# Die Threat Intelligence und Incident-Response-Services von Unit 42

Datenbasiert, reaktionsbereit.

## Konkurrenzlose Erfahrung

Wir kennen Ihre Herausforderungen – ob es die Reaktion auf einen Sicherheitsvorfall ist oder der Schutz vor Cyberrisiken. Die Experten von Unit 42 stammen aus US-amerikanischen Regierungs- und Strafverfolgungsbehörden sowie globalen Sicherheitsunternehmen und waren bei der Abwehr einiger der bedeutendsten Datenschutzverletzungen im Einsatz. Unser Response-Team ist extrem gefragt und reagiert auf mehr als 1.300 Sicherheitsvorfälle pro Jahr. Diese beispiellose Erfahrung fließt in unsere Risikomanagementlösungen ein und wir legen den Fokus unserer Bewertungen sowie unsere Empfehlungspriorisierung auf Angriffsvektoren, die wir tagtäglich in Unternehmen beobachten. Unsere Teams haben bereits Tausende Cyberrisiken bewertet und arbeiten mit Unternehmen in aller Welt zusammen, um Cyberbedrohungen zu identifizieren und abzuwehren.

## Schnell und effizient

Im Ernstfall eilen wir unseren Kunden umgehend zu Hilfe, um ihnen bei der Analyse akuter Bedrohungen und der Implementierung wirksamer Abwehrmaßnahmen unter die Arme zu greifen. Dabei erweist es sich als großer Vorteil, dass unser Incident-Response-Team aus forensischen Beratern, Malwareanalysten, erfahrenen Einsatzleitern und anderen Spezialisten in Minutenschnelle startklar ist. Wir handeln schnell, um Bedrohungen einzudämmen, zu untersuchen und unsere Abwehrmaßnahmen zu koordinieren. Wir arbeiten mit Ihnen zusammen, um die Sachlage zu ermitteln und kritische Entscheidungen für die Wiederaufnahme Ihrer Geschäftsprozesse zu treffen. Bei unseren Risikomanagementeinsätzen sind wir uns bewusst, dass Cybersicherheitsausgaben eine Investition sind und eruieren sorgfältig, auf was sich die Budgets unserer Kunden konzentrieren sollten. So können Sie den größten Mehrwert bezüglich des Risikomanagements aus Ihrer Investition schöpfen. Wir stellen Lösungen zeitnah, budgetkonform und mit Blick auf die erwünschte Wirkung bereit.

## Kontinuierliche Innovation und ausgereifte Technologien

Um der sich schnell entwickelnden Bedrohungslandschaft immer einen Schritt voraus zu sein, bedarf es der besten Technologien und konstanter Innovation. Unsere Recherchen, Entwicklungen und die Kreativität, mit denen wir den Cybersicherheitsherausforderungen unserer Kunden begegnen, sind für uns ein Aushängeschild. Palo Alto Networks hat ein leistungsstarkes Portfolio an technologiegestützten Lösungen für die Bedrohungsprävention und -erkennung sowie für Incident Response aufgebaut und entwickelt dies stetig weiter. Wir integrieren cloudnatives Computing und KI für maschinelles Lernen, damit unsere Teams global und unternehmensweit innerhalb von wenigen Minuten reagieren können – statt über Tage oder Wochen. Dank unserer Produkte kann Unit 42 schneller reagieren, intelligenter nach Bedrohungen suchen, Untersuchungen vertiefen und Bedrohungen komplett eindämmen.

Weitere Informationen finden Sie unter www.paloaltonetworks.com/unit42

**15**
Jahre Erfahrung (durchschnittlich)

**>1.000**
Einsätze in 2021

**Rund um die Uhr**
verfügbar für Incident Response

# Die Threat Intelligence und Incident-Response-Services von Unit 42

## Incident Response

### Incident Response

**BEC-Untersuchungen**
Reagieren Sie auf nicht autorisierten Zugriff auf Ihre geschäftliche E-Mail-Umgebung. Dämmen Sie den Vorfall ein, bestimmen Sie die Ursache, die Verweildauer der Angreifer sowie ihre Aktivitäten und identifizieren Sie die betroffenen Datenbestände.

