Ordr and Splunk:
IOT Device SOC Solution

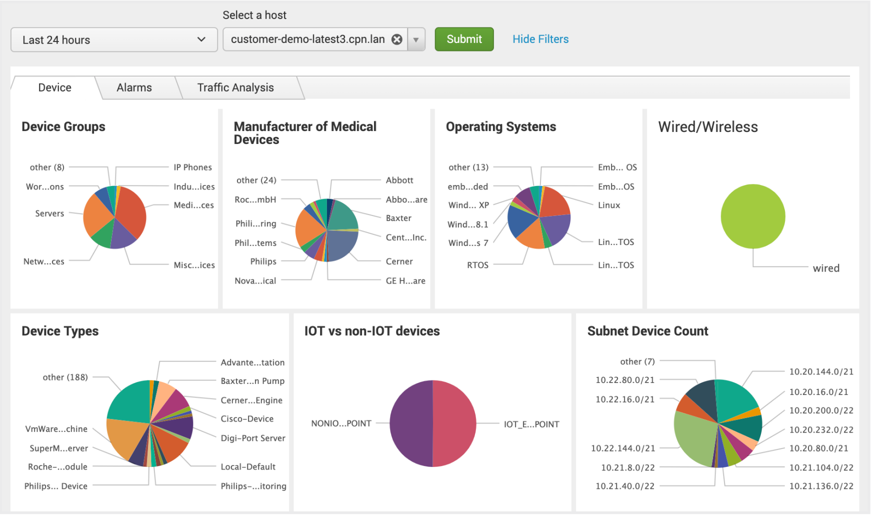
Enterprise Security Operations Centers (SOCs) were designed to detect and respond to cybersecurity issues for IT-managed assets. Facilities devices, physical security cameras, research systems, medical equipment, OT systems, printers, and other IOT were never considered in-scope for the SOC. With no-one actively on the lookout for security threats and no process accountability to remediate issues, many organizations are challenged to manage cybersecurity risk. Threats posed by modern malware—WannaCry and the more recent Urgent/11—demonstrate the importance of upgrading security operations to cover IOT and OT devices.

Ordr and Splunk have partnered to expand the coverage of the SOC so it can include IOT and OT systems. Ordr System Control Engine (SCE) identifies and classifies every device in the network with high-resolution details including make, model, software, and serial number. It learns where every device is located, how and where it is connected, what it is doing, and continuously risk scores assets based on a wide set of security intelligence. This information is fed into Splunk's Security Incident and Event Management (SIEM) platform, which integrates threat intelligence from multiple sources, streamlines investigations, and facilitates consistency in response and remediation with operational playbooks.

The solution enables enterprise organizations to manage risks in the facilities, physical security, clinical, industrial, and other IOT-based networks in the provider's environment. By providing the IOT device context, their vulnerabilities, communications, and observed threats empowers the SOC to respond to issues quickly and consistently.

COMPLETE VISIBILITY

The solution ensures the SOC has complete visibility of every device in the enterprise environment that is always current and accurate. Devices are grouped by type automatically, streamlining asset management.

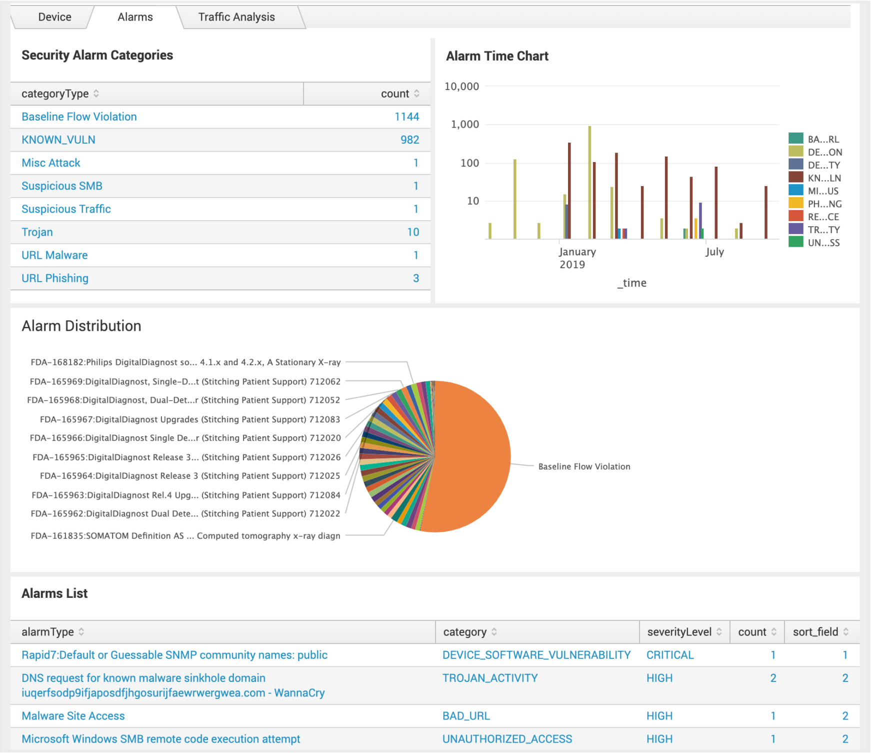


Select a host

Last 24 hours | customer-demo-latest3.cpn.lan

SECURITY MONITORING & RISK SCORING

Ordr SCE tracks a variety of security feeds (ICS-CERT advisories, the FDA recall database, intrusion detection signatures, and known-bad websites) to risk score IOT and OT devices. SCE also actively monitors devices for anomalous behaviors that indicate they are under attack or compromised. These security events are shared with Splunk in real-time so the SOC can expedite a playbook for incident detection, trouble-ticketing, and response.



