Huntress Managed EDR

Entdecken Sie die Leistungsfähigkeit von Process Insights: Endpoint Detection & Response, unterstützt durch das Huntress 24/7 Security Operations Center (SOC)

Verschaffen Sie sich einen tieferen Einblick in die Endpunkte und stoppen Sie Hacker effektiv und nachhaltig

- Entwickelt, um das Rauschen herauszufiltern und nur dann einen Vorfallsbericht zu liefern, wenn eine Bedrohung verifiziert wird oder Massnahmen erforderlich sind.

- Einfach für Nicht-Sicherheitsexperten, da das Team des Huntress Security Operations Centers zusätzlichen Kontext und Anweisungen zur Behebung des Problems oder zur Einleitung geeigneter nächster Schritte liefert.

- Entwickelt für die wichtigsten EDR-Funktionen, die Versicherungsunternehmen benötigen.

- Die kontinuierliche Überwachung von Prozessausführungen und zugehörigen Metadaten macht es Bedrohungen schwerer, sich zu verstecken, wenn sie die Präventivmassnahmen bereits hinter sich gelassen haben.

- Die EDR-Technologie von Huntress sammelt zielgerichtete Prozessdaten von Endpunkten, ohne Ihre vorhandenen Sicherheitstools zu blockieren oder zu behindern.

> “Ich sage anderen Unternehmen immer, dass Huntress mich nachts schlafen lässt, und das ist der Beweis dafür. Process Insights identifizierte einen Angreifer, der sich auf den Einsatz von Malware vorbereitete, und stoppte einen Angriff, der sehr gefährlich gewesen wäre.”
>
> **Dustin Bolander**
> Inhaber | Clear Guidance Partners

Hauptmerkmale

Die Power von „Managed“
Verabschieden Sie sich von Fehlalarmen und riesigen Alarmwarteschlangen. Unsere Sicherheitsexperten untersuchen verdächtiges Verhalten, ordnen Warnmeldungen ein und bringen Hacker zur Strecke - ohne Ihr Team damit zu belasten.

Verbesserte Bedrohungsanalyse
Erfassen Sie die Aktivitäten von Bedrohungsakteuren zwischen dem ersten Zugriff und den letztendlichen Auswirkungen, um ein vollständiges Bild davon zu erhalten, wie Hacker Ihre geschützten Endpunkte angreifen.

Bessere Sichtbarkeit von Endpunkten
Identifizieren Sie aktiv ausgenutzte Systeme - einschließlich der Rückverfolgung der Ursache - mit einer Granularität, die es Hackern extrem schwer macht, sich zu verstecken.

Forensik nahezu in Echtzeit
Im Falle eines Vorfalls führen die SOC-Analysten von Huntress mit Managed EDR nahezu in Echtzeit forensische Untersuchungen durch und suchen nach Bedrohungen in Ihrem geschützten Netzwerk.

Anpassung an das Cybersecurity-Framework
Verstehen Sie Verhaltensweisen und Motive von Bedrohungsakteuren besser, indem Sie bösartige oder verdächtigen Prozessen auf gängige Cybersicherheits-Frameworks anpassen.

Managed EDR in Aktion

1

Sammeln
Der Huntress-Agent erfasst fortlaufend Daten zur Prozessausführung direkt vom Endpunkt, einschliesslich, aber nicht beschränkt auf die Berechtigungsstufe und den Verlauf des Prozesses.

2

Erkennen
Huntress wendet eine individuell abgestimmte Erkennungslogik auf die von unserem Agenten gesammelten Daten an und macht SOC-Analysten auf verdächtige Aktivitäten aufmerksam, die untersucht werden müssen.

3

Analysieren
SOC-Analysten analysieren den kontinuierlichen Datenstrom, um zu bestätigen, dass die Aktivität tatsächlich bösartig ist.

4

Melden
Unser SOC stellt Ihnen einen individuellen Bericht über den Vorfall zur Verfügung, in dem wir unsere Erkenntnisse mitteilen und die nächsten Schritte darlegen. Dieser kann per E-Mail oder über ein Ticket-System zugestellt werden.

5

Abhilfe schaffen
Sie können die empfohlenen automatischen Behebungsschritte ausführen oder detaillierte Anweisungen für zusätzliche Arbeiten erhalten, die durchgeführt werden sollten.

6

Adaptieren
Bedrohungsdaten werden in unsere Plattform eingespeist, um mit der Zeit intelligenter zu werden und bisher unbekannte Bedrohungen noch effektiver zu stoppen.

Starten Sie heute Ihre Testphase!

Der Huntress-Unterschied

Mit unserer leistungsstarken Managed EDR-Funktionalität und den darin enthaltenen Funktionen arbeitet Huntress mit Ihrem IT- und Sicherheitsteam zusammen, um bösartige Bedrohungen auf Ihren Endpunkten zu erkennen, zu isolieren und zu beseitigen, einschliesslich anhaltender Bedrohungen, Antiviren-Umgehung, Ransomware und mehr.

Hartnäckige Bedrohungen
Beseitigen Sie hartnäckige Bedrohungen, die sich auf Windows im Verborgenen halten. Wir überwachen Eindringlinge und wenn wir sie finden, liefern wir Empfehlungen und Anweisungen zur Entfernung.

Verwaltete Antivirenprogramme
Nutzen Sie Ihren Virenschutz mit Microsoft Defender optimal, dieser wird von Huntress für Sie verwaltet. Mit zentraler Verwaltung und Transparenz können Sie Ihre bestehenden Investitionen in Microsoft Defender verstärken und weitere Optionen zur Stärkung Ihres Sicherheitsstapels eröffnen.

Ransomeware-Kanarienvögel
Das frühzeitige Erkennen von Ransomware ist entscheidend. Wie der Kanarienvogel im Kohlebergwerk ermöglicht Huntress eine schnellere und frühere Erkennung potenzieller Ransomware-Vorfälle, damit Sie schneller reagieren und die Verbreitung eindämmen können.

Externe Aufklärung
Heben Sie externe Schwachstellen hervor, um die Perimeter-Verteidigung zu stärken. Huntress verschafft Ihnen Einblick in externe Angriffsflächen, indem es auf potenzielle Gefährdungen durch offene Ports in Verbindung mit Remote-Desktop-Diensten, Schatten-IT und mehr achtet.

24/7 SOC-Abdeckung
Unübertroffenes menschliches Fachwissen in Ihrer Hosentasche. Unser SOC-Team untersucht potenzielle Bedrohungen, analysiert die Vorgehensweise von Hackern, erstellt Berichte über Vorfälle, hilft bei der Beseitigung von Cyber-Bedrohungen und bietet ein Mass an Fachwissen und Support, das reine Software-Lösungen nicht bieten können.

ROCKIT.CH

rockIT
INFORMATIK - DIE EINFACH FUNKTIONIERT