Palo Alto Networks Takes Aim At Cyber Attacks with the Expansion of Unit 42's Digital Forensics & Incident Response Service Globally

April 24, 2023

With 60% of organizations taking more than four days to resolve cybersecurity issues, Unit 42's Global Incident Response Service dramatically reduces time to remediate threats

SANTA CLARA, Calif., April 24, 2023 /PRNewswire/ -- Palo Alto Networks (NASDAQ: PANW), the global cybersecurity leader, today announced the expansion of its Unit 42 Digital Forensics and Incident Response Service. The Global Digital Forensics and Incident Response service combines depth of incident response experience with the breadth of AI-powered solutions, including Cortex® XDR® and Xpanse ™, and Prisma® Cloud, to equip enterprises to respond immediately and recover faster than most any digital forensics and incident response (DFIR) service in the market.

To help organizations better respond to complex threats, Palo Alto Networks' unique knowledge of security and a deep understanding of advanced attacker behavior enables Unit 42 to undertake a rigorous investigation with rapid response. According to Wendi Whitmore, senior vice president of Palo Alto Networks Unit 42, "No other security vendor in the industry can match Palo Alto Networks' telemetry or our breadth of products to stop attacks in real-time. We analyze data from thousands of customers globally, generating over 500 billion daily events. This massive dataset enables responders to contextualize threats and respond effectively. Coupled with our expertise in cloud threats, SOC automation, and network security, this advanced intelligence helps companies recover and emerge stronger than before."

Unit 42 specializes in cyber DFIR and responds to thousands of customer events annually from ransomware incidents to the rising cloud attacks. Backed by a global team of incident responders, threat intelligence experts, and consultants, Unit 42 has handled some of the largest data breaches in history.

According to the recent Unit 42 Cloud Threat report, more than 60% of organizations take over four days to resolve security issues, while threat actors typically exploit a misconfiguration or vulnerability within hours. Unit 42 recently engaged with a large enterprise customer after a zero-day vulnerability allowed an authentication bypass and remote code execution (RCE) exploit. The threat actor leveraged the vulnerability to drop web shells and launch a crypto miner onto the client's unpatched CRM system hosted on a popular cloud service provider (CSP). Through unauthorized access, the threat actor stole a CSP credential that provided access to sensitive databases, which they made publicly available on the Internet. As part of the investigation, Unit 42 leveraged Cortex XDR to ingest the CSP CloudTrail logs for rapid threat hunting and analysis and Prisma Cloud to assess the client's CSP environment. Using Prisma Cloud, Unit 42 assisted the client in remediating the CSP misconfigurations and implementing security best practices during the incident, in real-time, improving their security posture overall.

The Unit 42 Digital Forensics and Incident Response Service includes

- **Assessments**: To evaluate and test controls against real-world threats proactively, Unit 42 offers many assessments, including compromise assessments, ransomware readiness assessments, attack surface assessments, and more.
- **IR Preparedness:** Helping organizations pressure test technical controls, network security, response playbooks, and more. Services include Penetration Testing, Purple Teaming and Tabletop exercises.
- **Incident Response**: Quickly jumpstart an intelligence-led investigation, deploying Palo Alto Networks tools within minutes to contain threats and gather the evidence needed to analyze an incident fully. Unit 42 IR services include cloud incident response, expert malware analysis, and ransomware investigation.
- **Managed Threat Hunting:** Offers round-the-clock monitoring from Unit 42 experts to discover attacks anywhere in an organization. Threat hunters work on an organization's behalf to discover advanced threats, such as state-sponsored attackers, cybercriminals, malicious insiders, and malware.
- **Managed Detection and Response:** Combines Cortex XDR with Unit 42's industry-leading threat intelligence to offer continuous 24/7 threat detection, investigation and response.

In the Forrester Wave™: Cybersecurity Incident Response Services, Q1 2022 Forrester noted that organizations "…seeking support in preparing for and responding to incidents in sprawling cloud environments should look at Palo Alto Networks."

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 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.

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? 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.

Follow Palo Alto Networks on Twitter, LinkedIn, Facebook and Instagram.

About Palo Alto Networks
Palo Alto Networks is the world's cybersecurity leader. We innovate to outpace cyberthreats, so organizations can embrace technology with confidence. We provide next-gen cybersecurity to thousands of customers globally, across all sectors. Our best-in-class cybersecurity platforms and services are backed by industry-leading threat intelligence and strengthened by state-of-the-art automation. Whether deploying our products to enable the Zero Trust Enterprise, responding to a security incident, or partnering to deliver better security outcomes through a world-class partner ecosystem,

we're committed to helping ensure each day is safer than the one before. It's what makes us the cybersecurity partner of choice.

At Palo Alto Networks, we're committed to bringing together the very best people in service of our mission, so we're also proud to be the cybersecurity workplace of choice, recognized among Newsweek's Most Loved Workplaces (2021 and 2022), Comparably Best Companies for Diversity (2021), and HRC Best Places for LGBTQ Equality (2022). For more information, visit www.paloaltonetworks.com.

View original content to download multimedia:https://www.prnewswire.com/news-releases/palo-alto-networks-takes-aim-at-cyber-attacks-with-the-expansion-of-unit-42s-digital-forensics--incident-response-service-globally-301805134.html

SOURCE Palo Alto Networks, Inc.

Matt Manturi, Manager, Public Relations, mmanturi@paloaltonetworks.com