DATENBLATT

Threat Intelligence Services

Optimal ergänzt durch Informationen von unserem Counter Threat Unit™ (CTU) Forschungsteam

Wir liefern unseren Kunden relevante Bedrohungsindikatoren für ihre spezifische Umgebung.

Bedrohungsakteure entwickeln kontinuierlich neue Methoden, um in Ihre Umgebung einzudringen. Haben sie es auf eine bestimmte Organisation abgesehen, führen sie hartnäckige Kampagnen über lange durch, beidenen sie zielgerichtet, erfinderisch und technisch raffiniert. Die Konsequenz: Herkömmliche Erkennungstechnologien und -methoden reichen nicht mehr aus, um die Gefahren durch gezielt agierende Bedrohungsakteure effektiv zu neutralisieren.

Bei SecureWorks spielen Informationen eine essenzielle Rolle für die Abwehr von Angreifern – ganz gleich, ob sie zielgerichtet vorgehen oder breiter gestreute, allgemeinere Angriffstaktiken einsetzen.

Das Counter Threat Unit Forschungsteam von SecureWorks sucht flächendeckend nach relevanten Informationen, analysiert sie und erarbeitet auf ihrer Grundlage sinnvolle, konkret umsetzbare Richtlinien, mit denen Sie manchmal bereits vorbeugende Abwehrmaßnahmen einleiten können, bevor eine Bedrohung Ihre Organisation überhaupt erreicht. Unsere Daten können Sie auf neue globale Bedrohungen aufmerksam machen, die sich auf Ihre Betriebsabläufe und Ihre finanzielle Leistung auswirken, den Verlust von Kundendaten nach sich ziehen und ihren guten Ruf schädigen könnten. Zusätzlich helfen Ihnen die Threat Intelligence Services, Akteure zu identifizieren, die es vielleicht spezifisch auf Ihre Organisation und Ihre Führungskräfte abgesehen haben könnten, und geben Ihnen praxistaugliche Richtlinien an die Hand, um eventuelle Angriffe effektiv abzuwehren.

Erstklassige Informationen zu Cyberbedrohungen als Grundlage unserer Services

Bedrohungsinformationen bilden die Grundlage für alle Aspekte unseres Serviceportfolios. Wir haben einen globalen Überblick über das gesamte Bedrohungsspektrum. Die Daten, die das SecureWorks Counter Threat Unit (CTU) Forschungsteam zusammenstellt, fließen in Signaturen, Richtlinien, Angreifer-Blacklists und Ereigniskorrelationen für Sicherheitsgeräte ein. Über offenes Feedback werden Informationen zu Bedrohungsakteuren und ihren Praktiken aktiv unter unseren Sicherheitsanalysten, Beratern und Vorfallagenten weitergegeben, sodass bei jedem akuten Ereignis detaillierter Kontext verfügbar ist. Das Ergebnis: Unsere Kunden profitieren von präziserem und effektiverem Support in unserem gesamten Serviceportfolio.

Starker Schutz dank detaillierter Informationen

Die SecureWorks Information Security Services greifen aufDaten unseres Counter Threat Unit (CTU) Forschungsteamszurück und helfen Organisationen so, Bedrohungen vorherzusehen,ihre Verteidigungsmaßnahmen proaktiv zu verstärken, kontinuierlichnach Cyberattacken zu scannen, Angriffe zu stoppen und sichschneller von Sicherheitsverstößen zu erholen. SecureWorks schützt bereits Tausende Organisationen weltweit.

Wir kennen die Gefahren, denen Sie sich gegenübersehen

Die CTU erfasst Milliarden Bedrohungsdatenpunkte aus verschiedenen Quellen auf der ganzen Welt. Auf ihrer Grundlage formuliert sie Informationen, die in das SecureWorks Serviceportfolio einfließen:

Erstklassige Informationen zu Cyberbedrohungen, erstklassige Mitarbeiter

Das Counter Threat Unit Forschungsteam besteht aus einigen der renommiertesten Sicherheitsexperten weltweit. Sie blicken auf ein breites Erfahrungsspektrum zurück und waren zuvor in privaten Sicherheitsunternehmen, im Militär sowie in Nachrichtendiensten tätig. Ob Staaten oder Toporganisationen der Cyberkriminalität – unsere Spezialisten verfolgen und analysieren kontinuierlich die Aktivitäten der ressourcenstärksten und technisch höchst entwickelten Bedrohungsakteure und geben Prognosen über ihre Strategien ab.

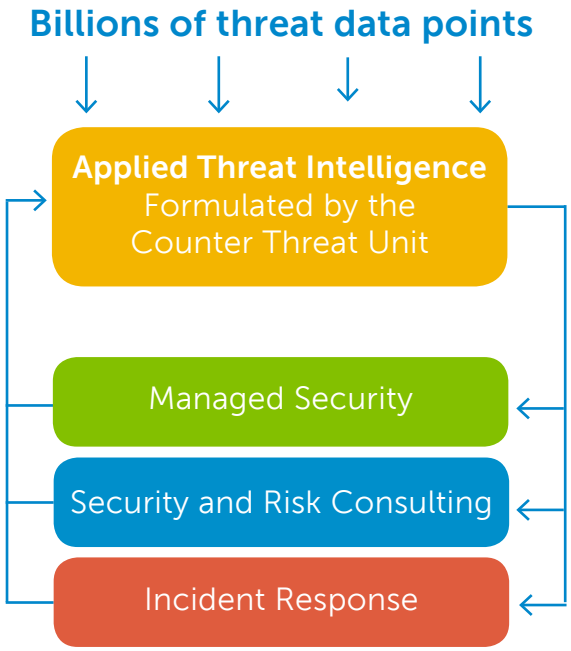
Die CTU Forscher zählen zu den kompetentesten Köpfen der Branche und verfügen über herausragende Fähigkeiten in puncto Malware-Analyse, Reverse-Engineering, Spionageabwehr, Forensik und Untersuchung von Cyberkriminalität.

