Enhancing Threat Intelligence with Ordr SCE and STIX/TAXII 2.1

Rich Device Context for Incident Response Workflows

The 2020 Cost of a Data Breach Report by the Ponemon Institute, commissioned by IBM Security, identified two key methods to greatly reduce data breach costs: incident response (IR) process automation by incorporating advanced machine learning, analytics, and orchestration; and preparedness training such as workflow documentation and resiliency testing. Two standards, introduced by the MITRE Corporation and the Department of Homeland Security (DHS), have emerged to facilitate these methods and share threat intelligence data. Security-conscious organizations now widely use Structured Threat Information eXpression (STIX) and Trusted Automated Exchange of Intelligence Information (TAXII) to rapidly correlate data around motivations, abilities, capabilities, and response to inform workflows.

STIX is the language for standardized threat intelligence data communication, with each piece of information categorized into objects, while TAXII was designed to exchange STIX objects to facilitate threat intelligence sharing. Running over HTTPS, TAXII supports multiple source feeds and aggregation of STIX objects. STIX and TAXII are structured, machine-readable formats that can be easily incorporated into existing security workflows.

STIX and TAXII Integration with Ordr SCE

Many security-conscious organizations have standardized on specific threat feeds they have vetted to meet their requirements of comprehensiveness, accuracy, and industry relevance. These feeds then empower a wide variety of security controls, ensuring a consistent view of the threat landscape across a multivendor defense-in-depth security strategy. Ordr’s ability to consume STIX and TAXII – and incorporate these threat feeds into the Ordr Data Lake – now extends this security strategy to the critical realm of agentless devices such as IoT, medical devices, smart office appliances, and operational technology, and more. Additionally, Ordr’s extensive APIs, Syslog output, and integrations with workflow tools such as SIEMs (e.g., Splunk Enterprise, IBM QRadar, Exabeam, etc.), CMDB and IT Asset Management systems (e.g., ServiceNow), and CMMS (e.g., Nuvolo) create seamless connections to workflow tools for threat monitoring, remediation, and prevention.

Benefits of Integrating STIX/TAXII with Ordr SCE:

Broaden the number and type of threats discovered while identifying unique threats against previously unknown devices connected to your network.

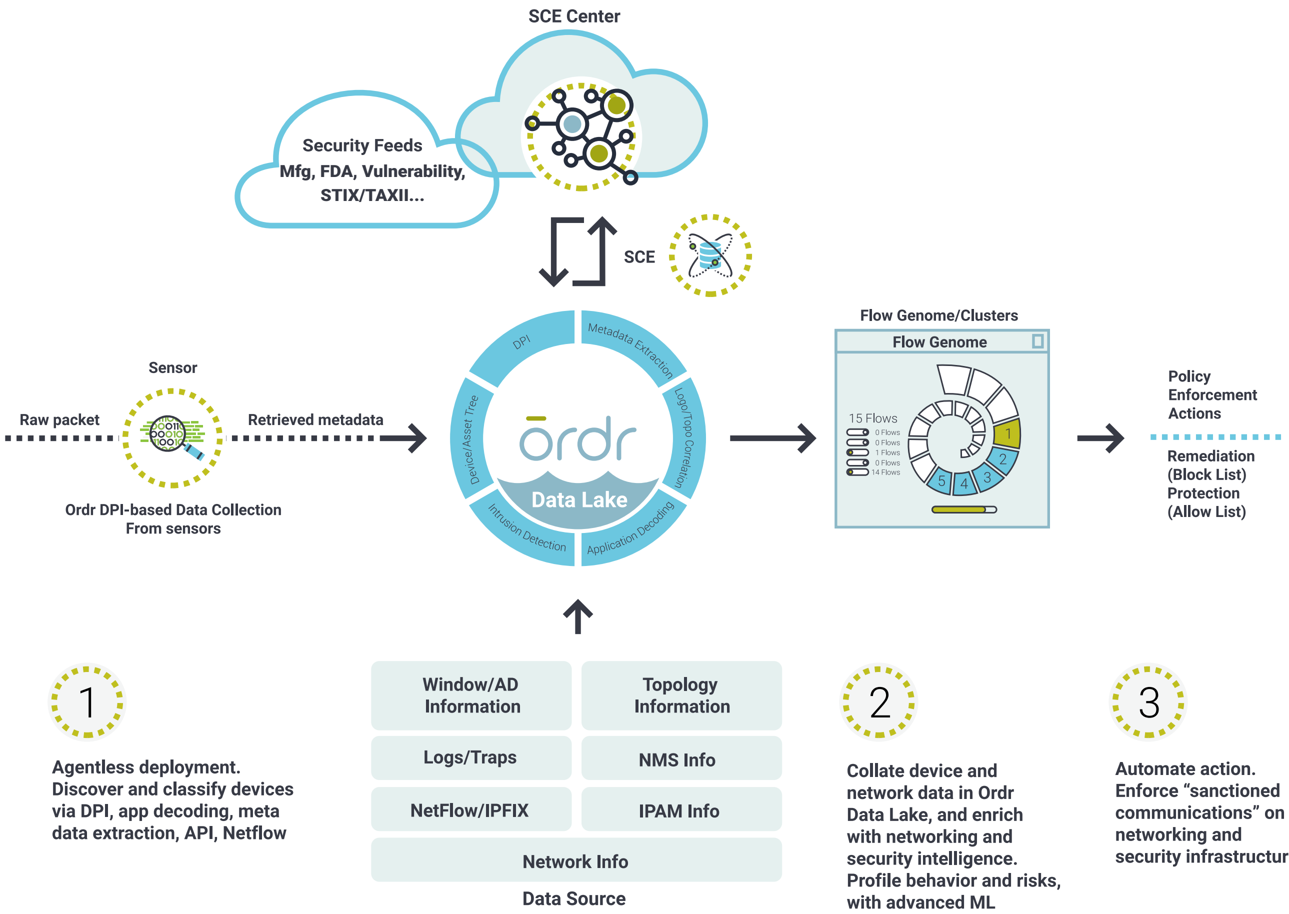
Leverage a full ecosystem of a TIP with multiple, industry-specific threat feeds and increase the value of your existing investments.

