Kaspersky Threat Hunting Services

www.kaspersky.de
#truecybersecurity

Kaspersky Threat Threat Hunting Services

Sicherheitsteams in allen Branchen arbeiten hart daran, Systeme aufzubauen, die umfassenden Schutz vor sich immer schneller entwickelnden Cyberbedrohungen bieten. Die meisten dieser Systeme nutzen jedoch einen reaktiven Benachrichtigungsansatz bei Vorfällen der Cybersicherheit: Sie warnen erst, nachdem ein Vorfall bereits eingetreten ist. Neueste Forschungen zeigen jedoch, dass ein Großteil der Sicherheitsvorfälle unerkannt bleibt. Diese Bedrohungen bleiben unter dem Radar und sorgen so dafür, dass Unternehmen sich zu Unrecht sicher fühlen. Unternehmen sind sich jedoch zunehmend bewusst, dass Bedrohungen, die zwar unerkannt, aber aktiv in ihren eigenen Infrastrukturen lauern, aktiv gejagt werden müssen. Kaspersky Threat Hunting Services unterstützen Sie bei der Entdeckung hoch entwickelter Bedrohungen in Ihrem Unternehmen. Hierfür setzen hoch qualifizierte und erfahrene Sicherheitsexperten präventive Techniken zur Bedrohungserkennung ein.

Servicevorteile

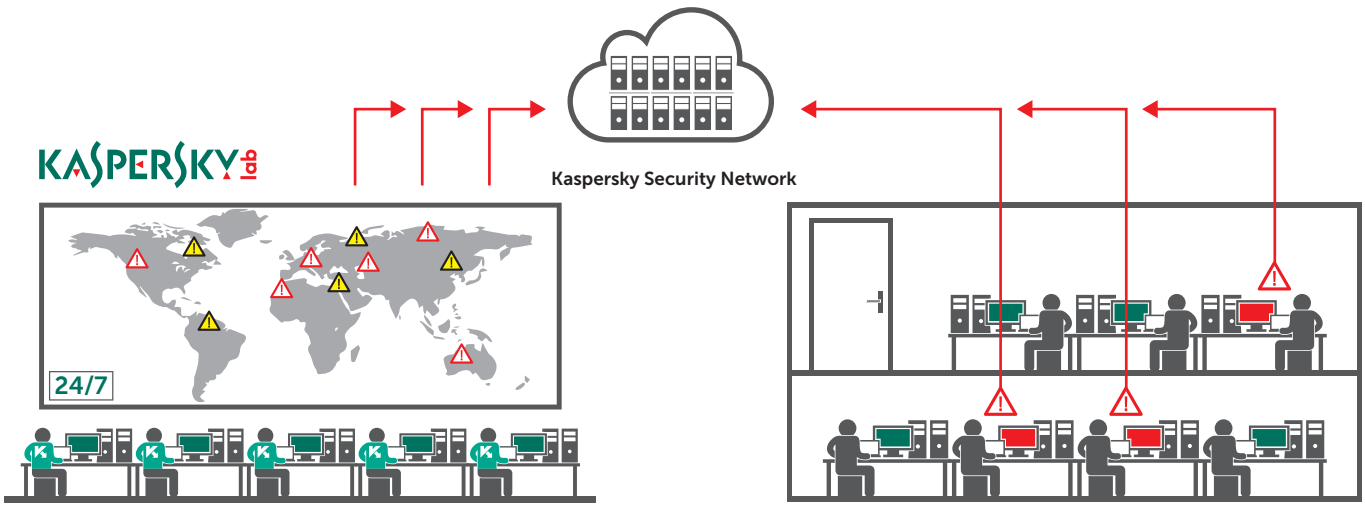
- Schnellere und effektivere Abwehr dank schneller und effizienter Erkennung
- Kein Zeitverlust durch Fehlalarme dank der klaren und umgehenden Identifizierung und Klassifizierung sämtlicher verdächtiger Aktivitäten
- Geringere Gesamtkosten für die Sicherheit. Keine Einstellung und Schulung verschiedener interner Experten
- Die Gewissheit, dass Sie bestens vor den komplexesten und innovativsten Bedrohungen abseits von Malware geschützt sind
- Erkenntnisse zu Angreifern, ihrer Motivation, ihren Methoden und Tools und dem potenziellen Schaden, den sie anrichten können – zur Entwicklung einer fundierten und effektiven Verteidigungsstrategie

Kaspersky Managed Protection

Kaspersky Managed Protection bietet Benutzern von Kaspersky Endpoint Security und Kaspersky Anti Targeted Attack Platform einen vollständig verwalteten Service, der eine einzigartige Kombination aus Technologien zur Erkennung und Vermeidung gezielter Angriffe bietet. Der Service umfasst die Überwachung durch Kaspersky-Experten rund um die Uhr und die kontinuierliche Analyse von Bedrohungsinformationen, um die Echtzeiterkennung bekannter und neuer Kampagnen für Cyberspionage und Cyberkriminalität zu erkennen, die auf wichtige Informationssysteme abzielen.

