
</tr>
<tr>
<td>We actively participate in industry information-sharing partnerships.</td>
<td>46.2%</td>
<td>44.2%</td>
<td>-2.0%</td>
</tr>
<tr>
<td>We use anomaly detection tools to identify trends.</td>
<td>35.3%</td>
<td>44.2%</td>
<td>+8.9%</td>
</tr>
</tbody>
</table>

**Survey Results (Q29)**

- **Safety**
- **Reliability**
- **Resiliency**
- **Continuity**
- **Operational Integrity**
- **Productivity**
- **Sustainability**
- **Profitability**
WE THINK IT'S TIME FOR YOU TO COME SIT AT THE BIG KIDS' TABLE!!!
SANS 2019 State of OT/ICS Cybersecurity Survey & Whitepaper

Co-authors: Barb Filkins and Doug Wylie
Advisor: Jason Dely

www.sans.org/reading-room/whitepapers/analyst/