CROWDSTRIKE

FALCON OVERWATCH – VERWALTETE BEDROHUNGSSUCHE

Verborgene komplexe Bedrohungen erkennen und stoppen

FALCON OVERWATCH – DEM DATENDIEBSTAHL KEINE CHANCE

Falcon OverWatch™ ist ein Service von CrowdStrike für die verwaltete Bedrohungssuche auf der CrowdStrike Falcon®-Plattform. Auf der Suche nach anomalen oder neuartigen Angriffstechniken, die darauf ausgelegt sind, übliche Sicherheitstechnologien zu umgehen, führen Experten rund um die Uhren tiefgehende und kontinuierliche Analysen durch.

Hinter OverWatch steht ein hochkarätiges Team von Spezialisten aus mehreren Disziplinen. Das Team nutzt die enorme Leistungsfähigkeit des CrowdStrike Threat Graph® unter Berücksichtigung der Bedrohungsaufklärung von CrowdStrike. Es sucht kontinuierlich nach ausgefeilten Bedrohungsaktivitäten in Kundenumgebungen, untersucht diese und berät die Ansprechpartner im Unternehmen entsprechend. Dank der umfangreichen Telemetriedaten aus der Cloud und detaillierten Informationen über mehr als 130 Angreifergruppen ist OverWatch in der Lage, auch hochkomplexe Bedrohungen zu erkennen und zu stoppen.

„OverWatch kontaktierte mich vor einer Woche und teilte mir mit, dass das Team Aktivitäten entdeckt habe, die einer bekannten, auf Server-Manipulation spezialisierten Organisation zugeschrieben werden. Dank dieses Hinweises konnten wir der Sache gezielt nachgehen. OverWatch hat sehr schnell reagiert und uns alamiert. So konnten wir verhindern, dass einer unserer Server auf dem Schwarzmarkt an Spammer oder andere böswillige Akteure verkauft wurde."

Mark Sauer
Director of Information Technology, TransPak

VORTEILE IM ÜBERBLICK

Verborgene komplexe Bedrohungen erkennen und stoppen: Das Team von OverWatch sucht unermüdlich nach verdeckten Bedrohungen um diese aufzudecken und zu stoppen. Dies sind die entscheidenden 1 % aus 1 % der Bedrohungen, die normalerweise im Verborgenen bleiben und unentdeckt zu Datendiebstählen führen.

Maximale Effektivität und Effizienz: OverWatch stellt hochqualifizierten Analysten fortschrittlichste Technologien bereit und liefert damit erstklassige Ergebnisse. Die Spezialisten von CrowdStrike nutzen umfangreiche Daten aus der Cloud, individuelle Tools und hochaktuelle Bedrohungsaufklärung, um mit beispielloser Geschwindigkeit und Reichweite Bedrohungen aufzuspüren.

Nahtlose Erweiterung Ihres Teams: Als Kernkomponente der Falcon-Plattform liefert OverWatch Ergebnisse für Unternehmen jeder Größenordnung und arbeitet als nahtlose Erweiterung Ihres eigenen Team. So minimieren Sie Aufwand, Komplexität und Kosten.

FALCON OVERWATCH – VERWALTETE BEDROHUNGSSUCHE

WICHTIGE PRODUKTMERKMALE

EXPERTENWISSEN 24/7

- **Denken wie die Angreifer:** Wer erfolgreich nach Bedrohung suchen will, muss sich in Angreifer hineinversetzen können.
- **Fachübergreifende Kompetenz:** OverWatch beschäftigt Spitzenkräfte mit Erfahrung aus den verschiedensten Bereichen, wie z. B. Behörden, der Strafverfolgung, freien Wirtschaft, Geheimdiensten und der Verteidigung.
- **Verfügbarkeit 24/7/365:** Wenn es zum Ernstfall kommt, ist Zeit ein kritischer Faktor. Ihre Gegner schlafen nicht und halten sich weder an Zeitzonen noch an Ländergrenzen: Gleiches gilt für das Team zur Bedrohungssuche.
- **Kontinuierliche Wachsamkeit:** Die kontinuierliche, proaktive Arbeitsweise von OverWatch liefert Ergebnisse – Minute für Minute und Tag für Tag.
- **Fein abgestimmte Reaktion:** OverWatch identifiziert und reagiert auf Hunderte von potenziellen Datendiebstählen pro Woche. Jede erkannte Bedrohung hilft den Mitgliedern des Teams Kompetenzen und Prozesse zu verfeinern und aufeinander abzustimmen. So bleiben diese stets zielgenau und wirksam.

