Unit 42 Threat Intel and Incident Response Services

Intelligence Driven. Response Ready.

Unparalleled Experience

Whether responding to a breach or managing cyber risk, we understand your challenges. Hailing from US government agencies, law enforcement, and global security firms, Unit 42 security consultants have handled some of the largest data breaches in history. Our breach response team is one of the busiest, responding to security incidents at a rate of more than 1,300 per year. Our risk management solutions are informed by this unparalleled experience, and we focus our assessments and prioritize recommendations based on attack vectors we see affecting organizations day in and day out. Our teams have conducted thousands of cyber risk evaluations and worked with organizations across the globe to identify and mitigate cyberthreats.

Built for Speed and Efficiency

We move fast to help our clients. Everything we do, from deployment to analysis and delivery of findings, is built for speed. We activate our incident response teams within minutes, integrating the specialized skill sets needed—from forensic consultants to malware analysts and team leaders. We move quickly to contain, investigate, and coordinate our response. We work with you to find the facts and maneuver through the critical decisions that get you back to business fast. In our risk management engagements, we appreciate that cybersecurity spending is an investment. We take care to consider where our clients' security budgets are focused—achieving the best return on investment in terms of risk mitigation. We deliver solutions on time, on budget, and designed for maximum impact.

Constant Innovation and Advanced Technology Drive Us

Staying ahead of the rapidly evolving threat landscape requires the best technology and constant innovation. We pride ourselves on the research, development, and creativity we put into solving our clients' cybersecurity challenges. Palo Alto Networks has developed and continues to evolve a powerful suite of technology-enabled threat prevention, detection, and incident response solutions. We integrate cloud native computing and machine learning AI to enable our teams to respond globally and at enterprise scale in minutes, not days or weeks. Our products allow Unit 42 to deploy faster, hunt smarter, investigate deeper, and contain completely.

For more information, please visit us at www.paloaltonetworks.com/unit42.

15

Average Years of Experience

1K+

Matters in 2021

24/7/365

Incident Response

Unit 42 Threat Intel and Incident Response Services

Incident Response

Incident Response

BEC Investigation

Respond and recover from unauthorized access to your enterprise email environment. Contain the incident, determine root cause, window of compromise, attacker activity, and quantify sensitive information exposed.

Ransomware Investigation

Respond to and recover from a ransomware attack. Contain the threat, determine root cause, window of compromise, attacker activity, and quantify sensitive information exposed. If needed, negotiate with threat actors, acquire and validate decryption keys, and develop and implement a recovery plan.

Cloud Incident Response

Respond to and recover from a cloud-based attack. Contain the threat incident. Identify initial attack vector, extent of unauthorized access and exfiltration, and identify scope of systems for remediation. Identify and implement additional safeguards.

Web App Compromise

Respond to and recover from a web application attack. Contain the threat, analyze logs, review code, quantify exposure or loss of sensitive information, and get recommendations for design hardening countermeasures.

Advanced Persistent Threat (APT) Investigation

Respond to and recover from a suspected APT incident. Contain the threat, determine root cause, window of compromise, attacker activity, and quantify sensitive information exposed.

PCI Investigation

Respond to and recover from a credit card data breach. Navigate the PFI process. Contain the threat, determine root cause, window of compromise, attacker activity, and quantify PCI information exposed.

Malware Analysis

Analysis of malware samples using open source intel, sandboxing, reverse engineering, and delivery of a report, including the behavior and functionality of the malware.

Data Mining

Identify and quantify sensitive data at risk as a result of a data breach for purposes of making notification decisions, including PHI, PII, PCI, and other sensitive and regulated information.

Cyber Risk Management

Strategic Advisory

Board of Directors & CISO Advisory

An assessment and review to identify cyber risk, create a current state profile, and build a security strategy to share with your executives and board.

M&A Cyber Due Diligence

Assess people, process, and technology to identify potential red flags, highlight hidden cybersecurity risks, and obtain an independent assessment of overall InfoSec program maturity in the context of a merger or acquisition.

Cyber Risk Assessment

Framework-based or regulated (NIST, CIS, ISO, CCPA, HIPAA, etc.) cybersecurity risk assessment to identify the current state of control implementation and gaps and create a strategic plan for a future state-enhanced InfoSec program.

Proactive Assessments

Compromise Assessment

Hunt for historical or ongoing indicators of compromise to identify evidence of unauthorized access or activity (across cloud, email, endpoints).