Service-Highlights

- Dauerhaft hohes Maß an Schutz vor gezielten Angriffen und Malware inklusive Rund-um-die-Uhr-Überwachung und -Support von Ihrem persönlichen Kaspersky-Expertenteam sowie stets aktuelle Bedrohungsinformationen.
- Rechtzeitige und präzise Erkennung von Nicht-Malware-Angriffen, Angriffen mit bisher unbekannten Hilfsmitteln und Angriffen, die Zero-Day-Schwachstellen ausnutzen
- Umgehender Schutz vor sämtlichen unbekannten Bedrohungen durch automatische Updates der Virendatenbank
- Rückwirkende Analyse von Vorfällen und Bedrohungsermittlung, einschließlich der von den Angreifern gegen Ihr Unternehmen eingesetzten Methoden und Technologien
- Integrierter Ansatz – das Kaspersky-Portfolio beinhaltet sämtliche Technologien und Services, die Sie für die Implementierung eines vollständigen Zyklus für den Schutz vor gezielten Angriffen benötigen: Vorbereitung, Erkennung/ Untersuchung, Datenanalyse, automatisierter Schutz



Überwachungscenter

* Für isolierte Infrastruktur – Kaspersky Private Security Network

Der Service im Detail

Die Erkennung gezielter Angriffe von Kaspersky Lab umfasst die folgenden Aktivitäten:

Sammlung und Analyse von Bedrohungsinformationen. Ziel ist es, eine Momentaufnahme Ihrer Angriffsfläche zu erstellen. Dabei werden die Bedrohungen durch Cyberkriminalität und Cyberspionage sowie Angriffe ermittelt, die Ihre Ressourcen aktiv oder potenziell schädigen. Zu diesem Zweck tauchen wir in interne und externe Informationsquellen ein, darunter Untergrund-Communitys von Betrügern, und überwachen Ihre Umgebung mithilfe von internen Überwachungssystemen von Kaspersky Lab. Die Analyse der erfassten Daten ermöglicht uns das Aufspüren von Schwachstellen in Ihrer Infrastruktur, die Cyberkriminelle ausnutzen könnten, sowie von gefährdeten Konten.

Datenerfassung am Standort und frühe Vorfallsreaktion. Neben den Aktivitäten zur Informationsbeschaffung in unseren eigenen Labors kommen Experten von Kaspersky Lab vor Ort, um Netzwerk- und Systemartefakte sowie verfügbare SIEM-Informationen zu erfassen. Wir führen ggf. auch ein Vulnerability Assessment durch, um die kritischsten Sicherheitslücken zu erkennen, und sofort darauf zu reagieren. Hat ein Vorfall bereits stattgefunden, sammeln wir Beweise für weitere Untersuchungen. In diesem Stadium geben wir Ihnen vorläufige Empfehlungen für kurzfristige Abhilfemaßnahmen an die Hand.

Datenanalyse. Zurück im Labor werden die erfassten Netzwerk- und Systemartefakte mithilfe der Wissensdatenbank von Kaspersky Lab analysiert, die IOCs, C&C-Blacklists (Command-and-Control-Serveradressen), Sandboxing-Technologien usw. enthält, um genau zu verstehen, was in Ihrem System passiert. Wird in diesem Stadium zum Beispiel eine neue Malware gefunden, stehen wir Ihnen mit Rat und Tat sowie Tools (z. B. YARA-Tools) zur Seite, um sie sofort zu identifizieren. Wir halten Sie stets auf dem Laufenden und greifen bei Bedarf per Fernzugriff auf Ihre Systeme zu.

Berichterstellung. Abschließend erstellen wir unseren formellen Bericht, der die erkannten gezielten Angriffe sowie unsere Empfehlungen für weitere Abhilfemaßnahmen enthält.

Targeted Attack Discovery

Kaspersky-Experten bieten den Targeted Attack Discovery-Service an, um die Sicherheit Ihrer Betriebsvermögen zu gewährleisten.