**Ransomware-Untersuchungen**
Wir helfen Ihnen während und nach einem Ransomwareangriff. Dämmen Sie die Bedrohung ein, bestimmen Sie die Ursache, die Verweildauer der Angreifer sowie ihre Aktivitäten und identifizieren Sie die betroffenen Datenbestände. Außerdem unterstützen wir Sie auf Wunsch bei Verhandlungen mit den Erpressern, validieren Entschlüsselungsschlüssel und entwickeln und implementieren einen Plan für die Wiederherstellung des Normalbetriebs.

**Bedrohungsabwehr in Cloud-Umgebungen**
Wir helfen Ihnen während und nach einem cloudbasierten Angriff. Dämmen Sie den Vorfall ein. Bestimmen Sie den ersten Angriffsvektor, den Umfang des nicht autorisierten Zugriffs und der Datenausschleusung sowie die betroffenen Systeme für die Behebungsmaßnahmen. Identifizieren und implementieren Sie zusätzliche Sicherheitskontrollen.

**Web-App-Bedrohungen**
Wir helfen Ihnen während und nach einem webbasierten Angriff. Dämmen Sie die Bedrohung ein, analysieren Sie Logs und Code, beziffern Sie den Umfang des Vorfalls oder der gestohlenen sensiblen Daten und erhalten Sie Empfehlungen zum Aufbau präventiver Gegenmaßnahmen.

**Advanced Persistent Threat (APT)-Untersuchungen**
Wir helfen Ihnen während und nach einem mutmaßlichen APT-Angriff. Dämmen Sie die Bedrohung ein, bestimmen Sie die Ursache, die Verweildauer der Angreifer sowie ihre Aktivitäten und identifizieren Sie die betroffenen Datenbestände.

**PCI-Untersuchungen**
Wir helfen Ihnen während und nach einem Kreditkartendatenleck. Finden Sie sich im PFI-Prozess zurecht. Dämmen Sie die Bedrohung ein, bestimmen Sie die Ursache, die Verweildauer der Angreifer sowie ihre Aktivitäten und identifizieren Sie die betroffenen Zahlungskartendaten (Payment Card Information, PCI).

**Malwareanalysen**
Erhalten Sie Analysen zu Malwaresamples mit Open-Source-Bedrohungsdaten, Sandboxing, Reverse Engineering und Berichterstellung zum Verhalten und der Funktionalität der Malware.

**Data Mining**
Identifizieren und beziffern Sie sensible Daten, die aufgrund eines Datenlecks gefährdet sind, um Benachrichtigungsentscheidungen zu treffen, darunter PHI-, PII-, PCI- und andere sensible oder gesetzlichen Vorgaben unterliegenden Informationen.

## Cyberrisikomanagement

### Strategische Beratung

**Beratungsservices für Vorstände und CISOs**
Sie erhalten eine Einschätzung und Bewertung des Cyberrisikos sowie ein aktuelles Statusprofil und Unterstützung bei der Erarbeitung einer Sicherheitsstrategie, die Sie mit Ihren Führungskräften und dem Vorstand teilen können.

**Cybersicherheit bei Fusionen und Übernahmen**
Prüfen Sie Benutzer, Prozesse und Technologien, um potenzielle Warnsignale zu identifizieren, decken Sie verborgene Cybersicherheitsrisiken auf und profitieren Sie von einer unabhängigen Einschätzung des Reifegrads Ihrer Informationssicherheit im Zusammenhang mit einer Unternehmensfusion oder -übernahme.

**Einschätzung von Cybersicherheitsrisiken**
Eine auf Frameworks oder gesetzlichen Vorschriften wie NIST, CIS, ISO, CCPA oder HIPAA basierte Cybersicherheitseinschätzung bestimmt den aktuellen Stand der Kontrollfunktionen sowie bestehender Lücken und erarbeitet einen strategischen Plan für ein verbessertes Programm zur Informationssicherheit.

### Proaktive Einschätzungen

**Bedrohungseinschätzung**
Suchen Sie nach historischen oder aktuellen Gefahrenindikatoren, um Beweismaterial für nicht autorisierte Zugriffe oder Aktivitäten in Cloud-, E-Mail- oder Endpunktumgebungen zu sammeln.

**Bewertung des Security Operations Center (SOC)**
Nutzen Sie Beratungsservices für das Design und die Struktur eines Next-Gen SOC.

**Einschätzung der Cloud-Sicherheit**
Bewerten Sie aktuelle Kontrollen für Cloud-Computing oder Service-Workloads sowie Sicherheitskonfigurationen und Richtlinien zur Identifizierung von Cybersicherheitsrisiken.

