Cyberdefense

Managed Cybercrime Monitoring

Erweiterung von Managed Detection and Response über die Unternehmensgrenzen hinaus.

Der Schutz Ihrer Marke und Ihres geistigen Eigentums in der digitalen Welt hat höchste Priorität.

Cyberkriminalität ist ein florierendes Geschäft und verursachte im Jahr 2021 weltweit Schäden in Höhe von 6 Billionen US-Dollar. Markenmissbrauch durch böswillige Akteure hat in der digitalen Welt epidemische Ausmaße angenommen, zerstört den Ruf von Unternehmen und beeinträchtigt ihre Gewinne. Die Auswirkungen reichen von rechtlichen Klagen und regulatorischen Bußgeldern bis hin zu einem Vertrauensverlust bei Kunden. Die von Angreifern eingesetzten Techniken entwickeln sich genauso schnell wie die Bedrohungslandschaft selbst. Die meisten Bedrohungen gehen von organisierten und hochentwickelten Netzwerken von Cyberkriminellen mit globaler Reichweite aus.

Zusätzlich zu diesen Bedrohungen entsteht weiteres digitales Risiko durch die versehentliche Verbreitung von Informationen im Internet, sei es durch die Nutzung von Cloud-Datenfreigabe-Apps, den leichtfertigen Einsatz von Code-Repositories wie GitHub durch Entwicklergemeinschaften oder durch Fehler von Mitarbeitern oder Dritten bei der Veröffentlichung von Daten.

Die Managed Cybercrime Monitoring Services von Orange Cyberdefense erweitern die Erkennungs- und Reaktionsfähigkeiten über die Grenzen Ihres Unternehmens hinaus. Sie überwachen kontinuierlich das Internet, das Deep und Dark Web auf digitalen Betrug, Markenausbeutung und Datenlecks.

Durch die Bekämpfung von Cyberkriminalität über verschiedene Angriffsflächen und Anwendungsfälle hinweg ermöglicht Orange Cyberdefense es Ihnen, digitales Risikomanagement als Geschäftsfunktion zu etablieren – ohne die sonst üblichen hohen Kosten.

Dieser Service ist außerdem ein integrierter Bestandteil unseres umfassenderen Managed Detection and Response (MDR)-Angebots. Dadurch wird dieser wichtige Bestandteil der Sicherheitsoperationen nicht länger isoliert betrachtet, sondern erweitert die MDR-Abdeckung über die traditionelle interne Überwachung von Endpunkten, Netzwerken und Logdaten hinaus.

Herausforderungen bei der Überwachung von Aktivitäten von Cyberkriminellen:

Zugang: Der Zugang zu Untergrund-Marktplätzen und Cyberkriminellen-Foren wird zunehmend schwieriger, da diese sich infolge hochkarätiger Strafverfolgungsmaßnahmen immer weiter fragmentieren.

Sprache: Cyberkriminelle sprechen eine andere Sprache, sowohl im wörtlichen als auch im übertragenen Sinne. Die Cyberkriminalitätsgemeinschaft hat ihren eigenen, einzigartigen Ton und ihre eigenen Regeln für die Kommunikation.

Intelligente Datenverarbeitung: Es können enorme Datenmengen gesammelt werden, um ein Unternehmen und dessen digitalen Footprint zu analysieren – jedoch befindet sich darunter auch eine erhebliche Menge an völlig legitimen und für die Überwachung von Cyberkriminalität irrelevanten Inhalten.

