How Nine Organizations Respond to—and Prepare for—Cyberthreats

Before, During, and After an Attack, Unit 42® Is the Partner of Choice

paloalto® NETWORKS | UNIT 42®

Intelligence Driven and Response Ready

Unit 42 supports organizations around the world with unparalleled threat intelligence and deep security expertise.

Attack surfaces are expanding. The threat landscape continues to change rapidly, and security and resiliency are under more scrutiny than ever. Organizations everywhere are feeling the effects—and you can't solve the problem with technology alone.

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. We serve as your trusted advisors to assess and test your security controls against the threats most likely to impact you, transform your security strategy with a threat-informed approach, and respond to incidents in record time.

Incident Response

Proactive Services

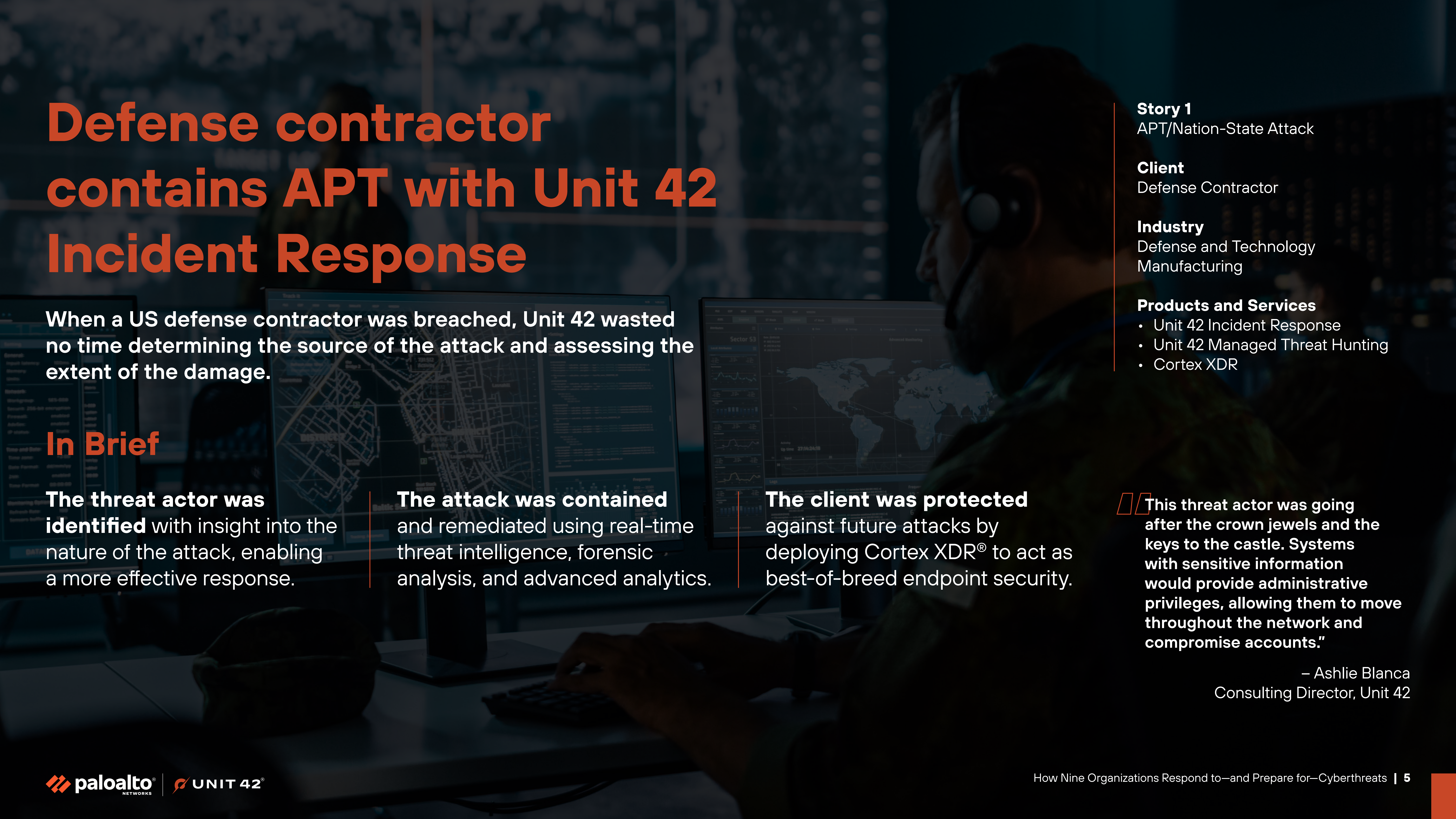
Managed Services

Contents

Incident Response Stories

Respond with confidence. The clock starts immediately when a potential breach is identified. That's when you need a partner who can swiftly investigate and provide crucial answers to the difficult questions: How did the attackers get in? Which systems or data were compromised? What is the impact? How do you evict the intruders and keep them out?

