Unit 42 Managed Detection and Response Service

Best-in-Class Extended Detection and Response and Unit 42 Security Expertise, Delivered as a Managed Service

A Service Delivered by Palo Alto Networks World-Renowned Unit 42

Unit 42 experts work for you to detect and respond to cyberattacks 24/7, allowing your team to scale fast and focus on what matters most. We use Cortex XDR, so our analysts have unmatched visibility into all data sources (endpoint, network, cloud, and identity) to quickly identify and stop malicious activity most likely to impact your organization:

- Built on Cortex XDR
- Backed by Unit 42 expertise
- Enriched with world-class threat intelligence

Let Unit 42 MDR Address These Challenges

- **Cyberattacks are increasing in speed and sophistication**. The threat landscape is shifting to advanced, multistep attacks. Without constant coverage, proactive hunting, and immediate response, you may not stop these attacks before it's too late.
- **Prioritizing limited resources to combat the changing threat landscape**. Threat actors and their tactics change daily, and many organizations lack broad visibility to interpret and recognize attack indicators.
- **Security teams need help managing an endless backlog of alerts**. Overwhelmed by too many low-fidelity alerts, many security teams don't have additional time for threat hunting.

Key Benefits

- 24/7 monitoring of your Cortex XDR environment by Unit 42 security experts
- Direct communication with Unit 42 analysts if you ever have questions
- Proactive threat hunting when new vulnerabilities are identified in the wild
- Detailed threat and impact reports
- Continuous posture optimization drives improved security outcomes

Unit 42 MDR Delivers Complete Visibility Across Your Environment

Unit 42 experts leverage Cortex XDR to aggregate security telemetry from endpoints, network, cloud, and identity sources and apply high-fidelity threat intelligence; next-generation behavioral indicators; and AI-powered analytics to prevent, detect, and respond to even the most advanced threats.

Flexible Coverage Options to Fit Your Needs

Unit 42 MDR service starts with endpoints but can be configured to cover any combination of the following data sources:

Endpoint
Protect and detect threats on workstations and servers

Network
Firewall integration provides NTA and NIDS coverage

Cloud
Integrate third-party cloud security data, including cloud host data, traffic logs, and audit logs

Identity
Identity analytics from AD and Workday provide a 360-degree view of user behavior

The People and Operational Expertise to Keep Your Organization Safe

Our deep knowledge of Cortex XDR and connection to the Cortex R&D team allow us to scale the service without eroding service levels. The Unit 42 MDR team uses a mix of proprietary processes, infrastructure, and enrichment to accelerate detection, response, and threat hunting to quickly stop malicious activity most likely to impact your organization.

Unit 42 Service Features

Continuous Monitoring

- **Comprehensive visibility:** Cover endpoints, network, cloud, and identity data with SLO-driven, 24/7 monitoring and analysis of security incidents identified in Cortex XDR.
- **Alert management and incident triage:** Automated and manual review to analyze alert details, incidents, and generate BIoC or IoC rules to understand context and follow-up actions.
- **Notification and security event escalation:** Escalation of incidents that require attention, leveraging built-in logic and alert stitching aligned with MITRE ATT&CK framework.

Proactive Advanced Threat Hunting

- **24/7 hunting for advanced threats:** Sophisticated threat hunting based on analysis of suspicious signals, Cortex XDR analytics, custom detection rules, and Unit 42 research to identify and stop new threats.
- **High-fidelity threat intel:** Integration of industry-leading, comprehensive Unit 42 threat intelligence based on telemetry and detections from Palo Alto Networks products across our global customer base to inform and enrich investigations.
- **Actionable reporting:** Threat reports detailing the scope, source, and attack tools of threats, along with recommended actions; impact of emerging threats affecting multiple organizations to stay ahead of high-profile cyberattacks.
- **Direct assistance:** Easy access to threat hunting team to ask questions and get guidance about threats.

Managed Investigation & Response

- **Contain threats quickly:** Analysts will quickly contain active threats by isolating endpoints and removing malicious files or processes using Cortex XDR.
- **Streamlined investigations:** Investigate endpoints, analyze forensic artifacts, and network and cloud telemetry to identify incident root cause and scope.
- **Recover rapidly:** Use of Cortex XDR to remove malicious files, registry keys, and restore damaged files.

Security Posture Optimization

- **Health checks:** Identify gaps in hardening requirements with endpoint security profiles, device control, host firewall, and disk encryption.
- **Vulnerability assessments:** Identify and quantify security vulnerabilities (CVEs) for applications installed on your endpoints.
- **Host inventory:** Review the inventory of hosts to quickly identify any IT or security issues.

Extend Your Team with Unit 42 Experts

Unit 42 MDR provides a co-managed Cortex XDR user interface with integrated **two-way communication** with the Unit 42 team and **dashboards** for real-time visibility into incidents being managed as well as **key performance indicators**.

As new vulnerabilities are identified or a new threat actor is in the news, our threat hunters will proactively look for indicators of attack or vulnerable systems that have not been patched, providing detailed impact reports and recommended actions.