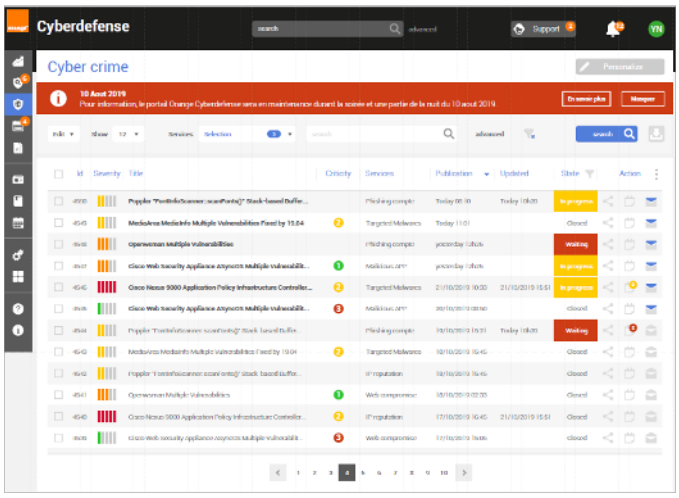
Minderung: Es ist deutlich schwieriger, auf identifizierte externe digitale Risiken zu reagieren, als bei den traditionellen Aktivitäten der Vorfallreaktion in Umgebungen, die unter eigener Kontrolle stehen. Häufig sind Rechtsabteilungen nicht für solche spezialisierten Aufgaben aufgebaut und verfügen auch nicht über die notwendigen Ressourcen.
to act quickly and efficiently.

Erfahren Sie mehr über unseren modularen Ansatz unter:

https://www.orangecyberdefense.com/de/leistungsspektrum/managed-services/threat-and-risk-management/managed-cybercrime-monitoring

Ein modularer Ansatz

Bauen Sie Ihre digitalen Risikomanagementfähigkeiten entsprechend Ihren Bedürfnissen aufLange Zeit war es zu kostspielig, unseren digitalen Footprint und das damit verbundene Risiko abzusichern, selbst mit den Einsparungen, die durch die Auslagerung dieser Aufgabe an einen vertrauenswürdigen MDR-Spezialisten wie Orange Cyberdefense erzielt wurden.Der Managed Cybercrime Monitoring Service kann modular genutzt werden, sodass Sie Ihre Kapazitäten je nach Bedarf aufbauen können – mit der Möglichkeit zur zukünftigen Erweiterung. All dies wird in unserem Threat Defense Center-Portal dargestellt, sodass Sie die Ergebnisse des Services einfach anzeigen, filtern und berichten können. Darüber hinaus haben Sie die Möglichkeit, zusätzliche Assets einzureichen, wenn neue digitale Daten erstellt oder entdeckt werden.



Über das Orange Cyberdefense CERT:

- Unser hauseigenes Computer Emergency Response Team (CERT) wird als das führende private CERT in Europa anerkannt. Es pflegt Beziehungen zu 20 Strafverfolgungsbehörden auf mehreren Kontinenten, darunter das FBI, Interpol und Europol.
- Ein dediziertes Cybercrime Monitoring-Team mit über 20 Intelligence-Analysten an 3 Standorten, die aus spezialisierten Geheimdienstbereichen kommen und über mehr als 16 Jahre Erfahrung in diesem Bereich verfügen.
- Unsere firmeneigenen, verborgenen Web-Crawler und Bots sind darauf spezialisiert, eine enorme Anzahl von Seiten im offenen Internet, dem Deep Web und Dark Web zu analysieren, um potenzielle Bedrohungen für die Marke und IP-Adressen Ihrer Organisation aufzuspüren.
- Dies wird durch eine tiefgehende Qualifizierung durch mehrsprachige Experten ergänzt, die rund um die Uhr an 365 Tagen im Jahr verfügbar sind. Sie überwachen mehr als 10.000 Marken und nehmen jedes Jahr etwa 20.000 betrügerische Webseiten herunter.

Der Lifecycle-Prozess des Managed Cybercrime Monitoring:

Anticipate
- Verstehen der Intelligenzziele
- Verstehen des Geschäftskontexts
- Sammeln der richtigen Asset-Daten

Identify
- Millionen von Quellen durchsucht
- Eigene Tools und Infrastruktur des Orange Cyberdefense CERT
- Best-in-Class DRM-Plattformen

Respond
- Beweise zur Lösung des Vorfalls
- Formalisierung der Empfehlungen und angemessene Eskalation
- Ergreifen von Maßnahmen, (z. B. Domain- oder Inhaltsentfernung)

Detect
- Millionen von Quellen durchsucht
- Eigene Tools und Infrastruktur des Orange Cyberdefense CERT
- Best-in-Class DRM-Plattformen

Mehr Infos finden Sie auf www.orangecyberdefense.de

Orange Cyberdefense
Paul-Gerhardt-Allee 24, 81245 München

info@de.orangecyberdefense.com
+49 89 2000148 00