Unit 42 Business Email Compromise Readiness Assessment

Defend Against Email-Based Threats

Unauthorized access to email leading to financial fraud—or business email compromise (BEC)—is one of the most prevalent cyberattacks organizations face today.

The threat continues to grow. The broad adoption of SaaS-based email platforms, such as Gmail and Microsoft 365, creates a target-rich environment for threat actors who use phishing and stolen or reused credentials to gain access to internet-accessible accounts.

The FBI Internet Crime Complaint Center (IC3) estimates that in the aggregate, BEC attacks cost organizations three times more than any other cybercrime.[1]

The Unit 42 BEC Readiness Assessment addresses this challenge. We deliver a targeted cybersecurity risk assessment focused on controls and the people, processes, and technologies necessary to defend against BEC and other email-based attacks. We work with you to identify email control enhancements, remediation recommendations, and create a response playbook based on threat intelligence and best practices to prevent and better respond to email-based threats, helping you:

- Prevent and detect attacks with email-specific safeguards.
- Recover faster with a best practice response playbook.
- Test your readiness with BEC Tabletop Exercises and Red Teaming.
- Put our IR team on speed dial with SLA-driven response times.

Benefits of the BEC Assessment

- Harden your enterprise email system to prevent unauthorized access.
- Improve your response to BEC attacks.
- Lower the likelihood and impact of email-based attacks.

1. *2020 Internet Crime Report*, Federal Bureau of Investigation, March 16, 2021.

BEC Incidents Represent Nearly a Third of the Incidents Investigated by the Unit 42 Incident Response Team in 2022

The Unit 42 BEC Readiness Assessment comes in three tiers designed to match your organization's needs.

Tier 1: BEC Readiness Assessment

Security Configuration Assessment

- **Outcomes:** Improve your organization's ability to prevent BEC and other email-based attacks.
- **Services**: We perform an in-depth technical review of the security configuration of your email environment, leveraging multiple hardening standards and battle-tested best practices.
- **Deliverables:** We'll provide a report of control enhancements and recommendations for your organization to better prevent BEC and other email-based attacks.

BEC Tabletop Exercise

- **Outcomes:** Improve your organization's ability to quickly and effectively respond to a BEC attack.
- **Services:** We'll design and facilitate a BEC attack Tabletop IR Exercise based on the thousands of investigations our IR team has performed to test your readiness with a simulated attack as well as to help you practice IR processes and workflows.
- **Deliverables:** We'll provide an after-action report with recommendations for policy and process improvement.

Unit 42 Retainer with 250 Credits for Incident Response

- **Outcomes:** Extend your IR team's capabilities by putting the world-class Unit 42 IR team on speed dial with SLA-driven response times. Improve recovery times and the efficacy of IR.
- **Services:** Your retainer hours are valid for one year and can be used for IR services or proactive cybersecurity advisory services as needed.
- **Deliverables:** What we provide will vary depending on the service request.

Tier 2: Email Compromise Assessment (Includes everything in Tier 1)

Email Compromise Assessment

Drawing on our deep expertise in responding to BEC and other email-based attacks, the Unit 42 Email Compromise Assessment identifies evidence of historical or ongoing compromise in your email environment. Unit 42 IR experts analyze account logs and telemetry to search for unauthorized access, including rule creation and data exfiltration:

- **Outcomes:** Gain visibility into suspicious email account activity and take action to secure your email environment.
- **Services**: Unit 42 IR experts analyze account data to identify IoCs and hidden threats.
- **Deliverables:** You'll get a report with findings and recommendations for control enhancements based on empirical observations, configuration settings, and opportunities to reduce your attack surface.

Email Attack Readiness Benchmark

- **Outcomes:** Identify gaps in your defenses before the threat actors do and increase security awareness.
- **Services:** The Unit 42 Offensive Security team launches a targeted spear phishing attack against high-value targets in your organization.
- **Deliverables:** Report of results and recommendations for control enhancements.

BEC Incident Response Playbook

- **Outcomes:** Improve your ability to respond to and recover from email-based attacks.
- **Services:** The Unit 42 Security Consulting team reviews your existing IR processes and recommends a best practice playbook based on your specific environment and capabilities, including our extensive experience responding to email-based threats.
- **Deliverables:** Tailored BEC incident response playbook.

Tier 3: Purple Team and Cyber Awareness Enhancement (Includes everything in Tiers 1 & 2)

Email Attack Purple Team Exercises

- **Outcomes:** Increase security awareness. Validate and improve your defenses against advanced email attacks.
- **Services**: The Unit 42 Offensive Security team targets your email accounts and conducts a custom-designed campaign of advanced email-based attacks, including credential theft, phishing, and other advanced attack methods.
- **Deliverables:** Receive reports of the results of each simulated attack and training and control enhancement recommendations.

Cyber Awareness Training Enhancement

- **Outcomes:** A cyberaware workforce, informed of today's advanced threats and their role in preventing cyberattacks.
- **Services:** We deliver cyberawareness training tied to the outcomes of your Purple Team Exercise and tailored to your industry vertical, sensitive information assets, and key functional roles throughout the organization.
- **Deliverables:** Get a live training session via webinar.

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:

- Fill out the form at start.paloaltonetworks.com/contact-unit42.html.
- 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.
- Email **unit42-investigations@paloaltonetworks.com**.

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. Visit paloaltonetworks.com/unit42.

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

© 2023 Palo Alto Networks, Inc. Palo Alto Networks and the Palo Alto Networks logo are registered trademarks of Palo Alto Networks, Inc. A list of our trademarks can be found at https://www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.
unit42_sb_business-email-compromise_080223