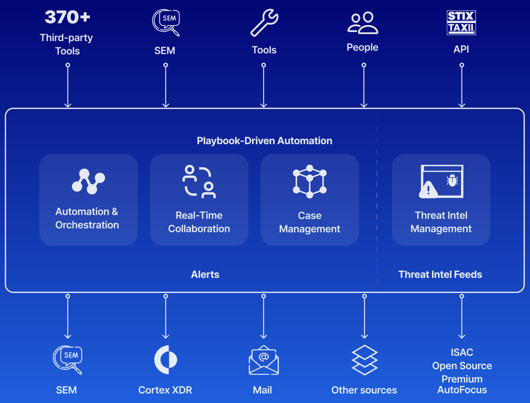
MAXIMIZE YOUR CORTEX XSOAR CAPABILITIES



Customize Your XSOAR App

Organizations typically implement out-of-the-box integrations and playbooks with the aim of rapidly automating threat incident response. Initial “proof of concept” playbooks are often implemented quickly and used to demonstrate that the concept works. The problems, however, often begin when you need to implement medium to high-complexity logic in your existing playbooks.

Common Problems You Might Encounter When Doing it In-house

- **Monitoring the App:** Changes to the API or version used by an integrated tool can disrupt functionality.
- **In-House Development Limits:** Custom development to address technical issues may not cover everything. This includes missing commands, API downtime, duplicate API responses, and event transmission/capture failures.
- **Out-of-the-Box Shortcomings:** Pre-built integrations may not be sufficient. Specific vendors in the toolchain may either have no content packs or have outdated ones.
- **Complexity:** Cortex XSOAR is a powerful tool, but its extensive functionality can be complex to set up and manage. You may need to invest in training for your security team to fully utilize its capabilities.
- **Compatibility:** Ensuring smooth integration with existing security tools can be tricky. Compatibility issues may arise between XSOAR and your existing platforms, requiring customization or workarounds.
- **Data Integration:** Security platforms often have different data formats. Transforming and integrating data between XSOAR and your existing systems can be a hurdle.

Building End-to-End Solutions to Maximize Your XSOAR Capabilities

Metron Security has deep expertise in developing end-to-end solutions with Cortex XSOAR to alleviate a slew of potential issues:

- Is a command missing? We implement it directly in the content pack.
- Need business logic specific to your use case? We will implement Automation Scripts included in the content pack.
- Need guidance on implementing your solution? Scheduled jobs, incident triggers, data persistence - Metron Security is here.
- Want to keep your content pack private? Or publish it to the XSOAR Marketplace? We support both workflows.

Metron Advantage

Expertise: Well-built and continuously-supported XSOAR apps for any-sized organization.

Fully-Managed: Complete oversight on the end-to-end process of development, customization, app certification, and continued on-demand support.

Streamlined: Metron Security maintains coding standards, merges PR, and coordinates with the XSOAR team for all updates. Our team provides real-time progress monitoring, support issue tracking via a custom JIRA Dashboard, and facilitates seamless collaboration.

Speed: Get started within 24 hours with up to 2x-3x cost savings compared to in-house.

Zero Risk: Fixed cost and no upfront payment. Invoiced only after delivery.

Metron Capabilities and Deliverables

- Architecture for multiple use cases: Threat Intel, XDR, NDR, or any other platform.
- Custom Playbooks — data enrichment, vulnerability management, ransomware response.
- Develop and design 100s of custom workflows and content packs.
- Automated scripts and custom code.
- Support in publishing the app in Cortex XSOAR Marketplace. Includes documentation, user guide, and integration video for internal use.
- Assistance with Cortex XSOAR Adopt-a-Pack program.