Mithilfe der Ergebnisse der Targeted Attack Discovery können Sie aktuelle Aktivitäten rund um Cyberkriminalität und -spionage identifizieren, die Gründe für den Angriff sowie die Quellen der Vorfälle verstehen und effektiv Gegenmaßnahmen planen, die Sie künftig vor ähnlichen Angriffen schützen. Wenn Sie befürchten, dass Angriffe auf Ihre Branche abzielen, und Ihnen verdächtiges Verhalten in Ihren eigenen Systemen auffällt, oder wenn Sie proaktiv vorbeugen wollen ist unser Service „Targeted Attack Discovery" genau das Richtige für Sie, denn sie klärt Sie über Folgendes auf:

- Ob, wie und von wem Sie derzeit angegriffen werden
- Wie sich dieser Angriff auf Ihre Systeme auswirkt, und wie Sie sich wehren können
- Wie Sie zukünftige Angriffe vermeiden

Beschreibung des Service

Unsere global anerkannten, unabhängigen Experten decken aktive Vorfälle, anhaltende Bedrohungen (Advanced Persistent Threats, APT), Aktivitäten der Cyberspionage und Cyberkriminalität in Ihrem Netzwerk auf und analysieren diese. Unsere Experten unterstützen Sie dabei, schädliche Aktivitäten aufzudecken, die möglichen Quellen zu erkennen und die effektivsten Beseitigungsmaßnahmen zu planen.

Dies erfolgt auf folgende Weise:

- Analysieren von Quellen für Bedrohungsinformationen zur Erfassung Ihrer speziellen Gefährdungslage
- Durchführen umfassender Scans Ihrer IT-Infrastruktur und Daten (z. B. Protokolldateien) zur Aufdeckung von Gefährdungsanzeichen
- Analyse aktueller Netzwerkverbindungen zur Erkennung verdächtiger Aktivitäten
- Aufdecken möglicher Angriffsquellen und anderer potenziell gefährdeter Systeme

Die Ergebnisse

Sie erhalten die Ergebnisse in Form eines detaillierten Berichts mit folgenden Angaben:

Unsere allgemeinen Feststellungen: Bestätigung der Existenz oder Abwesenheit von Gefährdungshinweisen in Ihrem Netzwerk

Tief greifende Analyse der erfassten Bedrohungsinformationen und der gefundenen Gefährdungsindikatoren

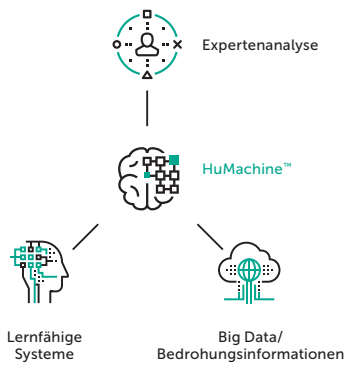
Genaue Beschreibung der ausgenutzten Schwachstellen, möglichen Angriffsziele und betroffenen Netzwerkkomponenten

Empfehlung von Abhilfemaßnahmen, einschließlich möglicher Schritte zur Verringerung der Folgen des Vorfalls und zum Schutz Ihrer Ressourcen vor ähnlichen Angriffen in der Zukunft

Zusätzliche Services

Unsere Experten unterstützen Sie auch dabei, die Symptome eines Vorfalls zu analysieren, tief greifende digitale Analysen für bestimmte Systemen durchzuführen, Malware-Binärdateien zu identifizieren (falls vorhanden) und Malware-Analysen durchzuführen. Die Ergebnisse dieses optionalen Service werden zusammen mit weiteren empfohlenen Abhilfemaßnahmen in einem separaten Bericht aufgeführt.

Auf Wunsch integrieren wir zudem die **Kaspersky Anti Targeted Attack (KATA) Platform** in Ihrem Netzwerk – dauerhaft oder als „Proof of Concept". Diese Plattform vereint die neuesten Technologien und globalen Analysen, die gezielte Angriffe in Ihrem System erkennen, sofort darauf reagieren und Angriffe auf allen Stufen des Lebenszyklus bekämpfen.



Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.de/enterprise**
Neues über Cyberbedrohungen: **www.viruslist.de**
IT-Sicherheitsnachrichten: **https://www.kaspersky.de/blog/b2b/**

#truecybersecurity
#HuMachine

www.kaspersky.de

© 2017 Kaspersky Labs GmbH. Alle Rechte vorbehalten. Eingetragene Handelsmarken und Markenzeichen sind das Eigentum ihrer jeweiligen Rechtsinhaber.