See how Unit 42's elite team has helped organizations stop attacks and prevent the next ones too.



Defense contractor contains APT with Unit 42 Incident Response

When a US defense contractor was breached, Unit 42 wasted no time determining the source of the attack and assessing the damage.

Story 1
APT/Nation-State Attack

Client
Defense Contractor

Industry
Defense and Technology Manufacturing

Products and Services
- Unit 42 Incident Response
- Unit 42 Managed Threat Hunting
- Cortex XDR

In Brief

The threat actor was identified with insight into the nature of the attack, enabling a more effective response.

The attack was contained and remediated using real-time threat intelligence, forensic analysis, and advanced analytics.

The client was protected against future attacks by deploying Cortex XDR® to act as best-of-breed endpoint security.

> **“This threat actor was going after the crown jewels and the keys to the castle. Systems with sensitive information would provide administrative privileges, allowing them to move throughout the network and compromise accounts.”**
>
> – Ashlie Blanca
> Consulting Director, Unit 42

Challenge

A breach at a US defense and technology manufacturer posed a national security risk. The organization enlisted Unit 42 Incident Response, which quickly determined that the attacker was still inside.

Solution

The high-stakes engagement required real-time threat intelligence alongside forensic analysis and advanced analytics capabilities.

To accomplish this, Unit 42 IR deployed Cortex XDR across the customer's environment. Leveraging Cortex XDR, Unit 42 Managed Threat Hunting (MTH) and Threat Intelligence teams identified indicators of compromise (IoC) matching those of a Chinese APT associated with the TiltedTemple campaign. Equipped with this information, Unit 42 IR was able to quickly investigate and contain the incident, stopping the threat actor in their tracks.

READ FULL STORY

Story 1
APT/Nation-State Attack

Client
Defense Contractor

Industry
Defense and Technology Manufacturing

Products and Services

- Unit 42 Incident Response
- Unit 42 Managed Threat Hunting
- Cortex XDR

Infrastructure manufacturer reclaims control after dual ransomware attacks

Facing significant potential financial, operational, and reputational consequences, the client turned to Unit 42 to restore operations and protect sensitive data.

Story 2
Black Basta and LockBit Ransomware Attack

Client
Infrastructure Manufacturer

Industry
Manufacturing

Products and Services
- Unit 42 Incident Response
- Unit 42 Managed Detection and Response
- Cortex XDR

Results

73%
reduction in ransom payment due to expert negotiation.

< 5 days
to identify patient zero and the extent of the data exfiltration plus block all known ransomware IoCs.

2.5+ million
files prevented from being exposed as a result of negotiations.

> **"This attack was very challenging, but Unit 42's knowledge, patience, and guidance were invaluable."**
>
> – Senior Director of Risk Management
> Infrastructure Manufacturer

Challenge

Dual ransomware attacks from Black Basta and LockBit crippled the operations of an infrastructure equipment manufacturer. The adversaries first exfiltrated sensitive data and then detonated ransomware that encrypted critical files within 24 hours.

Solution

Unit 42 got to work immediately:

- Assessing the scope of each attack and identifying the initial access points and extent of data exfiltration
- Containing the threats by deploying Cortex XDR to block ransomware IoCs and initiating 24/7 threat monitoring with Unit 42 MDR
- Eradicating the threat actors from the environment and negotiating down the ransom demands

READ FULL STORY

Story 2
Black Basta and
LockBit Ransomware Attack

Client
Infrastructure Manufacturer

Industry
Manufacturing

Products and Services
- Unit 42 Incident Response
- Unit 42 Managed Detection and Response
- Cortex XDR

Telecom provider contains Black Basta attack and restores operations

The client called on Unit 42 to assess the extent of unauthorized access, negotiate the ransom payment, and eradicate the threat.