**Risikobewertung für Lieferketten**
Sie erhalten Bewertungen und Einschätzungen von anbieterbasierten Cybersicherheitsrisiken für Lieferketten, um Angriffe auf Lieferketten zu identifizieren und abzuwehren.

**Bewertung der Resilienz gegen BEC-Angriffe**
Zielgerichtete Cyberrisikoeinschätzungen, die sich auf Kontrollen und Benutzer, Prozesse und Technologien stützen, sind für die Abwehr von BEC- und anderen E-Mail-basierten Angriffen notwendig.

**Einschätzung der Ransomwarebereitschaft**
Profitieren Sie von verbesserten Kontrollen, Behebungsempfehlungen und einem Playbook mit Best Practices für Resilienz bezüglich Ransomwareangriffen.

### Vorfallssimulationen

**Planübung**
Simulieren Sie anhand von maßgeschneiderten Szenarien, die auf branchenspezifischen Bedrohungen und Vorfällen aus der Praxis basieren, mit Stakeholdern Ihre Reaktion auf schwerwiegende Datensicherheitsvorfälle.

**Purple Teams**
Gemeinsam mit Unit 42 verbessern Sie Ihr Sicherheitsprogramm und können Sicherheitslücken identifizieren, Ihre Schutzmaßnahmen abstimmen und die Sicherheitsprozesse optimieren.

**Penetrationstests**
Prüfen Sie die Belastbarkeit Ihrer technischen Schutzmechanismen und die Cybersicherheit Ihres Unternehmens durch die Anwendung jener Taktiken, Techniken und Prozesse (TTPs), die von echten Hackern genutzt werden, um unbefugt in Systeme einzudringen und in kompromittierten Umgebungen Fuß zu fassen.

## Die Threat Intelligence und Incident-Response-Services von Unit 42 (weitergeführt)

### Incident Response

#### Digitale Forensik

**Digitale Untersuchungen**

Forensische Datenerfassung, Analysen, Wiederherstellung und Berichte zu Informationen, die mit wissenschaftlichen Methoden aus digitalen Medien erfasst wurden, helfen Ihnen, zu identifizieren, was passiert ist und was dabei genutzt wurde.

**Untersuchungen zu Insiderbedrohungen und ausscheidenden Mitarbeitern**

Untersuchen Sie Missbrauch privilegierter Zugriffsrechte durch anderweitig vertrauenswürdige Benutzer und stellen Sie fest, auf welche Daten zugegriffen wurde, welche unterschlagen wurden und/oder welche ungewünschten Aktivitäten ausgeführt wurden.

**Strukturierte Datenuntersuchungen**

Sie erhalten Zugang zu Sammlungen und Analysen von SQL- und NoSQL-Datenbankumgebungen, darunter interne Logs.

**Expertenzeugen/Aussagen/Unterstützung bei Rechtsstreitigkeiten**

Überprüfen Sie digitale Beweise und ihre Erfassungsmethoden und bieten Sie fachkundige Einschätzungen zu Fakten in Berichten, Deklarationen, eidesstaatlichen Aussagen oder öffentlichen Anhörungen.

### Cyberrisikomanagement

**Sicherheitslageprüfungen**

Prüfen Sie Benutzer, Prozesse und Technologien, die für eine effektive Reaktion auf Bedrohungen notwendig sind, und erstellen Sie eine strategische Roadmap zur Stärkung Ihres Sicherheitsstatus.

#### Beratungsservices und Threat Intelligence

**Erstellen eines Sicherheitsprogramms**

Erstellen Sie Governance-Frameworks, Betriebsmodelle und eine Roadmap für Ihre Informationssicherheit, darunter Richtlinien und Standards, ein Kontrollrahmen und eine Defese-in-Depth-Strategie.

**Virtuelle/r CISO**

Hierbei handelt es sich um einen vorübergehenden oder Teilzeit-CISO, mit dessen Hilfe Sie Cyberrisiken identifizieren und Ihr Programm für die Informationssicherheit ausreifen können. Der virtuelle CISO erstellt eine Cybersicherheitsstrategie und arbeitet gemeinsam mit Ihren IT- und Sicherheitsteams sowie der Führungsriege zusammen, um alle Aspekte des unternehmensweiten Sicherheitsniveaus abzuklären.

