KUNDENREFERENZ

Industrie

GESUNDHEITSWESEN

Falcon Host **Deployment**

750 ENDGERÄTE

ENTSCHEIDENDE **VORTEILE**

- Erhöhte Sicherheit und besserer Schutz vor bekannten und unbekannten Bedrohungen
- Durchgängige Transparenz in der gesamten Umgebung
- Multiplikation der eigenen personellen Ressourcen durch Falcon Overwatch mit proaktiver Bedrohungssuche rund um die Uhr

Genutzte **Dienste**

- Falcon Host
- Falcon Overwatch

ZUSAMMENFASSUNG

Der schnell wachsende US-amerikanische Gesundheitsdienstleister befürchtete, zur Abwehr der heutigen zielgerichteten Angriffe nicht ausreichend gerüstet zu sein. Das Unternehmen überlegte daher, vom herkömmlichen mehrschichtigen Konzept wegzugehen und zwei geeignete Lösungen für den erweiterten Schutz von sowohl Netzwerk als auch Endgeräten zu suchen. Dabei stieß man auf Falcon Host, die Next-Gen-Lösung für den Schutz von Endgeräten, die vor raffinierten zielgerichteten Angriffen schützt und zeitgleich Einblicke darüber gibt, wer und was die eigene Umgebung bedroht.

Die **Herausforderung**

Der Kunde hatte viel Geld in die Erneuerung seiner Infrastruktur investiert. Als Akteur in einer sensiblen Branche hatte man besonderen Wert auf die Standardisierung und Aktualisierung des Security Stack gelegt.

Der vorhandene Security Stack beruhte auf einem standardmäßigen mehrschichtigen Sicherheitskonzept, das bei "lauten" Angreifern durchaus funktionierte. Sorgen machten allerdings die verdeckten Angreifer und immer komplexer werdenden Angriffstechniken. Darüber hinaus wollte man auch bereits zur Prävention und Erkennung von komplexen gezielten Angriffen mehr Möglichkeiten in der Hand haben.

Daher entschloss man sich zu einem POV-Projekt (Proof of Value) unter Evaluierung von Falcon Host. Im Zuge des Projekts bestätigte sich schnell der Verdacht auf unbekannte Malware und gezielte Angriffe auf die eigene Umgebung. Das Unternehmen wuchs zwar dynamisch, aber war nicht groß genug , ein eigenes Security Operations Center rund um die Uhr zu besetzen. Aus eigener Kraft konnte also keine proaktive Suche nach gegnerischen Aktivitäten erfolgen. Dies wäre allerdings wichtig gewesen, um nicht ständig unter dem Druck zu stehen, entstandene Schäden im Nachhinein beheben zu müssen.

KUNDENREFERENZ

Die Lösung

Falcon Host, Falcon Overwatch

Das Resultat

Mit Falcon Host entdeckte der Kunde umgehend zwei bisher unbekannte Malware-Programme, die in der eigenen Umgebung aktiv waren, ohne dass der vorhandene, branchenübliche Virenschutz dies verhindert hätte. Falcon entdeckte zudem einen gezielten Phishing-Angriff auf mehrere hochrangige Führungskräfte.

Die proaktive Jagd durch das Team von Falcon Overwatch trug wesentlich dazu bei, gegnerische Aktivitäten in der Umgebung zu erkennen, wie z. B. die Verwendung kompromittierter Zugangsdaten. Der Kunde konnte schnell reagieren, indem er den Benutzerzugriff deaktivierte und kompromittierte Endgeräte innerhalb von 15 Minuten nach der Alarmierung aus der Umgebung entfernte.

Das Unternehmen verwirklichte sein Ziele, eine deutlich bessere und umfassendere Transparenz über das Geschehen an den Endgeräten zu gewinnen und die gesamte Angriffskette im Blick zu behalten Eine weitere Verbesserung ist der detaillierte Einblick anhand der Process-Explorer-Funktionen von Falcon Host. Darüber hinaus trägt die Priorisierung von Warnmeldungen dazu bei, die begrenzten Sicherheitsressourcen so zu optimieren, dass das Unternehmen effizienter und effektiver auf Bedrohungen reagieren kann.

CROWDSTRIKE

www.crowdstrike.com | 15440 Laguna Canyon Road, Suite 250, Irvine, CA 92618