Threat Intelligence-Plattform

Kaspersky CyberTrace

kaspersky bring on the future

Kaspersky CyberTrace

Eine Threat Intelligence-Plattform zur Zusammenführung von Bedrohungsinformationen, die die nahtlose Integration von Threat Intelligence Feeds in SIEM-Lösungen ermöglicht. So können Analysten die Bedrohungsinformationen in ihren bestehenden Sicherheitsabläufen nutzen.

Effektive Auswahl und Analyse von Sicherheitswarnungen

Die Zahl der von Cybersicherheitsanalysten verarbeiteten Warnmeldungen nimmt exponentiell zu. Angesichts dieser riesigen Datenmengen wird eine effektive Priorisierung, Auswahl und Validierung der Warnungen zur Mammutaufgabe.

Dies kann dazu führen, dass wichtige Warnungen übersehen werden und es zu einer Alarmmüdigkeit kommt. SIEMs und andere Tools zur Sicherheitsanalyse korrelieren Ereignisse und tragen dazu bei, die Anzahl der Warnmeldungen zu reduzieren, aber die Sicherheitsanalysten sind nach wie vor extrem überlastet.

SIEM-Systeme

Durch die Integration aktueller maschinenlesbarer Bedrohungsinformationen in bestehende Sicherheitskontrollen, wie z. B. SIEM-Systeme, können Sicherheitsexperten die Ersteinstufung von Warnmeldungen automatisieren und erhalten so ausreichend Kontext, um Alarme sofort zu identifizieren, die untersucht oder zur weiteren Untersuchung und Reaktion an Incident Response-Teams weitergeleitet werden müssen.

Durch die steigende Anzahl von Threat Intelligence Feeds und verfügbaren Bedrohungsinformationen können Unternehmen jedoch nur schwer herausfinden, welche Informationen wirklich relevant sind. Bedrohungsinformationen gibt es in verschiedenen Formaten und sie beinhalten viele Gefährdungsindikatoren (Indicators of Compromise, IOCs), die für SIEM-Systeme oder Sicherheitskontrollen nur schwer zu verarbeiten sind.

Integrationen

Kaspersky CyberTrace kann mit jedem Threat Intelligence Data Feed in den Formaten JSON, STIX, XML und CSV integriert werden:

1. Kaspersky Threat Intelligence Data Feeds
2. Data Feeds anderer Hersteller
3. Frei zugängliche Informationsquellen (OSINT) oder Ihre eigenen Feeds

CyberTrace unterstützt außerdem die sofortige Integration in zahlreiche SIEM-Lösungen und Protokollquellen.

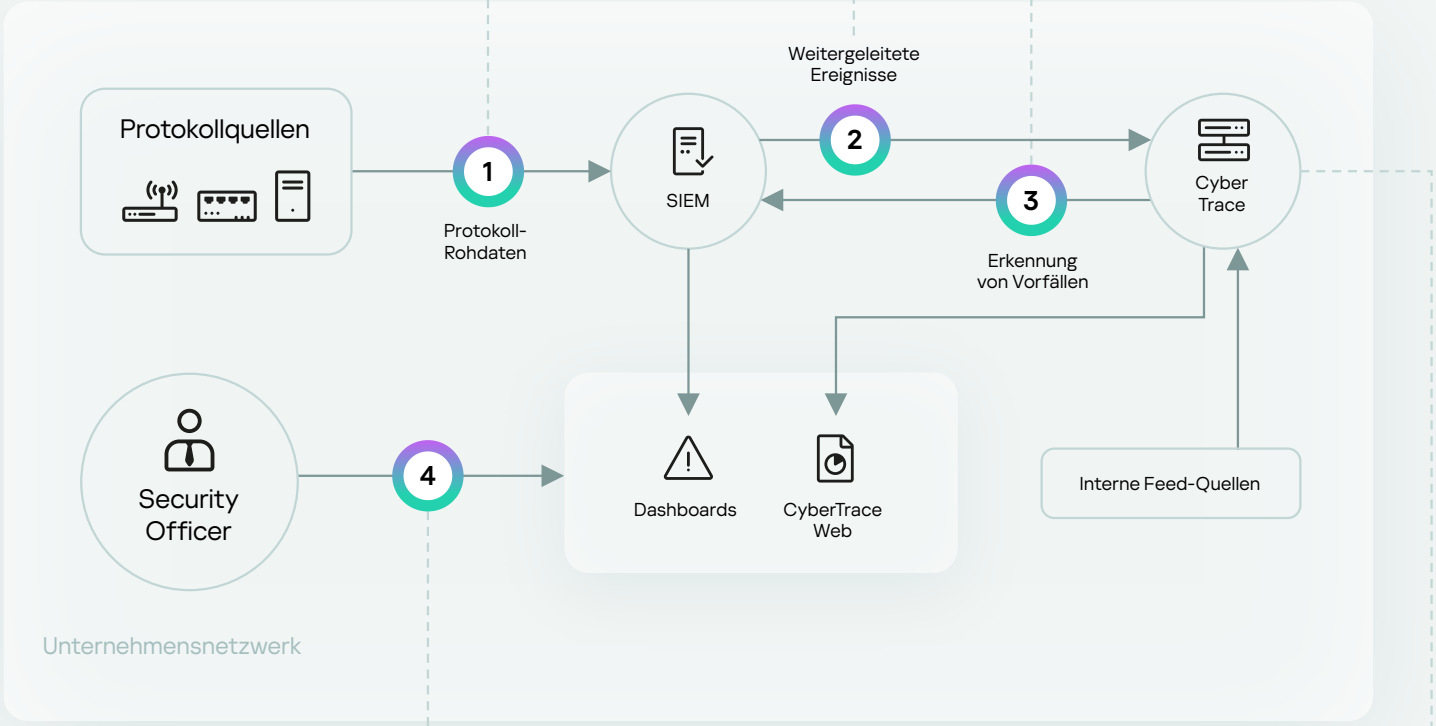
Integrationsschema von Kaspersky CyberTrace