Security Operations Center (SOC) Assessment

Design and advisory services for design and build of next-gen SOC.

Cloud Security Assessment

Assess current cloud compute or service workload controls, security configuration, and policies to identify cybersecurity risks.

Supply Chain Risk Assessment

Evaluation and assessment of vendor-based supply chain cybersecurity risk to identify and mitigate the threat of supply chain attacks.

BEC Readiness Assessment

Targeted cybersecurity risk assessment focused on controls and the people, processes, and technologies necessary to defend against BEC and other email-based attacks.

Ransomware Readiness Assessment

Develop control enhancements, remediation recommendations, and a best-practice playbook to achieve a target state of ransomware readiness.

Incident Simulation

Tabletop Exercise

Simulate your response to a severe data security incident with key stakeholders with customized scenarios based on industry-specific threats and real-world breaches.

Purple Teaming

Up-level your security program by collaborating with Unit 42 to identify alerting gaps, tune defenses, and enhance security operations practices.

Unit 42 Threat Intel and Incident Response Services (continued)

Incident Response

Digital Forensics

Digital Investigation

Forensic collection, analysis, recovery, and reporting on information gleaned from digital media using scientific methods to determine what happened on that media or how it was used.

Insider Threat & Departing Employee Investigation

Investigate abuse of privileged access afforded to otherwise trusted employees, including identification of data accessed or misappropriated and/or unwanted actions taken by insiders.

Structured Data Investigation

Collection and analysis of SQL and NoSQL database environments, including external logs.

Expert Witness/Testimony/Litigation Support

Review digital evidence and discovery and offer expert opinions to the trier of fact in reports, declarations, depositions, or open court testimony.

Cyber Risk Management

Penetration Testing

Stress-test your organization's technical controls and cybersecurity by applying tactics, techniques, and procedures used by threat actors to gain unauthorized access and maintain a foothold in compromised environments.

Breach Readiness Review

Assess the people, processes, and technologies necessary to effectively respond to threats and a strategic roadmap to achieve a target state of breach readiness.

Security Consulting & Threat Intelligence

Security Program Design

Design governance frameworks, operational models, and a roadmap for your InfoSec program, including policies and standards, a control framework, and defense-in-depth strategy.

Virtual CISO

An interim or part-time CISO assigned to identify cyber risk and develop and mature your InfoSec program. The vCISO will create a cybersecurity strategy and work with IT, security, and the executive team to answer questions about the company's security posture.

Incident Response Plan Development

Assessment and advisory service focused on your team's readiness to prevent, detect, respond, and recover from a ransomware attack.

Expert Threat Briefing

This strategic threat briefing delivers a customized view of the threat landscape by a Unit 42 analyst, with access to a depth and breadth of data across endpoint, network, and cloud.

Unit 42 Retainer

When your organization faces a severe cyber incident, will you be ready? The speed of your response, as well as the effectiveness of your tools and playbooks, will determine how quickly you can recover. Extend the capabilities of your team by putting the world-class Unit 42 incident response and cyber risk management teams on speed dial.

From cases involving rogue insiders to organized crime syndicates and nation-state threats, Unit 42 performs more than 1,000 incident response investigations each year. The Unit 42 retainer gives you deep forensics and response expertise when you need it most, with predetermined service-level agreements (SLAs).

You can also allocate your retainer hours for proactive Unit 42 cyber risk management services scoped during the contract term. Our trusted advisors can assist your team with security strategy, assessment of technical controls, and overall program maturity.

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. With a deeply rooted reputation for delivering industry-leading threat intelligence, Unit 42 has expanded its scope to provide state-of-the-art incident response and cyber risk management services. 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. Visit paloaltonetworks.com/unit42.

Approved by Cybersecurity Insurance Plans

Unit 42 is on the approved vendor panel of more than 70 major cybersecurity insurance carriers. If you need to use Unit 42 services in connection with a cyber insurance claim, Unit 42 can honor any applicable preferred panel rate in place with the insurance carrier. For the panel rate to apply, just inform Unit 42 at the time of the request for service.

Under Attack?

If you think you may have been compromised or have an urgent matter, get in touch with the Unit 42 Incident Response team at start.paloaltonetworks.com/contact-unit42.html or call North America Toll-Free: 866.486.4842 (866.4.UNIT42), EMEA: +31.20.299.3130, UK: +44.20.3743.3660, APAC: +65.6983.8730, or Japan: +81.50.1790.0200.

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