CROWDSTRIKE

CROWDSTRIKE FALCON ENDPOINT DETECTION AND RESPONSE (EDR)

Bedrohungen schnell, automatisch und mit unübertroffener Transparenz erkennen und abwenden

FALCON INSIGHT — EDR LEICHT GEMACHT

Herkömmliche Lösungen für die Endgerätesicherheit sind nicht in der Lage, fortgeschrittene Bedrohungen zu erkennen und zu stoppen. Kurz gesagt: Sie leiden unter blinden Flecken. Im Unterschied dazu macht CrowdStrike® Falcon Insight™ die Endgeräte in Ihrer gesamten Organisation umfassend transparent.

Falcon Insight™ überwacht kontinuierlich alle Endgeräteaktivitäten und analysiert die Daten in Echtzeit. So werden Bedrohungsaktivitäten automatisch identifiziert, sodass fortgeschrittene Bedrohungen erkannt und verhindert werden können. Parallel dazu werden alle Endgeräteaktivitäten zur CrowdStrike Falcon®-Plattform gestreamt, damit Sicherheitsteams die Vorfälle schnell untersuchen, auf Warnungen reagieren und proaktiv nach neuen Bedrohungen suchen können.

FALCON INSIGHT IST DER BRANCHENFÜHRER IN EDR

Spitzenreiter bei Forrester Wave™: Endpoint Detection and Response, 2018

Validiert gegen das MITRE ATT&CK™ Framework zur Verfolgung und Erkennung fortgeschrittener Angriffe in den MITRE National State Emulation Tests 2018

„Best Buy“ des SC Magazine mit fünf Sternen in allen Kategorien, bewertet von SC Labs 2018

Höchste Auszeichnung in allen Anwendungsfällen, die von Gartner 2017 im Bericht über den Vergleich von Technologien zur Endgeräteerkennung und Reaktion bewertet wurden

ENTSCHEIDENDE VORTEILE

- Automatische Erkennung fortgeschrittener Bedrohungen
- Sehr schnelle Untersuchungen mit ausgefeilter Forensik in Echtzeit
- Wirksame Reaktion und Behebung
- Datenbankabfrage in fünf Sekunden
- Ermöglicht die Bedrohungssuche mit Falcon OverWatch™
- Sofortiges Verständnis komplexer Warnmeldungen anhand des MITRE-basierten Erkennungs-Frameworks

WICHTIGE PRODUKT-MERKMALE

UNKOMPLIZIERTE ERKENNUNG UND BEHEBUNG

- **Automatische Erkennung von Angreifer-aktivitäten:** Falcon Insight verwendet Angriffsindikatoren (IOAs), um das Verhalten von Angreifern automatisch zu identifizieren und priorisierte Warnungen zu versenden. Dadurch entfallen zeitaufwendige Recherchen und manuelle Suchvorgänge. Die Datenbank CrowdStrike Threat Graph™ speichert Ereignisdaten und beantwortet Anfragen nach längstens fünf Sekunden – trotz mehrerer Milliarden dokumentierter Ereignisse.
- **Vollständige Angriffe in einem einzigen Fenster entziffern:** Ein leicht verständlicher Prozessbaum informiert Sie vollständig über Angriffsdetails im Kontext und macht Ihre Ermittlungen damit schneller und einfacher.
- **Beschleunigter Ermittlungsablauf:** Der Abgleich der Warnmeldungen mit dem ATT&CK™-Framework von MITRE (Adversarial Tactics, Techniques, and Common Knowledge) macht auch komplexe Ereignisse auf einen Blick verständlich. Das beschleunigt die Auslösung von Warnmeldungen ebenso wie die Priorisierung und Behebung. Die intuitive Benutzeroberfläche unterstützt zudem flexible Suchläufe innerhalb von Sekunden im gesamten Unternehmen.
- **Aussagekräftige Daten im Kontext:** Die Integration der Bedrohungsdaten stellt Ihnen den vollständigen Angriffskontext bereit, einschließlich Zuweisung.
- **Fundierte Entscheidungen:** Gegner werden in Echtzeit gestoppt. So beenden Sie Angriffe, noch bevor Datenschutzverstöße eintreten können. Bereits kompromittierte Systeme können Sie durch entsprechende Maßnahmen isolieren und untersuchen. Sicherheitsspezialisten können in Echtzeit auf die Endpunkte zugreifen, Aktionen im System durchführen und Bedrohungen mit chirurgischer Präzision stoppen.

