CASE STUDY

World's Top Gold Mining and Processing Company Selects Securolytics to Automate Industrial IoT (IIot) and IoT Device Discovery and Security

CUSTOMER PROFILE

One of the world's top 5 largest gold producers:

- Owns and operates over 13 mines and has processing facilities
- Employs over 40,000 people
- Utilizes Industrial IoT (IIoT) devices like SCADA Industrial Control Systems (ICS) to monitor and controlmining and processing operations.
- Other IIoT and IoT devices are used to further improve efficiencies, reduce costs and monitor environmental conditions.

Customer Challenges

Many of these devices could not run traditional endpoint security agents and were unmanaged. IT realized they needed better context and insight into what devices were on the network and where they were connected. They also were concerned with a lack of vulnerability detection because vulnerability scans were too intrusive on resource-constrained IIoT, which could disrupt operations. IT identified these main challenges that required a solution:

1. Lack of an up-to-date inventory of devices on the network:

- Operational Technology (OT) teams would commonly deploy devices without IT's knowledge or input for security. With SCADA and IoT devices becoming more prevalent on the network that lacked of device management, IT needed better context into:
  - exactly what each device was
  - where it was on the network
  - what other devices shared the same network with sensitive SCADA and IoT devices
- When ICS-CERT or other security advisories were published, they didn't have visibility into if they had the device(s) under advisory or even if they needed to take some action.

2. Problems with network / vulnerability scans on SCADA and IoT devices:

- Scans were too intrusive and could interfere with and even crash sensitive and mission-critical devices that monitored operations.
- No continuous capabilities - Since OT would deploy devices without IT's involvement, IT wanted to ensure that devices were checked for vulnerabilities as devices were connected to the network.
- Risks caused by lack of device identification:
  - Vulnerability scans could not always reliably fingerprint the device's software, which resulted in the scanner only running default/generic instead of device-specific security checks.
  - Without dynamic discovery, scan coverage was not complete.

3. Lack of continuous device security monitoring:

- Device manufacturers often lacked documentation and methods of operation. IT did not have the resources to research each device's communications, then build and maintain security rules for monitoring.
- Device manufacturers were not building security into the devices or providing support for patching. They simply used open source OSs for quick time to market and paid no attention to securing the devices. This further drove the need to do continuous security monitoring.

Solution

Securolytics Solution containing:

- Securolytics IoT Device Library
- Securolytics IoT Security Appliance
- Securolytics IoT Asset Discovery & Threat Defense

Delivered Results

Fast, Easy deployment - Safe on Devices

- The initial PoC took only 5 minutes to centrally deploy.
- The solution is agentless, not in line, runs passively and continuously, does not use network taps or collect sensitive data on the deployment.

New, Accurate Visibility into IT Assets

- Discovered, identified, categorized & tracked the SCADA and IoT devices, including unmanaged devices, many of which they had no visibility into, but also all other devices connected to the network.
- Identified sensitive IoT devices that were sharing networks with other vulnerbale devices like network devices, thin clients, virtual machines, printers, IP cameras, optical communication devices and access controls.

New Visibility into Vulnerable Devices

- Without interfering with devices, detected and alerted on the vulnerable devices, both as they connected to the network and continuously.
- Discovered vulnerabilities they did not previously have visibility into, including devices that were misconfigured, had exploitable ports, were deployed with default credentials, were subject to remote code execution vulnerabilities and were vulnerable to ransomware.
- Discovered that unmanaged devices accounted for the bulk of vulnerable devices.

New Ability to Track Vulnerable Devices and Streamline Remediation

- Automatically tracked vulnerabilities to devices, even as devices received new IPs. This made locating the device much easier vs. rescanning the environment with a traditional network scanner to locate the device's new location on the network.

Automated, device-specific profiling and monitoring

- Allowed IT to do security behavioral monitoring and analytics without tying up IT resources.

"Securolytics gave us new visibility into IoT threats."

By being able to continuously and non-intrusively identify devices and vulnerabilities on the network, Securolytics closed coverage gaps vs. traditional network scanners that were only run periodically. It also gave us detailed device identification and the context we needed to better prioritize remediation.

To ease remediation efforts, Securolytics actually tracked vulnerable devices even if they got new IPs or moved around on the network. This saved us from rescanning the environment to track down the location of vulnerable devices.

Competitive Review

Reasons other solutions were discarded:

- **Required a Network Tap.**
  - This meant Long, Complex Deployment - No centralized deployment as it required a network tap on all switches and at all locations to see all the devices. In addition, there was no complete inventory of their network switches so they could not identify where to even deploy the solution to get full coverage.
  - Sending all the network traffic, including sensitive data to the vendor's cloud. This was not compliant with the company's data privacy policy.
- **No Safe, Vulnerability Detection**
  - Did not have a proactive solution to non-intrusively detect vulnerabilities. They only provided a reactive behavior analysis security solution.
- **Not affordable**
  - Competitive solutions were 2x or more the cost of Securolytics.

securolytics®