CLOUD-SKALIERTE SICHERHEITS-TELEMETRIE

- **Werkzeuge für die Bedrohungssuche:** Die Bedrohungssuche verlangt nicht nur erfahrene Experten. Es kommt auch auf die richtigen Werkzeuge an. Eine skalierbare und wirksame Bedrohungssuche setzt den Zugriff auf große Datenmengen und die Fähigkeit voraus, diese Daten in Echtzeit auf Zeichen eines Angriffs zu untersuchen.
- **Sichtbarkeit in Echtzeit:** OverWatch nutzt die Vorteile der Cloud-skalierten Telemetrie des proprietären CrowdStrike Threat Graph und erzielt damit eine umfassende und weitgehende Sichtbarkeit in Echtzeit.
- **Große Datenmengen:** Der Threat Graph verarbeitet jede Woche Billionen von Ereignissen. Dadurch erhält Falcon OverWatch einen umfassenden und globalen Echtzeiteinblick in aktuelle Bedrohungsaktivitäten.

HOCHAKTUELLE BEDROHUNGSINFORMATIONEN

- **Bedrohungskontext:** Nur Bedrohungen, die man verstanden hat, kann man erkennen.
- **CrowdStrike Bedrohungsaufklärung:** Die Bedrohungsaufklärung verschafft OverWatch das detaillierte, stets aktuelle Wissen über die Aktivitäten von mehr als 130 Angreifergruppen.
- **Aktuelle TTP:** Diese intime Kenntnis der neuesten, aktuell eingesetzten TTP (Taktiken, Techniken und Verfahren) gewährleistet die Effektivität und Effizienz von Overwatch bei der Suche nach Bedrohungen.

PERFEKT INTEGRIERTER TEIL DER FALCON-PLATTFORM

- **Ein Team, ein Kampf:** OverWatch agiert als Erweiterung der Falcon-Plattform und Ihres Teams und liefert zeitnahe Informationen zu Bedrohungen über eine singuläre, Cloud-native Konsole.
- **Kontextangereicherte Warnungen:** Die von Analysten von OverWatch versendeten Warnungen enthalten kontextbezogene Details und Erkenntnisse. So sind Unternehmen in der Lage, Bedrohungen schnell zu verstehen und gezielt zu handeln.

ÜBER CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), ein weltweit führendes Unternehmen im Bereich der Cybersicherheit, definiert mit seiner von Grund auf neu konzipierten Endgeräteschutzplattform die Sicherheit im Cloud-Zeitalter neu. Die schlanke Single- Agent-Architektur der CrowdStrike Falcon®-Plattform nutzt Cloud-skalierte Künstliche Intelligenz und sorgt unternehmensweit für Schutz und Transparenz. So werden Angriffe auf Endgeräte sowohl innerhalb als auch außerhalb des Netzwerks verhindert. Mit Hilfe des firmeneigenen CrowdStrike Threat Graph® korreliert CrowdStrike Falcon weltweit und in Echtzeit über 5 Billionen endpunktbezogene Ereignisse pro Woche. Damit ist die CrowdStrike Falcon Plattform eine der weltweit fortschrittlichsten Datenplattformen für Cybersicherheit.

Testen Sie jetzt kostenlos den Virenschutz der neuesten Generation

Erfahren Sie mehr unter **www.crowdstrike.de**

ANGEBOTE VON CROWDSTRIKE FÜR DIE VERWALTETE BEDROHUNGSSUCHE

Falcon OverWatch erkennt und stoppt ausgefeilte Bedrohungen. Anhand der Expertise von Fachleuten und Daten aus der Cloud wird unermüdlich nach Hinweisen auf komplexe Angriffe gesucht, die sonst unentdeckt bleiben können. Es gibt zwei Optionen, um den besonderen Anforderungen Ihrer Organisation gerecht zu werden.

Merkmal	Falcon OverWatch	Falcon OverWatch Elite
Experten verschiedener Disziplinen	X	X
Kontinuierliche Überwachung	X	X
Telemetrie im Cloud-Maßstab	X	X
Aufklärungsgesteuert	X	X
Nahtlose Integration in die Falcon-Plattform	X	X
Kontextangereicherte Warnungen	X	X
E-Mail-Benachrichtigungen	X	X
Eigens zugeordneter Bedrohungs-Analyst		X
Personalisiertes Onboarding		X
Coaching bei Bedrohungssuche und -untersuchung		X
Periodische Checkups der Umgebung		X
Proaktives Abstimmen		X
Individuelle Bedrohungsberichte und -Briefings		X
Handlungsempfehlungen, erweiterte Untersuchungen und Kontextunterstützung		X
Proaktive Closed-Loop-Kommunikation		X