Story 3
Black Basta Ransomware Attack

Client
Telecom Provider

Industry
Telecom

Products and Services
- Unit 42 Incident Response
- Unit 42 Managed Detection and Response
- Cortex XDR

Results

3 days
to determine the attack vector in an endpoint environment.

80%
reduction in ransom with expert negotiation.

48 hours
to contain the threat and ensure continuity of business operations.

Challenge

Over the course of 13 hours, a major telecom provider was hit with a severe ransomware attack that encrypted files on tens of thousands of systems, exfiltrated sensitive data, and brought 50% of its business operations to a halt.

Solution

Unit 42 IR began assessing the attack within 2 hours. Forensics and threat hunting quickly revealed Black Basta ransomware, the initial phishing email, and the extent of unauthorized access. Cortex XDR was deployed across the impacted environment to ensure that the attack was contained, enabling the Unit 42 Managed Detection and Response (MDR) team to begin 24/7 monitoring and threat hunting.

Unit 42 negotiated an 80% reduction of the initial ransom demand and obtained, tested, and implemented decryption keys. The team also identified vulnerabilities and deployed additional firewall and access control technologies.

READ FULL STORY

Story 3
Black Basta Ransomware Attack

Client
Telecom Provider

Industry
Telecom

Products and Services

- Unit 42 Incident Response
- Unit 42 Managed Detection and Response
- Cortex XDR

Welfare warfare: Battling cyberthreats for a social agency

The Philippines' Department of Social Welfare and Development (DSWD) benefits from Unit 42 and the Cortex XDR endpoint security solution.

Story 4
Trigona Ransomware Attack

Client
The Philippines' Department of Social Welfare and Development (DSWD)

Industry
Government

Products and Services
- Unit 42 Incident Response
- Unit 42 Retainer
- Cortex XDR

In Brief

100% of Trigona ransomware attacks were stopped.

Minutes to block threats with Cortex XDR BIoC rules, implemented by Unit 42.

Eradicated previously missed threats. Unit 42 detected a threat actor that had been dormant for 1–2 years.

> **"Given the frequency and severity of cyberattacks presently, the DSWD needed to take steps to conduct a proper investigation and discover if threat actors were still within our infrastructure."**
>
> – Julius Gorospe
> Assistant Secretary and
> Chief Information Officer, DSWD

Challenge

The lead agency for social welfare in the Philippines, the DSWD was contending with inadequate visibility from legacy security tools, fragmented cybersecurity policies, and a lack of comprehensive response playbooks, making it vulnerable to attacks.

Solution

Unit 42's ongoing support has included:

- Remaining on call 24/7 to respond to incidents through a Unit 42 Retainer
- Thwarting an attack attempt via Trigona ransomware (with Cortex XDR)
- Establishing single-pane-of-glass visibility across different platforms
- Consolidating threat intelligence in accessible threat intelligence reports

READ FULL STORY

Story 4
Trigona Ransomware Attack

Client
The Philippines' Department of Social Welfare and Development (DSWD)

Industry
Government

Products and Services

- Unit 42 Incident Response
- Unit 42 Retainer
- Cortex XDR

> **"Unit 42's involvement ensured that any security incidents were dealt with swiftly and effectively, minimizing their impact on DSWD's operations and the people they serve."**
>
> – Julius Gorospe
> Assistant Secretary and
> Chief Information Officer, DSWD

Proactive Services Stories

Assess. Test. Protect. Information is key to protection. As an organization, you must identify security risks as well as understand your security posture. Only then can you build the foundations for strong cybersecurity, including policies, procedures, standards, workflows, and strategic roadmaps to success.

See how Unit 42 has delivered tailored proactive services to clients regardless of size, industry, and cybersecurity experience.

Multinational organization enhances defenses by stress-testing its cybersecurity program

Story 5
Security Program Design

Client
Multinational Corporation

Industry
Global Business

Products and Services
- Unit 42 Security Program Design
- Unit 42 Purple Team Exercises

In Brief

The client wanted a partner with the business and technical expertise to help improve its security posture in alignment with NIST standards, including uncovering inefficiencies across its people and processes.

The engagement required an assessment and attack simulation to measure the organization's security program—including the effectiveness of SecOps controls, security team processes, and communication.

Leveraging the expertise of Unit 42, the company improved readiness, strengthened controls and compliance, improved coordination among stakeholders, and increased visibility to the board of directors.

Challenge

A multinational corporation with a global workforce sought an expert partner to bolster its security posture—including uncovering inefficiencies across its people, processes, and technology. The organization chose Unit 42 to assess and test the effectiveness of its security operations.