**Entwicklung von Incident-Response-Plänen**

Dieser Bewertungs- und Beratungsservice bezieht sich auf die Bereitschaft Ihres Teams zur Prävention, Erkennung und Abwehr von Ransomwareangriffen sowie der nachfolgenden Systemwiederherstellung.

**Bedrohungsbeschreibung durch Experten**

Diese strategische Bedrohungsbeschreibung bietet Ihnen eine anpassbare Ansicht der Bedrohungslandschaft von Unit 42 sowie Zugriff auf eine Vielzahl an Daten aus Endpunkten, Netzwerken und der Cloud.

## Vereinbarung mit Unit 42

Ist Ihr Unternehmen auf die Abwehr schwerwiegender Cybersicherheitsvorfälle vorbereitet? Die Geschwindigkeit Ihrer Reaktion wie auch die Effektivität Ihrer Tools und Playbooks wirken sich letztendlich auch darauf aus, wie schnell Sie sich von Vorfällen erholen. Erweitern Sie die Fähigkeiten Ihres Teams mit den erstklassigen Incident-Response- und Cyberrisikomanagement-Teams von Unit 42.

Unit 42 führt jedes Jahr über 1.000 Incident-Response-Untersuchungen durch – von Fällen mit böswilligen Insidern zu Aktivitäten von organisierten kriminellen Kartellen und staatlich gesteuerten Bedrohungen. Die Vereinbarung mit Unit 42 bietet Ihnen detaillierte Forensik und Incident-Response-Erfahrung mit vordefinierten SLAs (Service-Level Agreements), wenn Sie sie am dringendsten benötigen.

Sie können unsere Angebote während der Vertragsdauer auch für die proaktiven Cyberrisikomanagement-Services von Unit 42 nutzen. Unsere fachkundigen Berater unterstützen Ihr Team bei der Erstellung von Sicherheitsstrategien und der Bewertung Ihrer Sicherheitsmaßnahmen sowie des Reifegrads Ihres gesamten Sicherheitsprogramms.

## Über Unit 42

Die datengestützte, abwehrbereite Unit 42 von Palo Alto Networks besteht aus weltbekannten Bedrohungsforschern, Incident-Response-Experten und Sicherheitsberatern, die eine Leidenschaft dafür haben, Kunden bei einer proaktiveren Bekämpfung von Cyberrisiken zu unterstützen. Die Teams der Unit 42 sind bereits für ihre branchenführenden Threat-Intelligence-Leistungen bekannt und haben ihr Angebot um modernste Incident-Response-Services und Leistungen im Bereich Cybersicherheitsmanagement ausgeweitet. Unsere Experten beraten Sie fachkundig, bewerten und testen die Resistenz Ihrer Sicherheitssysteme gegen relevante Bedrohungen, unterstützen Sie bei der Entwicklung einer bedrohungsbasierten Sicherheitsstrategie und helfen Ihnen, Vorfälle in Rekordzeit einzudämmen. Besuchen Sie unsere Website unter: paloaltonetworks.com/unit42.

### Von Cybersicherheitsversicherungen anerkannt

Unit 42 steht bei mehr als 70 großen Cybersicherheitsversicherungen auf der Liste genehmigter Anbieter. Falls Sie die Services von Unit 42 in Zusammenhang mit einer Cyberversicherungsforderung nutzen müssen, kann Unit 42 auf die geltenden bevorzugten Preise des Versicherungsanbieter Rücksicht nehmen. Damit diese Preise gelten, müssen Sie Unit 42 nur bei Ihrer Service-Anfrage darüber informieren.

### Sie werden angegriffen?

Wenn Sie vermuten, Opfer eines Angriffs geworden zu sein, oder eine dringende Frage haben, kontaktieren Sie das Unit 42 Incident-Response-Team unter start.paloaltonetworks.com/contact-unit42.html. Sie können uns auch unter einer der folgenden Telefonnummern erreichen: Nordamerika: +1 866 486 4842 (866.4.UNIT42), EMEA: +31 20 299 3130, Vereinigtes Königreich: +44 20 3743 3660, APAC: +65 6983 8730, oder Japan: +81 50 1790 0200.

Oval Tower, De Entrée 99–197
1101 HE Amsterdam, Niederlande

Telefon: +31 20 888 1883
Vertrieb: +800 7239771
Support: +31 20 808 4600

www.paloaltonetworks.de


unit42_ds_threat-intel-incident-response-services_042122