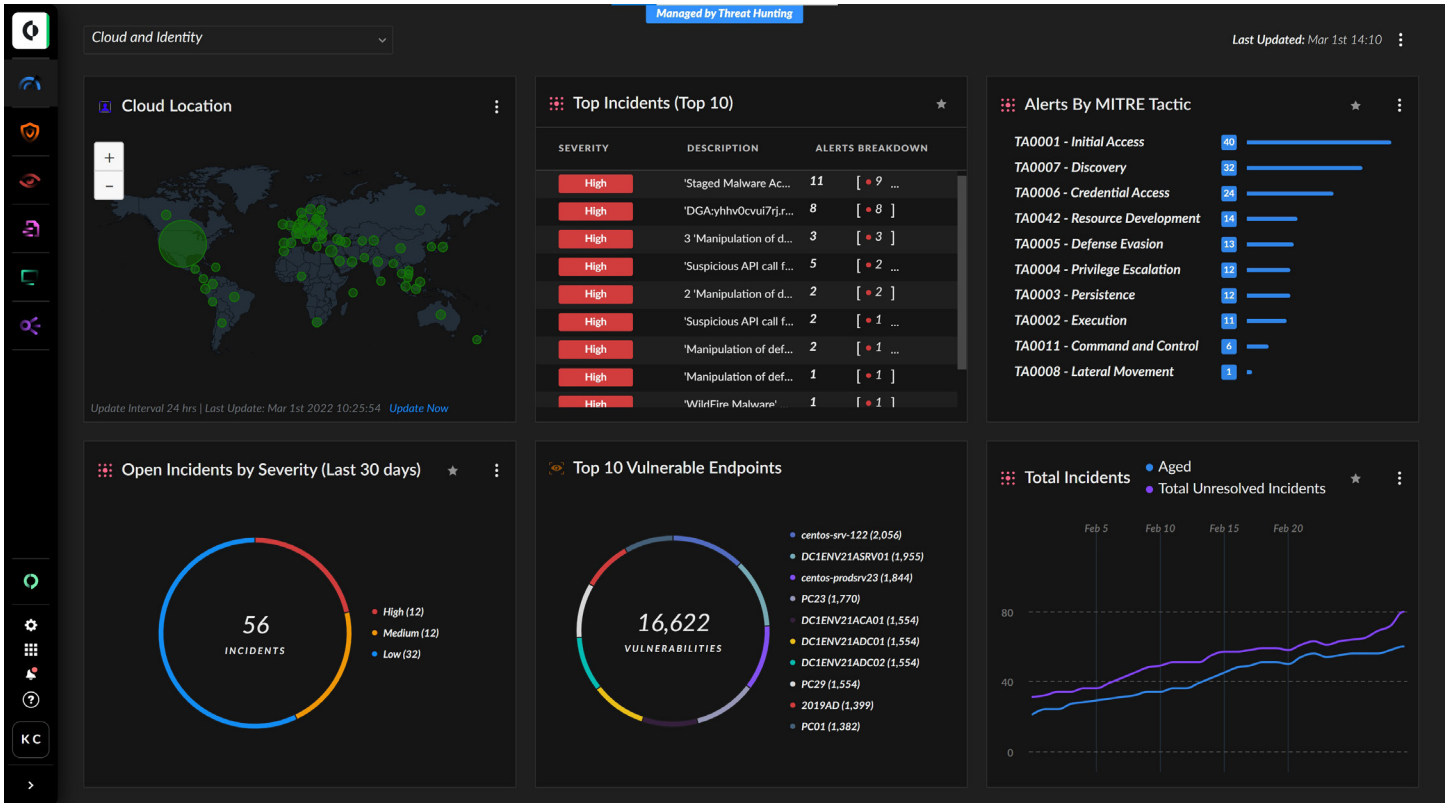

Figure 1: Cortex XDR dashboard

Backed by Unit 42 Expertise

Unit 42 security experts will continuously monitor your environment and hunt for threats. With more than 200 analysts, researchers, and engineers, the Unit 42 team advises and is trusted by CISOs around the globe. With this partnership, your team will be elevated by an elite team of security analysts, reducing the need to hire hard-to-find experts, giving you confidence in delivering the security, stability, and continuity your organization demands. And because Unit 42 will be familiar with your environment, we will be well positioned to respond to threats we've identified. Plus in the event of a major incident, you will have access to the Unit 42 Incident Response team. Our experts become an extension of your team—well-versed in your environment so they can respond quickly and accurately should an incident occur. This puts Unit 42 on speed dial, so we're ready to assist at a moment's notice.

When choosing Cortex XDR and an MDR service, why not choose the only service modeled after the SOC protecting the largest security company in the world—Palo Alto Networks?

About Cortex XDR

Cortex XDR® is the industry's first extended detection and response platform that integrates network, endpoint, cloud, and third-party data to stop sophisticated attacks. Cortex XDR has been designed from the ground up to help organizations like yours secure their digital assets and users while simplifying operations. Using behavioral analytics, it identifies unknown and highly evasive threats targeting your network. Machine learning and AI models uncover threats from any source, including managed and unmanaged devices.

About Unit 42

Palo Alto Networks Unit 42™ brings together world-renowned threat researchers, elite incident responders, and expert security consultants to create an intelligence-driven, response-ready organization that's passionate about helping you proactively manage cyber risk. Together, our team serves as your trusted advisor to help assess and test your security controls against the right threats, transform your security strategy with a threat-informed approach, and respond to incidents in record time so that you get back to business faster.

For the latest threat intel and research, please visit https://unit42.paloaltonetworks.com/.
To learn more about Unit 42, please visit https://www.paloaltonetworks.com/unit42.

paloalto® NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com