Solution

Using the Cybersecurity Framework from the National Institute of Standards and Technology (NIST) and other proprietary controls, Unit 42 assessed the client's capabilities in threat intelligence, threat hunting, detection, and response as well as its monitoring and reporting controls. Next, Unit 42 ran an attack simulation in the client's environment, ultimately delivering an in-depth technical report and empowering the client to maximize its security investments.

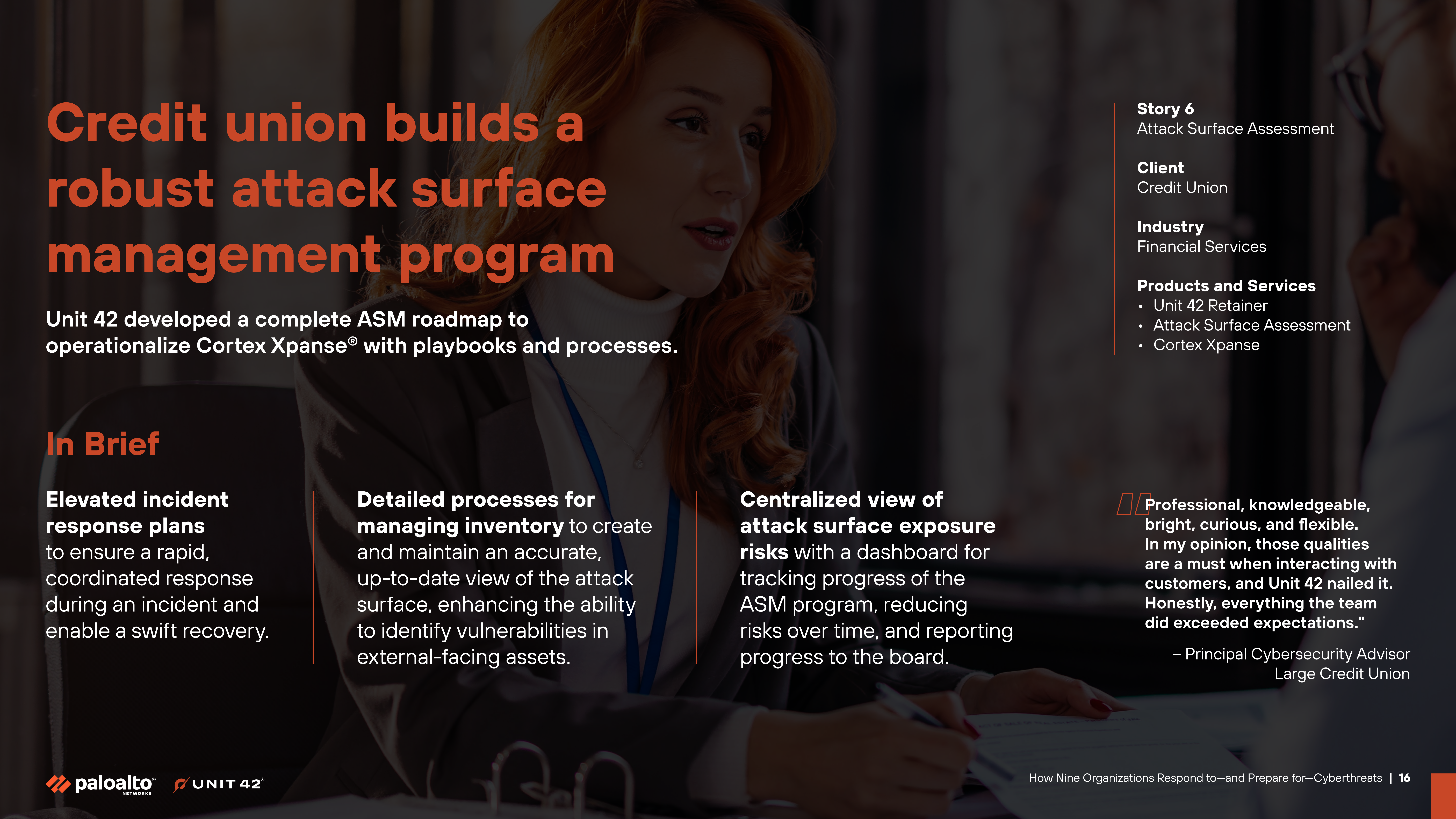
READ FULL STORY

Story 5
Security Program Design

Client
Multinational Corporation

Industry
Global Business

Products and Services
- Unit 42 Security Program Design
- Unit 42 Purple Team Exercises



Credit union builds a robust attack surface management program

Unit 42 developed a complete ASM roadmap to operationalize Cortex Xpanse® with playbooks and processes.