VOLLSTÄNDIGER EINBLICK IN ECHTZEIT

- **Jede Aktion in Echtzeit beobachten:** Dank der sofortigen Transparenz betrachten Sie alle Aktivitäten so, als würden Sie Ihrem Gegner „über die Schulter sehen".
- **So erfassen Sie wichtige Details für Bedrohungssuche und forensische Ermittlungen:** Der Kernel-Mode-Treiber von Falcon Insight erfasst über 400 Rohereignisse und zugehörige Informationen, die zur Verfolgung von Vorfällen nötig sind.
- **Antworten in Sekundenschnelle:** Die Datenbank CrowdStrike Threat Graph™ speichert Ereignisdaten und beantwortet Anfragen nach längstens fünf Sekunden, trotz mehrerer Milliarden dokumentierter Ereignisse.
- **Bis zu 90 Tage lang abrufbar:** Falcon Insight dokumentiert alle Endpunktaktivitäten im zeitlichen Verlauf, ganz unabhängig davon, ob Ihre Umgebung aus weniger als 100 oder aus mehr als 500.000 Endpunkten besteht.

SOFORTIGE WERTSCHÖPFUNG

- **Zeit, Aufwand und Geld sparen:** Falcon Insight wird von der CrowdStrike Falcon-Plattform in der Cloud bereitgestellt und benötigt keine lokale Verwaltungsinfrastruktur.
- **In Minutenschnelle implementiert:** Der Agent von Falcon wird über die Cloud bereitgestellt. Er kann für bis zu 70.000 Endpunkte an einem einzigen Tag implementiert werden.
- **Sofort einsatzbereit:** Falcon Insight benötigt nach der Installation weder Neustart, Feinabstimmung, Baselining oder komplexe Konfigurationen. Die unübertroffene Erkennung und Sichtbarkeit wird vom ersten Tag an bereitgestellt.
- **Keine Beeinträchtigung der Endpunkte:** Da an den Endpunkten nur ein schlanker Agent zum Einsatz kommt, werden Suchläufe in der Bedrohungsdatenbank ohne jegliche Leistungsbeeinträchtigung der Endpunkte oder des Netzwerks durchgeführt.

„UNBEMERKTE EINBRÜCHE" VERHINDERN UND DATENSCHUTZVERSTÖSSE STOPPEN

Präventionstechnologien sind niemals perfekt. Wenn es Angreifern gelingt, die Abwehrmaßnahmen Ihres Unternehmens zu umgehen, können Einbrüche wochen- oder monatelang unbemerkt bleiben. Da es an Sichtbarkeit und Erkennungstools fehlt, lassen sich die Aktivitäten kaum noch identifizieren. Während dieser Zeit agiert ein Angreifer sehr erfolgreich, während das Unternehmen unbemerkt auf eine mögliche Katastrophe zusteuert. Falcon Insight erkennt und identifiziert Vorfälle, die für bestehende Abwehrsysteme unsichtbar sind, und ermöglicht es Ihnen, schnell darauf zu reagieren.

ÜBER CROWDSTRIKE

CrowdStrike ist der führende Anbieter von cloudbasiertem Endgeräteschutz der nächsten Generation. CrowdStrike hat den Endgeräteschutz revolutioniert. Ein einziger, schlanker Agent vereint Virenschutz (AV) der nächsten Generation mit erstklassiger Endgeräteerkennung und Reaktion (EDR) – unterstützt durch Threat Hunting rund um die Uhr.

Erfahren Sie mehr unter
crowdstrike.com