Unit 42 Security Consulting Services

About Unit 42

Unit 42 brings together world-renowned threat researchers with an elite team of security consultants to create an intelligence-driven, response-ready organization. The Unit 42 Threat Intelligence team provides threat research that enables security teams to understand adversary intent and attribution while enhancing protections offered by our products and services to stop advanced attacks. As threats escalate, Unit 42 is available to advise customers on the latest risks, assess their readiness, and help them recover when the worst occurs. Unit 42 security consultants serve as trusted partners with state-of-the-art cyber risk expertise and incident response capabilities, helping you focus on your business before, during, and after a breach.

Unparalleled Experience

Whether responding to a breach or managing cyber risk, we understand your challenges. Hailing from U.S. 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 1,000 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 https://www.paloaltonetworks.com/unit42.

11
Average Years of Experience

1,300+
Matters in 2021

24/7/365
Incident Response

Unit 42 Security Consulting Service Offerings

Digital Forensics and Incident Response (DFIR)

Incident Response

Business Email Compromise
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 Breach 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/Credit Card Breach 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.

Proactive Services

Executive & Board Advisory

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.

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.

Board of Directors Security Strategy Review
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.

Proactive Assessments

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

BEC Readiness Assessment
Risk assessment focused on controls and the people, processes, and technologies necessary to defend against BEC and other email-based attacks.

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

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

Unit 42 Security Consulting Service Offerings (continued)

Digital Forensics and Incident Response (DFIR)

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.

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

Proactive Services

Red & Purple Team/Pentest Exercises
Simulated cyberattack to assess the strength of detection and countermeasures and to identify and exploit hidden security vulnerabilities. Can apply to web app, network, and cloud.

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 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.

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.

Get in Touch

If you'd like to learn more about how Unit 42 can help your organization defend against and respond to severe cyberthreats, visit https://start.paloaltonetworks.com/contact-unit42.html to connect with a team member.

Under Attack?

If you think you may have been breached, please email unit42-investigations@paloaltonetworks.com or call:

- US Toll-Free: +1.866.486.4842 (+1.866.4.UNIT42)
- EMEA: +31.20.299.3130
- JAPAC: +65.6983.8730

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_security-consulting-services_081121