Story 6
Attack Surface Assessment

Client
Credit Union

Industry
Financial Services

Products and Services
- Unit 42 Retainer
- Attack Surface Assessment
- Cortex Xpanse

In Brief

Elevated incident response plans to ensure a rapid, coordinated response during an incident and enable a swift recovery.

Detailed processes for managing inventory to create and maintain an accurate, up-to-date view of the attack surface, enhancing the ability to identify vulnerabilities in external-facing assets.

Centralized view of attack surface exposure risks with a dashboard for tracking progress of the ASM program, reducing risks over time, and reporting progress to the board.

> **“Professional, knowledgeable, bright, curious, and flexible. In my opinion, those qualities are a must when interacting with customers, and Unit 42 nailed it. Honestly, everything the team did exceeded expectations.”**
>
> – Principal Cybersecurity Advisor
> Large Credit Union

Challenge

A credit union based in Canada had recently established a program to scan for external vulnerabilities to identify potential security misconfigurations, but there was no dedicated solution to help manage the process. The organization saw an opportunity in Palo Alto Networks Cortex Xpanse and called on Unit 42 to build a roadmap and provide recommendations for 11 security functions.

Solution

Leveraging the capabilities of Cortex Xpanse, Unit 42 developed a comprehensive assessment and roadmap for an attack surface management program, including:

- Five incident response playbooks to respond to vulnerable, exposed assets found by Cortex Xpanse.
- Replacement of manual asset inventories leveraging ServiceNow, enabling a more efficient process to identify, prioritize, and remediate security issues.
- Monitoring of incidents and overall activity with dashboards that offer graphical overviews.
- A centralized view of the attack surface, including real-time alerts, incident trends, vulnerability discoveries, and asset distribution across cloud providers.

Story 6
Attack Surface Assessment

Client
Credit Union

Industry
Financial Services

Products and Services

- Unit 42 Retainer
- Attack Surface Assessment
- Cortex Xpanse

Global software provider enhances worldwide incident readiness

Unit 42's follow-the-sun Tabletop Exercise uncovers opportunities for improvement.

Story 7
Tabletop Exercises

Client
Cloud-Based Business Software Provider

Industry
Technology

Products and Services
- Unit 42 Retainer
- Unit 42 Tabletop Exercises

In Brief

A custom engagement was developed to stress-test specific concerns in the organization's incident response process.

Expert threat intelligence and guidance from Unit 42 validated the organization's defenses against threats.

A data-driven report was produced pinpointing strengths and opportunities for improvement to guide future investments.

Challenge

To continuously assess and improve its security posture, a multinational software provider invested in a Unit 42 Retainer. It tasked Unit 42 with assessing the strengths of and opportunities to improve its incident response capabilities across Europe, North America, and Asia-Pacific.

Solution

Leveraging unique threat intelligence about the sophisticated threat group Muddled Libra, Unit 42 developed and conducted a custom Tabletop Exercise evaluating the client's handling of a global attack from the group. Afterward, Unit 42 provided a comprehensive analysis of the company's incident response capabilities, with detailed guidance and recommendations.

Story 7
Tabletop Exercises

Client
Cloud-Based Business
Software Provider

Industry
Technology

Products and Services
- Unit 42 Retainer
- Unit 42 Tabletop Exercises

Managed Services Stories

Monitor. Threat hunt. Report. Unit 42 consultants work for you to detect and respond to cyberattacks. They build an intelligence-informed approach to cybersecurity strategy, and they respond to incidents in record time. It's 24/7/365 support, allowing you to scale fast and focus on what matters most.

See how Unit 42 experts strengthen the security posture of organizations like yours.

Boyne Resorts achieves game-changing SOC improvements with Cortex XSIAM and Unit 42 MDR

The company's partnership with Palo Alto Networks transformed its posture and its SOC.

Story 8
SOC Transformation

Client
Boyne Resorts

Industry
Hospitality

Products and Services
- Unit 42 Managed Detection and Response
- Unit 42 Retainer
- Cortex XSIAM

In Brief

98% reduction in median time to resolution, leveraging Cortex XISAM® automation capabilities and Unit 42 MDR.

