Automating Security Workflows with Rich Device Context

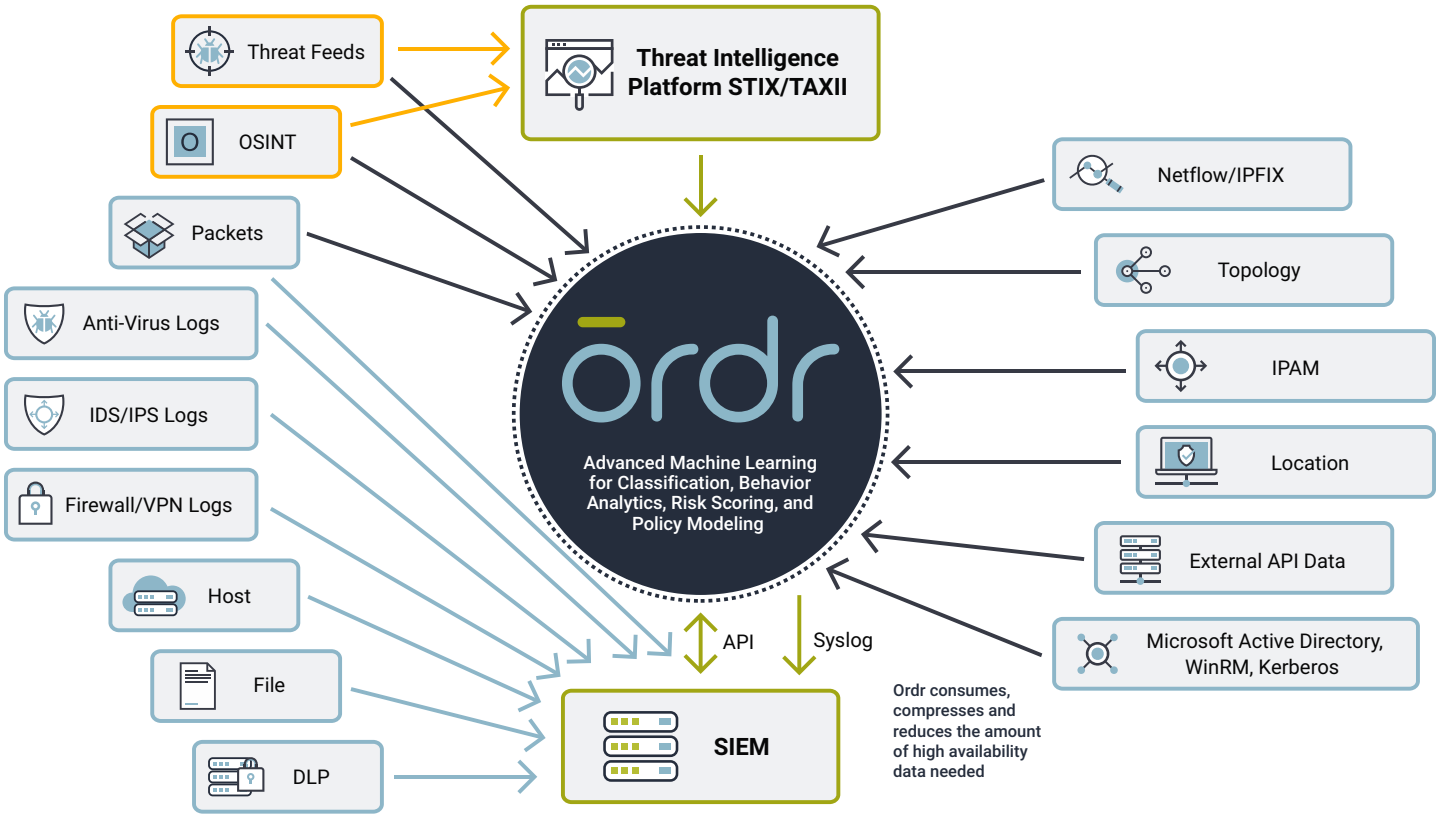
Ordr Systems Control Engine (SCE)

Digital transformation has brought many benefits to organizations, but also increased complexity and risk. Maintaining operations requires the collection, monitoring, and understanding of the status and behavior of thousands – if not hundreds of thousands – of managed and unmanaged devices. Security Information Event Management (SIEM) solutions correlate, normalize, and analyze device logs and other inputs to create a centralized repository of security events to give organizations a clear picture of their environment. SIEM solutions often serve as an organization's security "nerve center," prioritizing and alerting on incidents that warrant further investigation or an immediate response.

