Unit 42 Cloud Incident Response

A Dynamic Approach to Securing the Cloud with Unit 42 Incident Response Experts Who Understand the Special Nature of Cloud Security

Understanding Cloud Incident Response

As cloud adoption grows, even simple mistakes or misconfigurations lead to outsized impact. Traditional digital forensics and incident response (DFIR) was simply not designed for complex cloud-based threats. With Unit 42 expertise and tools, you won't have to learn a whole new set of tools, concepts, and capabilities during a crisis. Our cloud threat researchers continuously work to understand threats specific to the cloud, enabling you to undertake a more effective investigation and response. We help you identify and eradicate complex cloud incidents using digital forensics and response methods specifically designed for dynamic cloud environments.

Using our cutting-edge cloud technology, including Cortex XDR, Cortex Xpanse, and Prisma Cloud, we'll quickly discover the attack vector, identify the extent of access and the data at risk, and work with you to take the appropriate remediation actions. Cortex Xpanse provides an external view of your attack surface, while Prisma Cloud and Cortex XDR provide granular tooling, automated remediation, and forensic capabilities.

When an incident does occur, you can work with our team to cut through the petabytes of data and noise to home in on the key indicators of compromise in your cloud environments. As with all incident response matters, we jump-start your investigation with a wealth of threat intelligence. Unit 42 IR experts have experience and training performing incident response in a variety of cloud environments. We have cloud-specific methods to help you recover from cloud incidents, including methods for rapid scoping, access, collection, investigation, and containment specific to the different public cloud providers. To streamline your response, we have playbooks for the top cloud incidents you may face.

With the new capabilities you gain by working with Unit 42, you'll reduce the need to hire hard-to-find experts during your darkest hour and have confidence in moving to the cloud while still delivering the security, stability, and business continuity your organization demands.

Unit 42 Cloud IR Benefits

Investigate with Speed

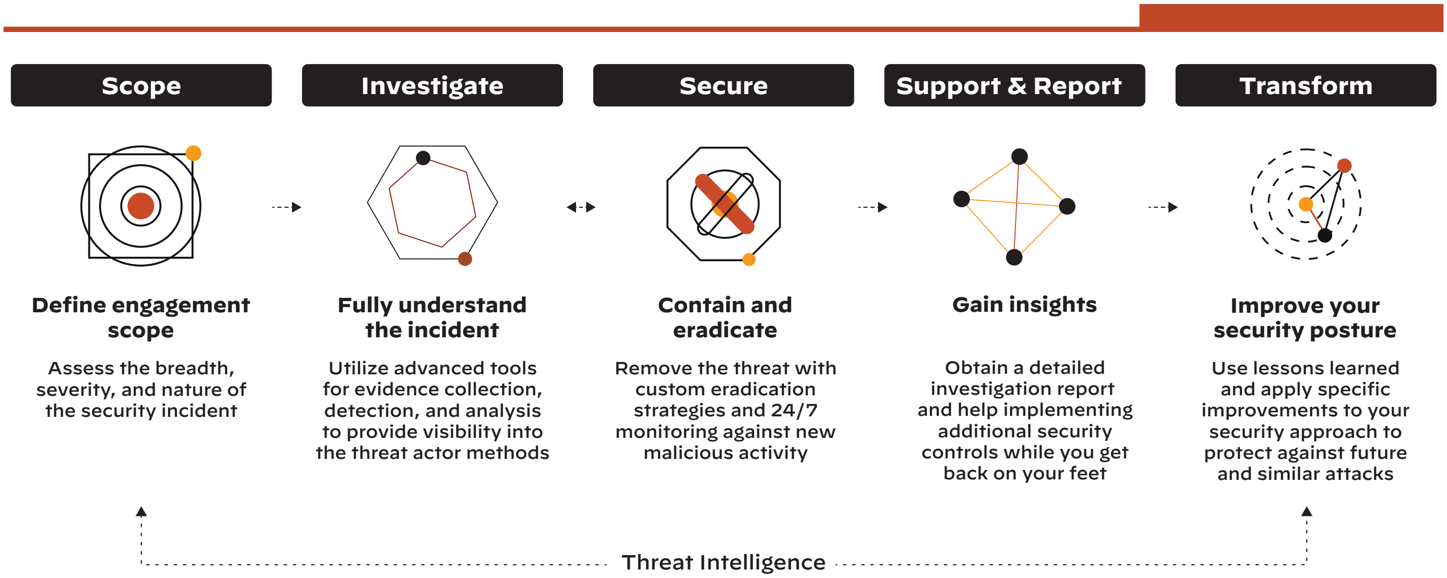
Understand the incident attack vector, extent of access, and quantify data at risk by working with Unit 42 cloud experts. Our knowledge of the special nature of cloud security enables you to undertake a more effective investigation and response.

Respond Fast to Reduce the Impact

Quickly address and contain cloud-specific threats using industry-leading cloud tools. We'll work with you to eliminate the threat and enhance your cloud security now and in the future.

Recover with Confidence

Return to normal faster with an optimized approach for each stage of the cloud incident lifecycle. Our SLA-driven response with prearranged communication channels and predefined playbooks reduces the costs of an incident so you can get back to business.



Scope

Define engagement scope

Assess the breadth, severity, and nature of the security incident

Investigate

Fully understand the incident

Utilize advanced tools for evidence collection, detection, and analysis to provide visibility into the threat actor methods

Secure

Contain and eradicate

Remove the threat with custom eradication strategies and 24/7 monitoring against new malicious activity

Support & Report

Gain insights

Obtain a detailed investigation report and help implementing additional security controls while you get back on your feet

Transform

Improve your security posture

Use lessons learned and apply specific improvements to your security approach to protect against future and similar attacks

Threat Intelligence

Figure 1: Cloud IR methodology

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, the unique insights and threat intelligence from Unit 42 experts can only be gained by working over 1,000 matters per 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 credits 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.

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.

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.

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