65% reduction in open incidents from 80–100 to 35 per day, due to reductions in false positive rates and duplicate incidents.

Data sources rose from 1 to 21, increasing visibility into potential threats and enabling more in-depth, proactive threat hunting by Unit 42.

> **"The MDR team handles our investigations, forwarding any alerts, and shares a detailed report that helps us make quicker, more accurate decisions on those incidents. This saves our team a huge amount of time."**
>
> – Kenny Hicks
> Lead Security Engineer
> Boyne Resorts

paloalto® NETWORKS | UNIT 42®

Challenge

At Boyne Resorts, strengthening security across thousands of devices and reams of data required more than its existing security controls could provide, so it made the transition to Cortex XSIAM. But Boyne's security leaders didn't only want to strengthen the company's security posture; they also needed a 24/7 SOC built on best practices.

Solution

Boyne engaged Unit 42 MDR services to provide 24/7/365 coverage using the Cortex XSIAM platform, enabling the company to leverage Unit 42's world-class threat intelligence and extensive expertise in both security and Cortex® products. With continuous monitoring and proactive threat hunting by Unit 42 MDR, Boyne analysts are confident that even when they don't have eyes on their environment, a trusted partner does.

READ FULL STORY

Story 8
SOC Transformation

Client
Boyne Resorts

Industry
Hospitality

Products and Services

- Unit 42 Managed Detection and Response
- Unit 42 Retainer
- Cortex XSIAM

> **"The Unit 42 Retainer played perfectly with our MDR and SIEM services. The MDR team's ability to transition directly to the Unit 42 team during an incident response scenario is exactly what we wanted."**
>
> – Kenny Hicks
> Lead Security Engineer
> Boyne Resorts

Enloe Medical Center strengthens security with Unit 42 MDR

The hospital needed 24/7 monitoring by a team with expertise in Cortex XDR. It found one in Unit 42.

Story 9
SOC Modernization

Client
Enloe Medical Center

Industry
Healthcare

Products and Services
- Unit 42 Managed Detection and Response
- Unit 42 Retainer
- Cortex XDR

In Brief

Risk and exposure were significantly reduced with proactive threat hunting and reporting.

Morale was boosted and turnover neutralized with SecOps process continuity.

Higher-value work was enabled with Unit 42 security experts continuously monitoring for threats.

> **“We're excited to be partnering with Palo Alto Networks Unit 42 MDR. They stay awake so you can sleep.”**
>
> – Tom Osteen
> Chief Information Officer
> Enloe Medical Center

Challenge

After a ransomware attack, Enloe Medical Center adopted Cortex XDR, gaining visibility and detection from the perimeter to the endpoint. But with turnover on its cybersecurity team, Enloe was losing the expertise needed to administer its cybersecurity tools. The company began looking for a trusted partner to ensure 24/7 coverage.

Solution

Enloe already had Cortex XDR and other Palo Alto Networks products, and Unit 42 MDR leverages those investments while offering round-the-clock coverage. Since the beginning of the engagement, Enloe has benefited from proactive notification of emerging threats and best-in-class SecOps, threat intelligence, and expert incident response.

READ FULL STORY

Story 9
SOC Modernization

Client
Enloe Medical Center

Industry
Healthcare

Products and Services

- Unit 42 Managed Detection and Response
- Unit 42 Retainer
- Cortex XDR

> **“Our experience with Unit 42 has been absolutely phenomenal... Not only did we get detection and response services, which are reactive, we got Managed Threat Hunting, which is proactive.”**
>
> – Jordan Sledge
> Cybersecurity Manager
> Enloe Medical Center

Go from reactive to proactive cybersecurity with support from the best in the business

We believe no organization should face advanced cyberthreats alone. Unit 42 strengthens your team with the tools and expertise needed to stay ahead of threats and protect your business. With our proven strategies and insights from thousands of engagements, we'll help your team handle the toughest situations with confidence.

To see how our specialists can help you stay ahead, **contact Unit 42**.

paloalto® NETWORKS | UNIT 42®

Under attack? Get in touch.

North America: Toll Free:	**+1.866.486.4842 (866.4.UNIT42)**
UK:	**+44.20.3743.3660**
Europe and Middle East:	**+31.20.299.3130**
Asia:	**+65.6983.8730**
Japan:	**+81.50.1790.0200**
Australia:	**+61.2.4062.7950**

start.paloaltonetworks.com/contact-unit42