Kaspersky CyberTrace ist in der Lage, die SIEM-Fähigkeit durch eine zusätzliche Ebene der Analyse und des Abgleichs eingehender Daten zu verbessern und damit die SIEM-Arbeitslast erheblich zu reduzieren. Der Abgleich von Ereignissen mit Informationen aus Data Feeds hilft bei der Identifizierung von Bedrohungen und liefert wertvollen Kontext zu erkannten Vorfällen. Die übergeordnete Architektur der Lösungsintegration wird in der unten stehenden Abbildung dargestellt.

SIEM sammelt Ereignisprotokolle von verschiedenen Netzwerkgeräten und IT-Systemen

Protokolle mit URLs, Hashes und IPs werden zur weiteren Analyse an CyberTrace gesendet

CyberTrace gleicht eingehende Ereignisse schnell mit Feeds ab und sendet erkannte Ereignisse an das SIEM-System und an CyberTrace Web.



- Zeigt Ereignisse im Sicherheitskontext an und empfängt Warnungen
- Untersucht Sicherheitsvorfälle basierend auf dem Kontext

Kaspersky Threat Data Feeds, kommerzielle Feeds, OSINT-Feeds, benutzerdefinierte Feeds

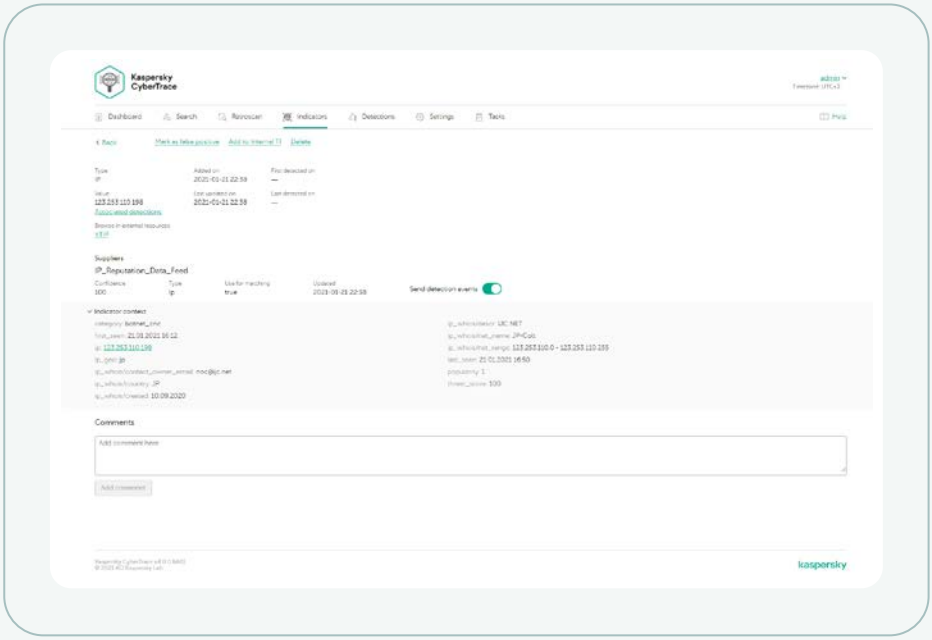
Produktmerkmale

Kaspersky CyberTrace bietet verschiedene Tools, um Bedrohungsinformationen optimal zu nutzen und eine effektive Auswahl von bzw. Reaktion auf Sicherheitswarnungen zu ermöglichen:

Detaillierte Zusammenstellung zu einem Indikator aus sämtlichen Threat Intelligence-Quellen

Eine Datenbank mit Indikatoren und Volltextsuche sowie die Möglichkeit zur Nutzung erweiterter Suchabfragen ermöglichen komplexe Abfragen über alle Indikatorfelder hinweg, einschließlich der Kontextfelder. Dank der Möglichkeit zum Filtern der Ergebnisse nach Informationslieferanten lassen sich Bedrohungsdaten sehr viel einfacher analysieren.

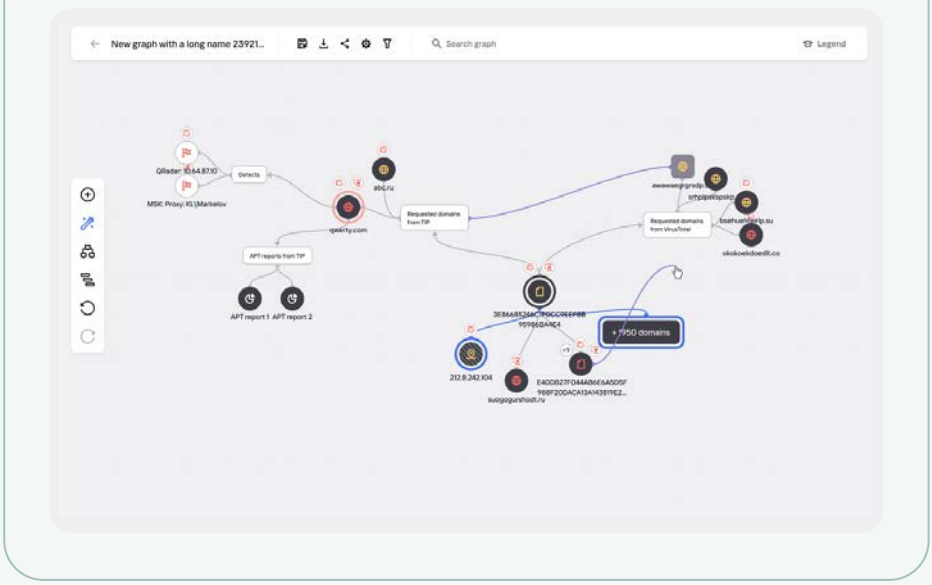
E-Mail-Abonnements und PDF-Dokumente von nationalen/ staatlichen/ Finanz-Computer Emergency Response Teams (CERTs), TI-Anbietern und Communities könnten in CyberTrace als Quelle für IoCs genutzt werden. Die Extraktion von IOCs kann sowohl aus dem E-Mail-Text als auch aus dem Anhang (XML, CSV, JSON, PDF) erfolgen. IMAP/POP3-Server und lokale/ freigegebene Ordner mit einer Sammlung von PDF-Dateien könnten als Feed-Quelle genutzt werden.



Seiten mit detaillierten Informationen zu jedem Indikator ermöglichen eine noch tiefere Analyse. Auf jeder Seite werden sämtliche Informationen zu einem Indikator aus allen Threat Intelligence-Quellen (ohne Dopplung) dargestellt. Analysten können die Bedrohungen in den Kommentaren diskutieren und interne Analysen zum Indikator hinzufügen. Neben Informationen, wann und wo der Indikator erkannt wurde, werden auch Links zur Liste der Erkennungen bereitgestellt.