Regierungsbehörden, Medienhäuser und Großunternehmen wenden sich oft spezifisch an uns, um ihr Know-how für sich zu nutzen.

CTU: Aufgabe und Leistungsprofil

Sinn und Zweck der CTU ist es, die Kunden von SecureWorks zu schützen, Innovationen voranzutreiben und neue Services zu entwickeln. Mit Blick auf dieses Ziel hält das Team seine Kompetenzen und Möglichkeiten in den folgenden Bereichen jederzeit auf höchstem Niveau:

- Entwicklung und Tests von Gegenmaßnahmen
- Beratung und Support
- Wissensaustausch Kontakt mit Strafverfolgungsbehörden, Militär und Nachrichtendiensten
- Malware-Analyse
- Sicherheitsinnovationen
- Erforschung von spezialisierten Bedrohungen
- Bedrohungsinformationen
- Schwachstellenanalyse und-management



Praktisch angewandte Informationen

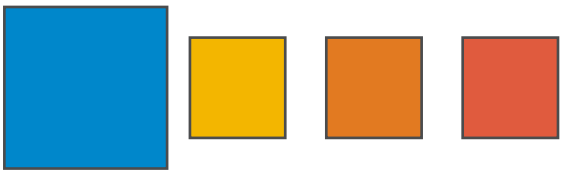
Die Daten der CTU fließen in das gesamte SecureWorks Serviceportfolio ein und ermöglichen unseren Analysten, Beratern und Vorfallagenten so einen tieferen, präziseren Einblick in die Taktiken, Techniken und Verfahren (TTP) der Angreifer.

Dank dieser praktisch angewandten Informationen können wir unsere Services für unsere Kunden schneller, exakter und effektiver erbringen.

Sicherheitsinnovationen und “Big Data”

SecureWorks hat einen globalen Überblick über Tausende von Client-Umgebungen und sonstige Datenquellen. Damit unsere Sicherheitsforscher die großen Volumina der so erfassten Bedrohungsdaten sammeln, analysieren und in unsere Services einfließen lassen können, arbeiten wir ständig an neuen Innovationen und Funktionen. Herzstück unserer Innovationsbemühungen ist die Threat Intelligence Management System (TIMS) Plattform, über die wir Milliarden von Bedrohungsindikatoren und Ereignisdaten zentralisieren, abfragen, analysieren und korrelieren. Die über das TIMS erfassten Daten werden für alle unsere Managed Security Prozesse genutzt und sorgen dafür, dass unsere Analysten, Berater und Vorfallagenten bei ihrer täglichen Arbeitbesser informiert sind.

Status: Guarded



Erweiterte Serviceoptionen

Für Sicherheitsteams, die die Informationserfassung und -verarbeitung in ihrer Organisation weiter stärken wollen, bietet SecureWorks die folgenden Services an:

Global Threat Intelligence

Unter Global Threat Intelligence verstehen wir Informationen zu allgemeinen oder nicht zielgerichteten Bedrohungen. Diese Informationen werden von unseren kompetenten Sicherheitsforschern zusammengestellt, die die Bedrohungsdaten unserer Client-Basis von mehr als 4,100 Managed Security-Clients erfassen und analysieren. Die Daten bieten einen globalen Überblick über neu aufkommende Bedrohungen, neue Taktiken, Techniken und Verfahren (TTP) von Bedrohungsakteuren, bekannte Bedrohungsinfrastrukturen sowie neu identifizierte Schwachstellen und geben unseren Kunden klare, umsetzbare Richtlinien für die Stärkung ihrer Sicherheitsprofile an die Hand.

Malware Analysis and Reverse Engineering

Mit dem Counter Threat Unit Forschungsteam verfügt SecureWorks über unerreichtes Know-how in den Bereichen Malware-Analyse und Reverse-Engineering. Mithilfe von erweiterten Tools und Techniken untersuchen unsere erstklassigen Forscher Malware bis ins Detail, um Funktionsweise, Zweck, Zusammensetzung und Quelle zu identifizieren. Unsere Experten geben Ihnen eine Einschätzung hinsichtlich des potenziellen Schadens, den der Malware-Code in Ihren Netzwerken, Systemen und Datenbeständen anrichten kann, und empfehlen effektive Schritte zur Entfernung des Schädlings.

Targeted Threat Intelligence

Im Rahmen des Targeted Threat Intelligence Service stellen unsere Sicherheitsforscher und Topsicherheitsberater Informationen zusammen, die spezifisch auf die Umgebungen, Organisationen und Führungskräfte unserer Kunden bezogen sind. Die SecureWorks Forscher und Sicherheitsberater sind Spezialisten für die Formulierung sinnvoller Bedrohungsdaten und wissen um jede Finesse in diesem Bereich. Unsere Informationen sind auf die Anforderungen des Kunden zugeschnitten und identifizieren potenzielle Bedrohungen und Bedrohungsakteure, die eine direkte und glaubhafte Gefahr für ihn darstellen. Die Bedrohungsinformationen können beispielsweise auf Daten zu Marke oder Firmenpartnerschaften des Kunden basieren, auf IP- und Domänendaten, den Profilen seiner Führungskräfte oder anderenfür ihn relevanten Parametern.

Für weitere Informationen erreichen Sie unsere SecureWorks Spezialisten unter
info-de@secureworks.com

www.secureworks.de