Welcome to SANS ICS Europe 2019 Summit & Training

#SANSICS EUROPE
Securing Large-Scale Industrial Networks
A Case Study of Europe’s Largest Manufacturing Site

Ofer Shaked, Co-Founder and CTO
June 24, 2019 | SANS ICS Europe Summit
How to Monitor a Large Scale Network?

Table of Contents:
• Gathering Customer Requirements
• Performing Site Survey
• Monitoring Infrastructure Challenges & Solutions
• Deploying the SCADAfence Platform
• Results of Monitoring
Customer Requirements

Motivation: Following recent attacks on manufacturers, IT management was given a task to present an OT protection program

Primary objective
- Cyber attack detection, including APTs (Advanced Persistent Threats)

Secondary objectives
- Automatically document all OT assets in a central location
- Discover vulnerabilities and kickstart an OT vulnerability management process

Previous deployment of a different solution failed due to scaling issues
Target Site Characteristics

- One of Europe’s largest manufacturing sites
- Cutting-edge automation & networking
- Two data centers set in redundancy
- 100s of switches & routers to monitor
- Over 25,000 network assets
- Multi-gigabit network traffic

AND: Extremely high security level required
Target Site

OT Data Centers x2
Core SW x2
Distribution SW x20
Access SW x200

SIEM/SOC
IT Network
ERP
Remote Access

Firewall
Backbone Switch
Distribution Layer Switch
Access Layer Switch

SCADAfence

Access Layer Switch
PLC
PLC
PLC
PLC

Distribution SW x2
Core SW x2
OT Network

Manufacturing Execution System (MES)
PLC
PLC
Historian Servers
Engineering Workstations
HMIs
ICS/SCADA Servers
Typical Deployment Architecture #2

Out of Band Monitoring Network

Source: SCADAfence Deployment Guide
Infrastructure Challenges

💧 Customer’s mandatory requirement:
  - “Full DPI (Deep Packet Inspection) of Access Layer Switches, to ensure high security level”

💧 Access Layer monitoring allows Deep Packet Inspection of devices on the same VLAN, connected to the same switch

💧 However, using our “Typical Deployment Architecture #2” – we can’t directly connect 200+ Access SWs to the aggregation switch without going into significant investment in labor and new hardware
One possible solution...

“Local SPAN: Mirrors traffic from one or more interfaces on the switch to one or more interfaces on the same switch.” – Source: Cisco online docs

“Remote SPAN (RSPAN): An extension of SPAN called remote SPAN or RSPAN. RSPAN allows you to monitor traffic from source ports distributed over multiple switches, which means that you can centralize your network capture devices.” – Source: Cisco online docs

But will it work at a scale of 200+ Access SWs, without congesting the OT network?
## Staged Deployment to Eliminate Risk

- **Main KPIs:** Load % (Rx/Tx Load) and output RSPAN traffic rates

<table>
<thead>
<tr>
<th>Stage</th>
<th># ASWs Monitored, % of Total</th>
<th>Output RSPAN Traffic Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5, 8%</td>
<td>26 Mb/s</td>
</tr>
<tr>
<td></td>
<td>--- Wait 4 days ---</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>10, 16%</td>
<td>58 Mb/s</td>
</tr>
<tr>
<td></td>
<td>--- Wait 3 days (weekend) ---</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>20, 33%</td>
<td>101 Mb/s</td>
</tr>
<tr>
<td></td>
<td>--- Wait 3 days ---</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>40, 66%</td>
<td>216 Mb/s</td>
</tr>
<tr>
<td></td>
<td>--- Wait 2 days ---</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>60, 100%</td>
<td>372 Mb/s (Final)</td>
</tr>
</tbody>
</table>

- **Total deployment time:** 2 Weeks
- **RSPAN:** Max 1 Gb/s per session

© Confidential and Proprietary Information of SCADAFence Ltd.
We have the data, now what?

⚠️ Challenges:

- Bandwidth requirements – 6Gb/s
  - 1Gb/s for Access SWs RSPAN
  - 3Gb/s for Core SWs and Distribution SWs SPAN
  - 2Gb/s for future expansion (allows 50% growth)
- Many duplicate packets that can skew statistics and create false positives
- Many alerts have the same response scenario, and can be handled automatically rather than by SOC team
Action Items to Resolve Challenges

Action Items:
- Install a 10Gb/s SCADAfence Platform DPI Analytics server
- Activate the SCADAfence De-duplication Module
- Alerts Tuning
- Automated Incident Response Configuration
De-duplication Module

Problem:
Packet traveling from endpoint A to B can “visit” many monitored switches/routers along the way, and will be processed multiple times.