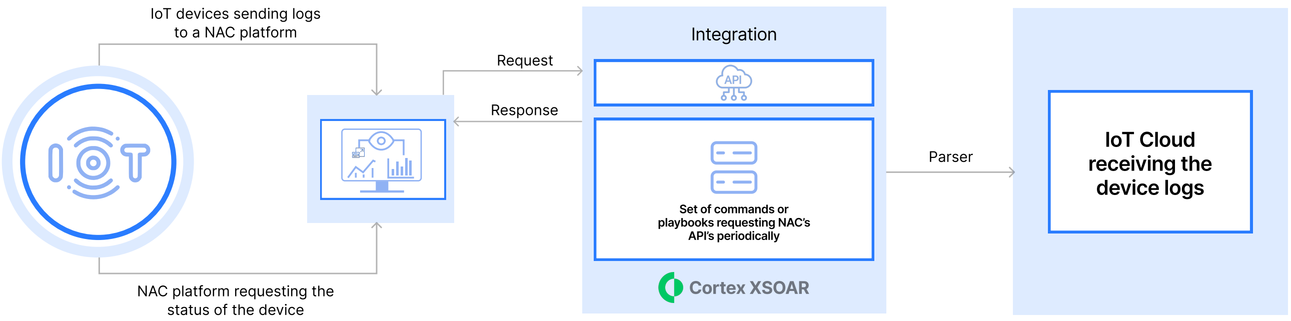
Case Studies

01 | XSOAR + WLC

This integration enables the security analyst to apply Access Control Lists (ACLs) and Quarantine Policies to the wireless IoT devices through the NAC platform.

It improves security by enabling a seamless data flow between the NAC platform and the IoT Cloud Management Service Provider through the APIs and minimizes the number of API calls and batch device updates.

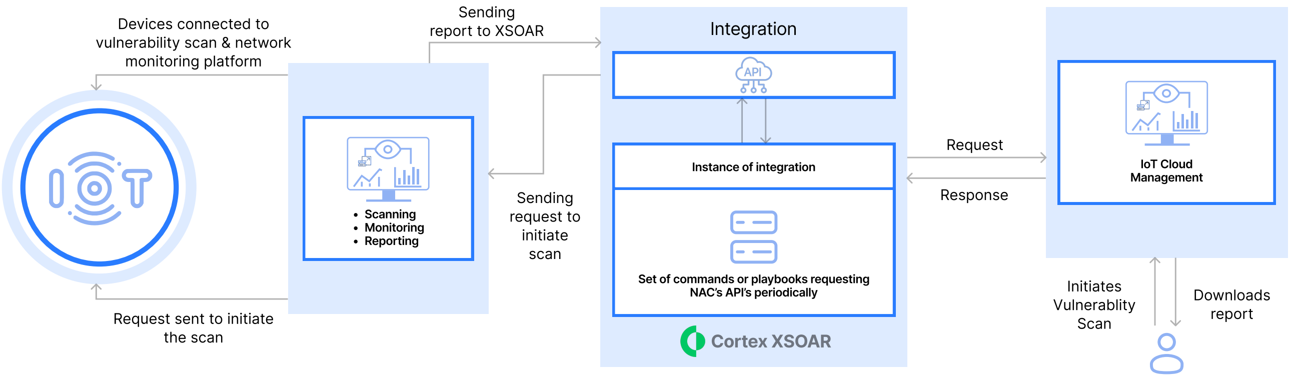
Mappers and classifiers were used to extract and map the required attributes related to the NAC platform and the policies to be applied to the devices. These techniques ensured that the correct incident-specific playbook was triggered to apply the appropriate policy to wireless IoT devices.


IoT devices sending logs to a NAC platform
IoT
Request
Response
Integration
API
Set of commands or playbooks requesting NAC's API's periodically
Cortex XSOAR
Parser
IoT Cloud receiving the device logs
NAC platform requesting the status of the device

02 | XSOAR + Vulnerability Management

The integration simplifies the vulnerability management process, allowing the organizations to initiate scans from both the Vulnerability Scanner and the IoT Cloud Management platform by syncing the data between the two platforms. It allows security analysts to download reports from the scan.