Device
Alarms
Traffic Analysis

Security Alarm Categories

categoryType	count
Baseline Flow Violation	1144
KNOWN_VULN	982
Misc Attack	1
Suspicious SMB	1
Suspicious Traffic	1
Trojan	10
URL Malware	1
URL Phishing	3

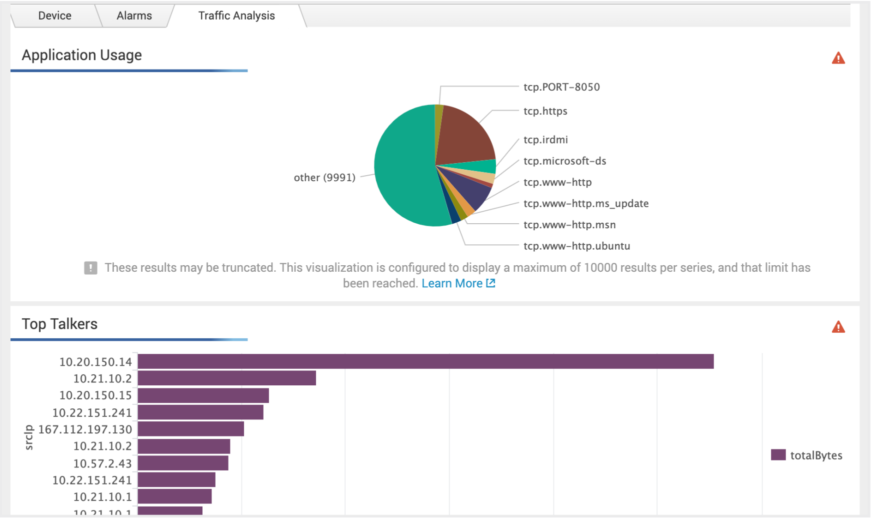
Alarm Time Chart
10,000
1,000
100
10
January
2019
July
_time
BA...RL
DE...ON
DE...TY
KN...LN
MI...US
PH...NG
RE...CE
TR...TY
UN...SS
Alarm Distribution
FDA-168182:Philips DigitalDiagnost so... 4.1.x and 4.2.x, A Stationary X-ray
FDA-165969:DigitalDiagnost, Single-D...t (Stitching Patient Support) 712062
FDA-165968:DigitalDiagnost, Dual-Det...r (Stitching Patient Support) 712052
FDA-165967:DigitalDiagnost Upgrades (Stitching Patient Support) 712083
FDA-165966:DigitalDiagnost Single De...r (Stitching Patient Support) 712020
FDA-165965:DigitalDiagnost Release 3... (Stitching Patient Support) 712026
FDA-165964:DigitalDiagnost Release 3 (Stitching Patient Support) 712025
FDA-165963:DigitalDiagnost Rel.4 Upg... (Stitching Patient Support) 712084
FDA-165962:DigitalDiagnost Dual Dete... (Stitching Patient Support) 712022
FDA-161835:SOMATOM Definition AS ... Computed tomography x-ray diagn
Baseline Flow Violation

Alarms List

alarmType	category	severityLevel	count	sort_field
Rapid7:Default or Guessable SNMP community names: public	DEVICE_SOFTWARE_VULNERABILITY	CRITICAL	1	1
DNS request for known malware sinkhole domain iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com - WannaCry	TROJAN_ACTIVITY	HIGH	2	2
Malware Site Access	BAD_URL	HIGH	1	2
Microsoft Windows SMB remote code execution attempt	UNAUTHORIZED_ACCESS	HIGH	1	2

COMMUNICATION MONITORING

Ordr SCE monitors the communications to and and from every device, categorizing them by application, protocol, and destination and identifies any anomalous flows. Splunk ingests this data, providing the SOC with detailed records to aid investigations into potential security incidents.



These results may be truncated. This visualization is configured to display a maximum of 10000 results per series, and that limit has been reached. Learn More

DEVICE PROTECTION

Traditional means of protecting critical and high risk assets do not work—manufacturers often don't provide timely patches and it isn't feasible to deploy software agents directly. Ordr SCE seamlessly integrates with network and security infrastructure to implement security policies directly and automatically that protect key systems. Using playbooks driven by Splunk, streamlining the incident response process of implementing device-centric segmentation can be achieved for business-critical assets.

SUMMARY OF BENEFITS

- Automated visibility & classification of all connected IOT and OT devices
- Rich device details including make, model, serial number, software, network connection details
- Asset risk scoring based on up-to-date security intelligence
- Real-time incident detection, including anomalous behaviors, that ties into SOC playbook responses with clinical context
- Detailed device communication monitoring to aid incident investigations
- Streamline device-centric segmentation to protect critical and at-risk assets

About Ordr

At Ordr, we're energized by the explosive growth in network-connected systems and devices. We recognize the tremendous opportunities that this represents for the hyper-connected enterprise. Improved delivery of care, efficient logistics and operations, quality enhancements in manufacturing, more stable and intelligent business-critical systems. We're energized because we give you the power to take control and realize these myriad opportunities.

Learn more at www.ordr.net.

About Splunk

Splunk is the world's first Data-to-Everything Platform. Now organizations no longer need to worry about where their data is coming from, and they are free to focus on the business outcomes that data can deliver. Innovators in IT, Security, IoT and business operations can now get a complete view of their business in real time, turn data into business outcomes, and embrace technologies that prepare them for a data-driven future.

Learn more at https://www.splunk.com.