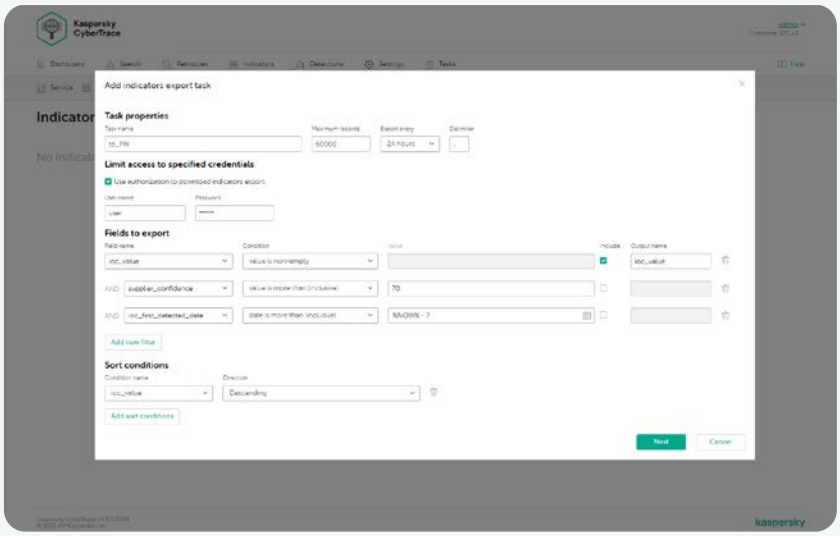
Research Graph

Mit einem Research Graph können Sie in CyberTrace gespeicherte Daten und erkannte Ereignisse visuell untersuchen und Gemeinsamkeiten von Bedrohungen erkennen. So wird die grafische Visualisierung der Zusammenhänge zwischen den im Rahmen der Untersuchungen gefundenen URLs, Domänen, IPs, Dateien und anderen Kontexten ermöglicht. Die Grafik umfasst die folgenden Funktionen: Transformationen, Minigrafik, Gruppierung von Nodes, manuelles Hinzufügen von Links, Hinzufügen von Indikatoren und Suchen nach Nodes in der Grafik. IoCs-Anreicherung auf Research Graph von VirusTotal wird unterstützt.



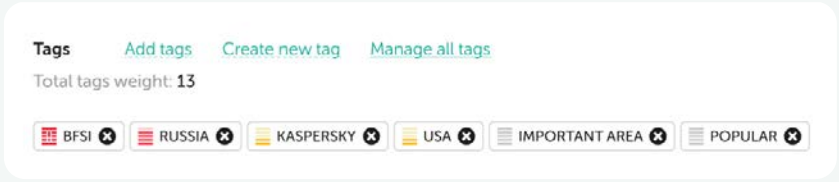
Export von Indikatoren

Mittels einer Exportfunktion für Indikatoren lassen sich exportierte IoCs nativ in Sicherheitssysteme von Drittanbietern wie Richtlinienlisten (Blockierlisten) integrieren. Außerdem können die Daten zwischen Kaspersky CyberTrace-Instanzen oder mit anderen TI-Plattform geteilt werden.



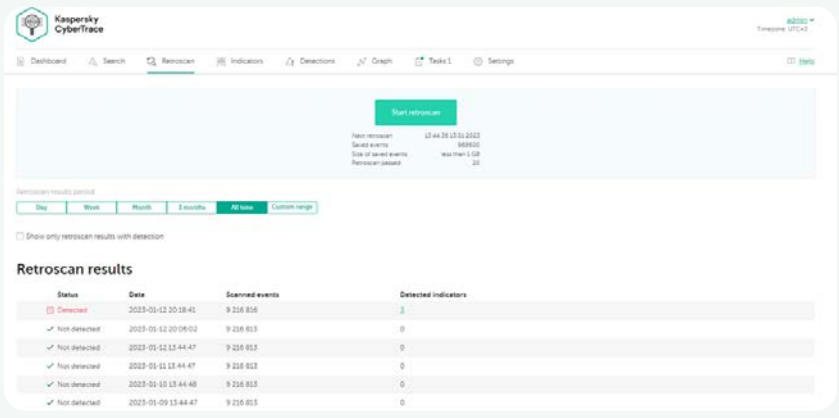
IoC-Tags

Versehen Sie Gefährdungsindikatoren (IoCs) mit Tags, um ihre Verwaltung zu vereinfachen. Sie können einen beliebigen Tag erstellen, seine Gewichtung (Wichtigkeit) festlegen und dann IoCs manuell mit dem Tag versehen. Sie können IoCs auch basierend auf diesen Tags und deren Gewichtung sortieren und filtern.