Unfortunately, SIEM deployments often have two blind spots:

- Lack of visibility into connected devices that don't produce logs, such as IoT, smart office, physical security, and medical equipment.
- Frequently do not provide detailed context about alerts, often reporting on IP or MAC addresses rather than human-friendly information like device names and classifications.

These gaps can increase the time to identify a threat, overlook critical information, and raise the workload of busy security analysts. That's where Ordr Systems Control Engine (SCE) comes in.



Ordr Systems Control Engine (SCE)

Ordr SCE is an IoT and unmanaged device security platform that discovers every connected device, profiles device behavior and risks, and automates security responses. Ordr not only identifies devices with vulnerabilities, weak passwords, expiring 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.

Organizations can use Ordr's rich device context and associated alarms to initiate specific workflow actions based on device type, group, manufacturer, model name and number, and more.

SIEM Integration with Ordr SCE

Ordr SCE integrates with SIEM solutions by transmitting security alerts, device information, and other critical information via the Syslog output format. The SIEM ingests the feed, parses the data into the proper fields, and allows SIEM users to leverage Ordr's rich device data to create alerts, reports, and custom analyses.

Ordr SCE provides four separate Syslog feeds:

Device Information: Notifications of new devices on the network, updates to network information (e.g., IP addresses or VLAN assignments), and risk states. Including information such as manufacturer, model, serial number, and device type.

Security Incidents: Alerts spanning a wide array of issues, such as malicious behavior, software vulnerabilities, accesses to known bad URLs, and more. Alerts include severity ratings, device identifiers, and alarm IDs to query Ordr for additional information.

Audit Trail: Notifications of privileged user access to Ordr, password changes, user account creation, and similar events to ensure the Ordr system itself remains secure.

System Events: Reports of Ordr system health, sensor connections and disconnections, and configuration data.

Additionally, Ordr offers a robust REST API that provides even deeper access into device information, security alerts, network flows, and medical device utilization. These APIs allow enterprise developers or services personnel to further augment SIEM solutions that support API programmability. Such extensions could allow:

- Rapid lookup of IP and MAC addresses, so SOC analysts or SIEM users can quickly map threats and risks to specific device, manufacturer, and product names.
- Evaluation of network neighbors and related traffic to identify potential malware spread.
- Detailed security alert information to augment the Syslog reports.
- Understanding of medical device utilization to identify time windows for patching and security upgrades.

Benefits to a SIEM / Ordr Integration:

- Integrate Ordr's insights into connected device security risks into your organizations "single pane of glass" security dashboard
- Increase efficiency for incident response (IR) workflows
- Identify security risks against device names, like "Axis P5532 Network Camera" instead of "AC:CC:8E:65:A6:B2"
- Complete visibility into every network-connected device, simplifying security, regulatory, and business reporting processes
- Integrates with SIEM solutions capable of parsing ingested syslog, including leading vendors such as:

exabeam | splunk> | IBM QRadar
LogRhythm | chronicle | MICRO FOCUS ArcSight

Case Study

An automotive parts manufacturer with more than 28 manufacturing plants, three technical centers, one software center and 13 customer service centers, serving more than 60 customers in every major region of the world including BMW, Ford, GM, Toyota, VW, and more, recently needed to address their managed and unmanaged device security risks.

Their environment included complex devices from infotainment (e.g., media players, in-car navigation, telematics, etc.) to fleet management and machine sensors. The team faced the daunting challenge of discovering and inventorying these managed and unmanaged devices, understanding the device behaviors and risks, then integrating this context into their IR workflow. Ordr mapped well to their key security requirements and the NIST Cyber Security Framework principles of Identify, Detect & Protect. Integrating Ordr with their existing SIEM solution allowed them to transform their IR workflow to incorporate rich device context to quickly and effectively triage incidents.

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.