SOLUTION BRIEF

IronNet

IronNet and Cortex XSOAR

Reduce the impact of cyber attacks through advanced threat detection and automated response

Why we work better **together**

CORTEX XSOAR BY PALO ALTO NETWORKS

SOLUTION BENEFITS AT A GLANCE

Gain visibility across the threat landscape

Receive real-time collective threat intelligence, contextual information on new threats, and higher-order analysis of anomalies correlated across communities.

Increased effectiveness of existing SOC resources

Streamline operations and eliminate alert fatigue with curated threat ranking, integrated security tools, and automation of manual tasks.

Reduce impact of an attack

Lessen business repercussions and security risk by detecting threats earlier in the attack lifecycle through shared expert insights and proactive threat hunting.

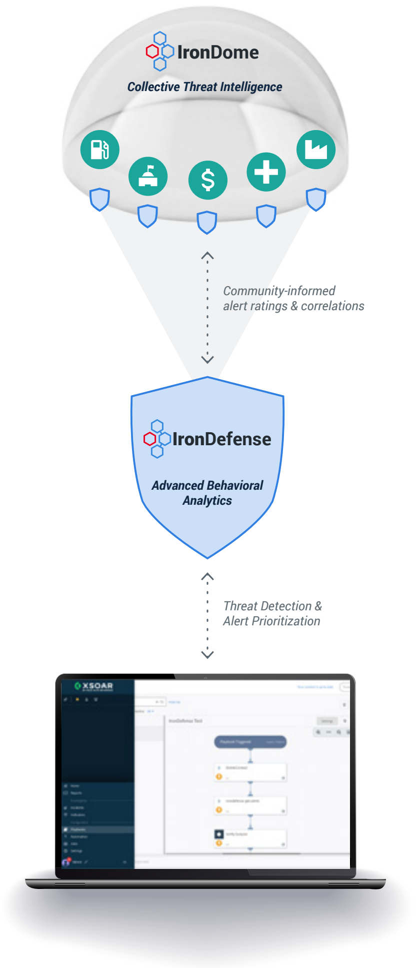
Designed by national security analysts and top intelligence data scientists, IronNet's scalable Network Detection and Response (NDR) solution and Collective Defense platform provide visibility across communities of enterprises. This approach allows peers to identify advanced threats often missed by existing commercial cybersecurity solutions.

Cortex XSOAR's security orchestration, automation, and response (SOAR) platform eliminates alert backlogs and maximizes the incident response capabilities of overburdened and understaffed security operations centers (SOC) by automating operational workflows and integrating security tools. The seamless integration of IronDefense with Cortex XSOAR enables more advanced threat detection, higher accuracy prioritization, faster mitigation, and proactive protection. IronDefense uses advanced behavioral analytics and collective intelligence to find unknown threats while weeding out false positives to avoid alert fatigue.

Meeting the challenge

Cyberdefense teams are isolated, using conventional tools that often miss advanced or unknown threats. These gaps increase the burden of already overworked security operations teams. There is a better way to defend. A collaborative, real-time, behavioral detection approach enables organizations to optimize their existing cybersecurity investments, reduce the impact of an attack, and gain broader visibility across their business ecosystems.

IronDefense works intuitively with Cortex XSOAR so security teams can easily manage resulting alerts by integrating teams, processes, and tools together to detect and mitigate suspicious network activity.


IronDome
Collective Threat Intelligence
Community-informed alert ratings & correlations
IronDefense
Advanced Behavioral Analytics
Threat Detection & Alert Prioritization
XSOAR

The feedback loop of information sharing between Cortex XSOAR and IronDefense continuously improves collective threat intelligence, speeds remediation, and strengthens your organization's cybersecurity stance.

How it works

IronDefense vets, prioritizes, and rates alerts long before they reach analysts. By automating time-consuming discovery steps and indicating the severity of anomalous traffic, analysts can make decisions on activity faster. Together with IronNet's IronDome Collective Defense solution, analysts have complete visibility into the threat landscape, delivering real-time, community-driven collective threat intelligence insights from peer enterprise SOCs.

When IronDefense data is ingested into Cortex XSOAR, it provides users with the ability to take proactive measures on next-generation firewall (NGFW) and endpoint detection and response (EDR) tools. Custom illustrations and dashboards make it easy to track data and operating metrics and perform mitigation actions, such as sending a containment command. This capability increases the effectiveness and ROI of other products integrated with Cortex XSOAR and helps to prevent future attacks. Leveraging the IronDefense Integration for Cortex XSOAR drives analyst workflow automation by eliminating many manual and tedious processes, allowing SOC analysts to focus their attention on analyzing alerts.

The IronDefense Integration for Cortex XSOAR also enables data upload and feedback. Users can share events, alerts, and analyst assessments with IronDefense to enable Collective Defense via the IronDome platform. Other IronDome participants will be able to see correlations across the community and use the information to improve their security posture. By sharing these discoveries with IronDome, Cortex XSOAR users are able to see attacker trends and achieve a cybersecurity Collective Defense for all IronDome participants.

Download the integration

The IronDefense Integration for Cortex XSOAR is available for download within the Cortex XSOAR user interface by selecting the Integrations tab, then Settings.

ABOUT IRONNET

IronNet is a global cybersecurity leader that is revolutionizing how organizations secure their enterprises by delivering the first-ever Collective Defense platform operating at scale. Our solutions leverage our unique offensive and defensive cyber experience to deliver advanced behavioral analysis and collective intelligence to detect known and unknown threats.