Unit 42 Managed XSIAM

24/7 Expert-Led Defense for Every Attack Surface

The Challenges of Modern SecOps

Today's cybersecurity operations are plagued by growing complexity, with 70% of attacks spanning across at least three attack surfaces.[1] The sheer volume of telemetry and siloed tools create noise rather than clarity, leaving organizations unable to connect fragmented events across endpoints, the cloud, networks, and identity systems.

As threats evolve, SecOps teams struggle to keep up. Outdated defenses allow threats to evolve quickly, with data exfiltration occurring three times faster over the last four years.[2] Reactive operations limit your ability to proactively hunt for threats, creating gaps in your security posture. Adding to these struggles, the constant need for security monitoring, adjustments, and fine-tuning security tools stretches internal SecOps resources thin, overwhelming SOCs and reducing operational efficiency.

Our Solution: Unit 42 Managed XSIAM

Managed XSIAM, powered by Cortex XSIAM® and delivered by Unit 42®, offers a transformative approach to managing the modern SOC. Combining the number one SOC transformation platform, Cortex XSIAM, with the cybersecurity expertise of the Unit 42 team addresses cyberthreats with precision and scalability. Because Unit 42 manages Cortex XSIAM, you'll be among the first to get automatic detections for emerging threats, ensuring proactive defenses across all your attack surfaces.

The elite Unit 42 team delivers end-to-end managed security operations that include:

- Zero-touch data onboarding and optimization.
- 24/7 protection for all attack surfaces.
- Intelligence-driven threat hunting.
- Custom detection engineering for your environment.
- Automation-fueled expert response.

With Unit 42 Managed XSIAM, you can rest easy knowing you'll get full visibility, stop attacks, hunt proactively, adapt detections, and respond faster.

75%

of incidents had evidence in logs, but silos prevented detection[3]

3X

faster time from compromise to data exfiltration over the last 4 years

See Everything

Zero-Touch Data Onboarding and Optimization

1K+ Integrations

Stop Attacks

24/7 Protection for All Attack Surfaces

7K Detectors | 2.4K ML | MITRE Proven

Hunt Proactively

Intelligence-Driven Threat Hunting

500B Events Daily[4]

30M+ Daily Malware Samples[5]

Adapt Detections

Custom Detection Engineering for Your Environment

2X Faster MTTD[6]

Respond Faster

Automation-Fueled Expert Response

Median Time to Resolution from Days to Mins.

A Better Approach

Many organizations continue to rely on legacy SIEM systems and outdated SOC infrastructures that can't keep pace with today's threat landscape. Security teams must juggle multiple roles—from incident response and threat research to writing correlation rules, fixing playbooks, and troubleshooting data ingestion issues—using tools that are reactive rather than proactive. This fragmented approach results in inefficiencies and gaps in visibility because static rules and delayed threat updates leave organizations vulnerable to fast-evolving risks. Meanwhile, the underutilization of automation playbooks and the lack of expert-level threat research further hinder a rapid and effective response.

Unit 42 offers a cutting-edge solution that manages your SOC, incorporates advanced analytics, applies machine learning, and uses proactive detection engineering to ensure round-the-clock detection and response across all potential attack surfaces. Proactive threat hunting is emphasized to swiftly identify and thwart evolving threats, while continuous enhancement is crucial through ongoing detection engineering and optimization of SOC operations. Implementing the automation playbooks helps streamline processes, decreases response times, and enhances overall SecOps effectiveness.

Let Unit 42 be your partner in building a proactive, future-ready SOC that stays ahead of even the most sophisticated attackers. You get:

- **Access to elite threat expertise:** Rely on the proven experience of the Unit 42 team to understand threats and bolster your security posture.
- **Enhanced threat detection:** Get broader coverage with ongoing detection engineering and data onboarding to identify and mitigate threats quickly and accurately.
- **Faster response:** Remediate threats faster with 24/7 threat response and expert-developed automation playbooks.
- **Proactive defense:** Stay ahead of adversaries with advanced and customized detection engineering and threat hunting.

About Unit 42

Palo Alto Networks Unit 42® brings together world-renowned threat researchers with an elite team of incident responders and security consultants to create an intelligence-driven, response-ready organization passionate about helping customers more proactively manage cyber risk. Our consultants serve as your trusted advisors to 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. For the latest threat intel and research, please visit https://unit42.paloaltonetworks.com.

1. *2025 Unit 42 Global Incident Response Report*, Palo Alto Networks, February 19, 2025.
2. Ibid.
3. Sam Rubin, "2025 Unit 42 Incident Response Report — Attacks Shift to Disruption," Palo Alto Networks, February 25, 2025.
4. "Palo Alto Networks Takes Aim At Cyber Attacks with the Expansion of Unit 42's Digital Forensics & Incident Response Service Globally," Palo Alto Networks, April 24, 2023.
5. "Unit 42: Threat Intelligence," Palo Alto Networks, accessed March 5, 2025.
6. Sharon Maydar, "Palo Alto Networks Excels in MITRE Managed Services Evaluation," Palo Alto Networks, June 18, 2024.

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

unit42_ds_unit-42-managed-xsiam_040325