Augment Ordr's expansive security controls with best-of-breed industry solutions.

Security vendors without the ability to incorporate STIX and TAXII feeds limit their customers to threat intelligence feeds that are proprietary, constrained, or of unknown origin. Why rely on your vendor's choices when you can control your own security destiny and incorporate the threat feed that's right for your organization?

STIX and TAXII in the Ordr SCE Architecture

Ordr SCE incorporates threat feeds via STIX and TAXII into its Data Lake, where they are combined with a deep understanding of devices, behaviors, and network intelligence to identify assets, alert on threats, and automate response actions.



1 Agentless deployment. Discover and classify devices via DPI, app decoding, meta data extraction, API, Netflow

2 Collate device and network data in Ordr Data Lake, and enrich with networking and security intelligence. Profile behavior and risks, with advanced ML

3 Automate action. Enforce "sanctioned communications" on networking and security infrastructure

Ordr Systems Control Engine (SCE)

Ordr Systems Control Engine (SCE) is an IoT and unmanaged device security platform that will discover every connected device, profile device behavior and risks, and automate response. Ordr not only identifies devices with vulnerabilities, weak ciphers, weak certificates, and active threats, but also those that exhibit malicious or suspicious behaviors. Finally, Ordr automates response for security and networking teams, such as dynamically generating policies and enforcing them on existing infrastructure, or alerting and triggering a specific security or operational workflow.

Through an agentless deployment, within just a few hours of installation – via a network tap or SPAN – Ordr passively discovers every network-connected device with detailed context: manufacturer, model, device type, network connectivity information, and more. Ordr then enriches this device context with threat intelligence, vulnerability data, and FDA/device manufacturer alerts, and incorporates it into the Ordr Data Lake for analytics, reporting, and granular classifications for every device. In the IR workflow, organizations use the Ordr Data Lake context to quickly identify devices with vulnerable operating systems, FDA recalls, and more.

Case Study

A large national bank with more than 780 branches in 17 states across the United States and 4,500 employees, recently needed to address their managed and unmanaged device security risks.

First, they needed to identify all network-connected infrastructure, from “big iron” to embedded controls, including servers, security cameras, IP phones, media devices, credit card readers, ATMs, and more. The team then faced the challenge of identifying the specific threats faced by each of these managed and unmanaged devices, then integrating the results into their existing security remediation workflow.

They selected Ordr SCE as the best tool for the job. The team installed Ordr and configured it to ingest a feed via STIX and TAXII from their existing threat intelligence platform (TIP). Ordr identified each network-connected device, combined the STIX/TAXII-based threat feed with rich context (such as manufacturer, model, operating system, serial number, network behavior, and more) to accurately map specific threats to specific devices, then risk-rated and prioritized the most critical issues. Closing the loop from discovery to remediation, Ordr then—and in real-time thereafter—pushed alerts to their security information event management (SIEM) solution to patch, quarantine, or investigate the issues per their standard security workflow.

About Ordr

Ordr makes it easy to secure every connected device, from traditional IT devices to newer and more vulnerable IoT, IoMT, and OT. Ordr Systems Control Engine uses deep packet inspection and advanced machine learning to discover every device, profile its risk and behavior, map all communications and protect it with automated policies. Organizations worldwide trust Ordr to provide real-time asset inventory, address risk and compliance and accelerate IT initiatives. Ordr is backed by top investors including Battery Ventures, Wing, and TenEleven Ventures. For more information, visit www.ordr.net and follow Ordr on Twitter and LinkedIn.