Secure Networks under your control

Jon Matias, PhD - CTO
<jon.matias@keynetic.es>

9 October 2019 // IT-SA 2019 Nuremberg
Hardening of Industrial Networks
USENIX Enigma 2016
NSA TAO Chief on Disrupting Nation State Hackers

- Deep knowledge Net–Dev–Tech
- Knowledge vs. actual knowledge
Cyber-attack that crippled NHS systems hits Nissan car factory in Sunderland and Renault in France

Japanese car giant latest to be affected

How a Smart Coffee Machine Infected a PLC Monitoring System with Ransomware

David Bisson | Jul 27, 2017 | C5 SECURITY

Hack attack causes 'massive damage' at steel works
Segmentation
PARADIGM SHIFT: SDN Technology

Zero Trust & Microsegmentation

Visibility  Control
# Software-Defined Networking

## Traditional Network vs Software Defined

<table>
<thead>
<tr>
<th>Traditional</th>
<th>Software Defined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Centric</td>
<td>Software Driven</td>
</tr>
<tr>
<td>Manual</td>
<td>Automated</td>
</tr>
<tr>
<td>Closed</td>
<td>Programmable</td>
</tr>
<tr>
<td>Reactive</td>
<td>Predictive</td>
</tr>
<tr>
<td>Network Intent</td>
<td>App and Cloud Intent</td>
</tr>
</tbody>
</table>

All the traffic from each port associated to one segment (VLAN id)
Firewall with Trusted Segments

1. All the traffic goes through the firewall
2. All the shopfloor traffic is redirected for inspection
3. All the traffic is concentrated for inspection
Micro-segmentation with SDN

1. Malware Not according to policy
   - Maintenimiento
   - Switch SDN
   - RED OT
   - Switch SDN
   - PLC

2. Dynamic deployment of policy at flow level

3. Malware Not according to policy
   - HMI
Key Functionalities

Solution adapted to the specificities of the industrial environment

- Complete Vision & Control to improve the security
- Automatic discovery of assets and policies using AI/ML technology
- Simplification and robustness of network management
- Customization to processes defined by IT/OT managers

Copyright © 2019 Keynetic Technologies All Rights Reserved.
Automatic Discovery

- Smart profiling of assets and traffic patterns
- Automatic definition of security policy and quality improvement based on best practices
- Drastic reduction of time and effort invested in this task
- Anomaly detection & continuous analysis
“If you really want to **protect** your network you have to **know** your network, including all the devices and technology in it”

Rob E. Joyce (Chief of NSA’s TAO)
Secure Networks under your control

<jon.matias@keynetic.es>