Unit 42 Threat Intelligence

From Frontline Intelligence to Operationalized Protection

The threat landscape is accelerating. Adversaries are discovering vulnerabilities, evolving their tactics, and executing attacks faster than many security teams can adapt their defenses.

Organizations, meanwhile, face a surplus of threat data but a shortage of actionable intelligence. Security teams are inundated with indicators, alerts, vulnerabilities, reports and feeds, but often lack the context to identify the threats that matter to their environment and the ability to translate intelligence into immediate defensive action.

Palo Alto Networks **Unit 42 Threat Intelligence** redefines how organizations access and turn threat data into action by bringing together Cortex® XTI eXtended Threat Intelligence and Unit 42 Threat Intel Services. Built on a shared intelligence foundation, Cortex XTI embeds Unit 42 curated intelligence directly into SOC workflows, while Unit 42 services provide direct access to the analysts behind that intelligence. The result enables security teams to move from consuming intel to acting on it with confidence and speed.

The Unit 42 Intelligence Foundation

Powered by industry-leading threat research, massive global telemetry, and lessons from thousands of incident response engagements, our engine fuses AI-scale analysis with deep human expertise to deliver curated, continuously updated intelligence. It transforms fragmented threat data into high-confidence insights on emerging campaigns, malware, and adversary tactics, providing the context necessary to prioritize risk and take decisive action.

Cortex XTI: Activate Intelligence Across the SOC

Cortex XTI acts as the operational intelligence layer for the Cortex platform, by embedding Unit 42 insights directly into the tools where analysts investigate, hunt, and respond. By integrating high-fidelity Unit 42 intelligence, global telemetry, organizational context, and agentic reasoning, it surfaces relevant threats, maps them to your specific environment, and fuels faster response. The result is accelerated investigations, higher-confidence decisions, and more effective response actions.

Cortex XTI Key Capabilities

- Unit 42 Threat Intel Library
- Unit 42 Indicator Feed
- Embedded intelligence in investigation workflows
- Automated IOC management and targeted alerting
- Behavioral Threat Analysis
- TI-based playbooks and automations

Unit 42 Threat Intel Services: Elite Expertise.

Gain direct access to Unit 42 analysts for frontline expertise, expert context, and tailored guidance. Whether accelerating technical investigations, informing strategic planning, or supporting executive decisions, our experts help you prioritize risk and build long-term cyber resilience.

Unit 42 Threat Intel Services are available through three complementary offerings, enabling you to choose the level of analyst engagement and intelligence capabilities that best align with your organization's needs.

Service Offerings

Unit 42 Threat Intel Expertise

- Threat profile assessment
- Analyst on-demand and 1:1 Briefings
- Threat Actor and Malware Profiles
- Emerging Threat Research
- Ask 42 AI
- Agentic Malware Analysis (xMRE)
- Unit 42 Threat Feed

Unit 42 Designated Threat Intel Analyst

Unit 42 Deep and Dark Web Service

Global Threat Visibility, Integrated Workflows, and Elite Expertise

Together, Cortex XTI and Unit 42 Threat Intel Services help your teams transform findings from indicators, alerts, and reports into actionable guidance helping you to:

See what matters

Prioritize the threats that matter most to your organization and improve analyst productivity.

Understand the adversary

Understand attacker behavior to make faster, more informed security decisions.

Operationalize intelligence

Turn intel into faster defensive action to strengthen your security posture and build greater cyber resilience.

Why Unit 42 Threat Intelligence?

Palo Alto Networks Unit 42 Threat Intelligence redefines how you access and turn threat intelligence into action. Whether you embed native Unit 42 intelligence into your security operations with Cortex XTI or engage directly with Unit 42 experts, you gain the context and expertise needed to make more confident decisions, accelerate responsive actions, and strengthen your cyber resilience.

That advantage is powered by:

Unmatched global visibility

We draw on Palo Alto Networks visibility across 38 million telemetry signals from more than 70,000 customers; analyze billions of events, and 9 million novel threats daily to identify the threats most relevant to your organization.

Elite frontline expertise

Gain intelligence informed by thousands of incident response engagements, delivering battle-tested insights that go beyond threat indicators to provide real-world adversary context.

Native platform integration

Eliminate manual overhead by embedding insights directly into the Cortex platform.

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. Visit 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

© 2026 Palo Alto Networks, Inc. A list of our trademarks in the United States and other jurisdictions can be found at https://www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

unit42_Threat Intelligence Solution Brief_07312026