Potential Result:
False positives, duplicate sessions and false traffic stats

Solution:
SCADAfence Deduplication Module removes duplicate packets at wire-speed even if they’re switched, routed or mangled in any other way.
Alerts Tuning

Goal

- Set alerts severity levels:
  - Log - Only log the event for forensics, don’t start an investigation
  - Alert – Start investigation based on the alerts

Parameters to take into account for each alert

- Is it important (from user’s perspective)?
- Is it manageable? (How many alerts per day?)
- Avoid common pitfalls - E.g. Wanting to monitor any WRITE command on PLCs, but those happen 170 times per day, is important but not manageable.

Noisy alerts: Research root cause, eliminate root cause and increase severity

- Example: Employees not working according to company policy => Train employees
Implementation Results – Asset Inventory

- Discovered over 25K network hosts
- 5K of them – unmanaged/unknown to IT team

- Imported all Excel asset inventories into one, unified & automated asset inventory
- Trained the local team to use SCADAfence Asset Inventory
Implementation Results - Vulnerabilities

List of top vulnerabilities, with priority given to endpoints used in the production process

<table>
<thead>
<tr>
<th>Risk</th>
<th>Vulnerability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open CVEs</td>
<td>List of unpatched PLCs + CVSS Score, insecure industrial protocols</td>
</tr>
<tr>
<td></td>
<td>Unsupported Operating Systems</td>
</tr>
<tr>
<td>Isolation &amp; segmentation violations</td>
<td>Unauthorized site-to-site, site-to-corporate, site-to-internet connections. PLCs accessible by unauthorized hosts. Too many hosts per network segment.</td>
</tr>
<tr>
<td>Insecure protocols</td>
<td>List of devices using insecure protocols (tftp, telnet, SNMPv1, SMBv1) – upgrade to secure versions</td>
</tr>
<tr>
<td>Asset management violations</td>
<td>List of unreachable/unmanaged devices</td>
</tr>
<tr>
<td>Password policy</td>
<td>List of devices / user accounts with default/weak passwords</td>
</tr>
</tbody>
</table>
Implementation Results – Operational Issues

 hü List of top misconfigurations and errors:

• Errors originating from PLCs in industrial protocols (e.g. Historian reading wrong addresses)
• Session latency issues
• Misconfigured PLCs / HMIs (wrong IPs, not accessible by network)
• Connectivity problems – sessions not established due to firewall
• Redundancy issues – Network redundancy not properly configured, will fail when required
• Misconfiguration in update server address, trying to reach internet, remaining unpatched
After reviewing current status, configured alerts on isolation/segmentation violations

Implemented 3 automated incident response scenarios:

- Isolate new devices that perform violations (Quarantine VLAN)
- Disable external access to devices that performed unauthorized actions (Firewall configuration)
- Isolate plants that are under attack from the global network (Firewall configuration)
## Key Takeaways – Large Scale Network Monitoring

<table>
<thead>
<tr>
<th>Topic</th>
<th>Key Takeaway</th>
</tr>
</thead>
<tbody>
<tr>
<td>More value</td>
<td>The more advanced and complex larger the site, the higher the risk level</td>
</tr>
<tr>
<td>Access layer monitoring</td>
<td>Possible even in large scale, and without any additional risk/costs</td>
</tr>
<tr>
<td>Prevent technical debt</td>
<td>Plan for future expansion (more assets/bandwidth/connectivity)</td>
</tr>
<tr>
<td>Centralized monitoring</td>
<td>Reduces upfront and maintenance costs</td>
</tr>
<tr>
<td>System tuning</td>
<td>Reduces noise. Not all alerts are equally important for you</td>
</tr>
<tr>
<td>Automate incident response</td>
<td>Manual incident response isn’t scalable nor fast enough. Plan for automation</td>
</tr>
</tbody>
</table>
Thank You!
Welcome to SANS ICS Europe 2019 Summit & Training

#SANSICS EUROPE