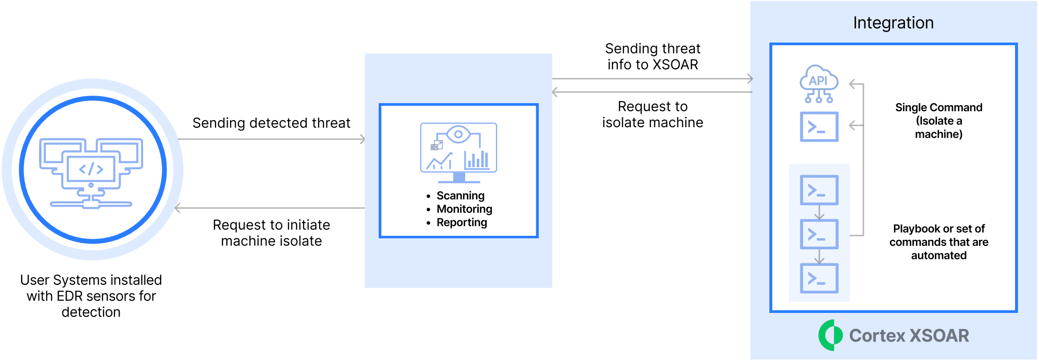
Real-time reporting on vulnerabilities in XSOAR enables organizations to prioritize vulnerabilities that require immediate attention, reducing the risk of data breaches.


Devices connected to vulnerability scan & network monitoring platform
Sending report to XSOAR
IoT
Scanning
Monitoring
Reporting
Sending request to initiate scan
Request sent to initiate the scan
Integration
API
Instance of integration
Set of commands or playbooks requesting NAC's API's periodically
Cortex XSOAR
Request
Response
IoT Cloud Management
Initiates Vulnerablity Scan
Downloads report

03 | XSOAR + EDR

XSOAR's integration with EDR enables automated workflows for quickly responding to threats, such as isolating infected machines and collecting forensic data. The integration offers an instance of EDR in XSOAR that requires configuring authentication credentials for the tool.

The playbooks developed in this integration can be used to automate the EDR process, including isolating machines, isolating users, and running custom scripts on the affected endpoint.


Sending detected threat
Request to initiate machine isolate
User Systems installed with EDR sensors for detection
• Scanning
• Monitoring
• Reporting
Sending threat info to XSOAR
Request to isolate machine
Integration
API
Single Command (Isolate a machine)
Playbook or set of commands that are automated
Cortex XSOAR

03 | XSOAR + EDR

XSOAR's integration with EDR enables automated workflows for quickly responding to threats, such as isolating infected machines and collecting forensic data. The integration offers an instance of EDR in XSOAR that requires configuring authentication credentials for the tool.

The playbooks developed in this integration can be used to automate the EDR process, including isolating machines, isolating users, and running custom scripts on the affected endpoint.

04 | XSOAR + IoT

his integration allows security teams to automate incident response workflows for IoT devices. By connecting Cortex XSOAR with IoT security platforms, organizations can automatically trigger actions based on detected threats or vulnerabilities.

This includes actions like isolating compromised devices, patching vulnerabilities, or notifying relevant stakeholders. This automation accelerates response times, reduces manual effort, and improves the overall security posture of IoT environments.

About Metron

Metron Security offers on-demand, effective third-party integration management for security ecosystems. Since 2014, Metron has delivered automation solutions for 300+ security applications and hundreds of custom solutions. Trusted by fast-growing security companies and MSSPs for their transparent process, security product expertise, and fixed-cost model, Metron helps clients achieve shorter development times and 2x-3x cost savings.

Metron Security is headquartered in Novato, CA, with development offices in Bangalore and Pune, India. Some of the scalable automation solutions we have built include:

- Custom middleware to ingest various types of security events
- Integration lab
- Custom playbooks for leading platforms
- Building Security Data Lakes in leading platforms
- Malware labs for security researchers

SafeBreach ZEROFOX cybereason servicenow
paloalto NETWORKS DEVO digital shadows_ a ReliaQuest company CROWDSTRIKE

Address

7250 Redwood Boulevard,
Suite 300,
Novato, CA 94945

AICPA SOC 2
AICPA Service Organization Control Reports
Formerly SAS 70 Reports

Contact Us

✉ prashant@metronlabs.com
www.metronlabs.com
☎ +1 888 840 3282 (DATA)