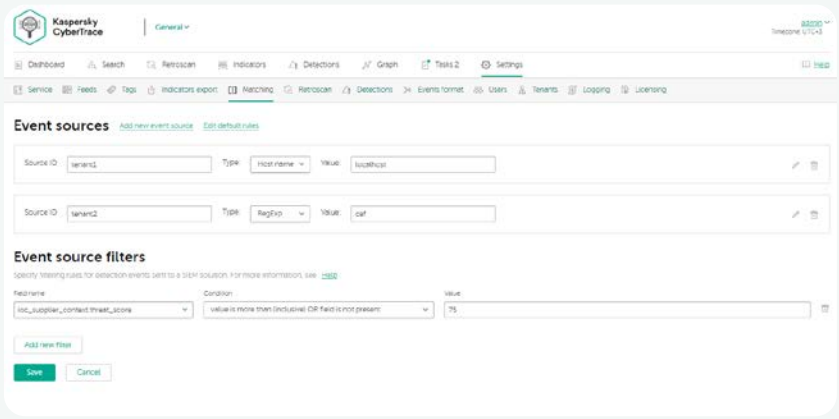
Retroscan-Funktion

Mithilfe der Korrelationsfunktion zu früheren Verläufen (Retroscan) können Sie beobachtete Phänomene aus zuvor geprüften Ereignissen anhand der neuesten Feeds analysieren, um bisher nicht erkannte Bedrohungen aufzuspüren. Der Bericht enthält alle bisherigen Erkennungen, um sie nachfolgend untersuchen zu können.



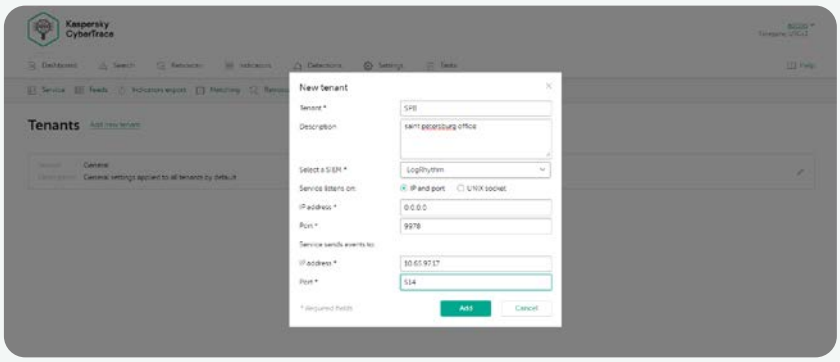
Filter für Ereignis-Quellen

Ein Filter zum Senden von erkannten Ereignissen an SIEM-Lösungen entlastet nicht nur diese Systeme, sondern verhindert auch die Alarmermüdung von Analysten. Dadurch werden nur die erkannten Ereignisse an SIEM weitergeleitet, die wirklich gefährlich sind und als Vorfälle behandelt werden müssen. Alle Weiteren werden in der internen Datenbank abgelegt und können bei Ursachenanalysen oder beim Threat Hunting eingesetzt werden.



Mehrmandantenfähigkeit

Mehrmandantenfähigkeit hilft MSSPs oder bei Anwendungsfällen in großen Unternehmen, wenn ein Service Provider Vorfälle aus verschiedenen Niederlassungen (Mandanten) bearbeiten muss. Dabei kann eine einzelne Kaspersky CyberTrace-Instanz mit den SIEM-Lösungen unterschiedlicher Mandanten verbunden werden und Sie können konfigurieren, welche Feeds bei welchem Mandanten verwendet werden sollen.



Indikatorenstatistik und Feed-Überschneidungsmatrix

Anhand von Nutzungsstatistiken zur Messung der Effektivität integrierter Feeds sowie einer Feed-Überschneidungsmatrix kann man entscheiden, welche Threat Intelligence-Quellen am zuverlässigsten sind.

Mit der HTTP Rest-API können Sie Bedrohungsdaten abrufen und verwalten

Durch die Verwendung der Rest-API kann Kaspersky CyberTrace leicht in komplexe Umgebungen integriert werden, um die Automatisierung und Orchestrierung zu ermöglichen. Integration mit der Kaspersky-Plattform zur Überwachung, Analyse und Reaktion auf Vorfälle.

Weitere Produktfunktionen

- SIEM-Konnektoren für verschiedenste SIEM-Lösungen zur Visualisierung und Verwaltung von Bedrohungsdaten
- On Demand-Suche nach Indikatoren (Hashes, IP-Adressen, Domains, URLs) für eingehende Untersuchungen
- Erweiterte Filterung für Feeds
- Batch Scans von Protokollen und Dateien
- Befehlszeilenschnittstelle für Windows- und Linux-Plattformen
- Standalone-Modus, bei dem Kaspersky CyberTrace die Protokolle von verschiedenen Quellen, wie z. B. Netzwerkgeräten, empfängt und analysiert
- Und vieles mehr

Kaspersky CyberTrace und die Kaspersky Threat Data Feeds können zwar separat verwendet werden, verbessern jedoch in Kombination deutlich die Bedrohungserkennung und ermöglichen einen sicheren Betrieb mit umfassendem globalen Einblick in Cyberbedrohungen.

Kaspersky CyberTrace und Kaspersky Threat Data Feeds bieten Organisationen folgende Möglichkeiten:

Effektive Analyse und Priorisierung von Sicherheitswarnungen

Weniger Arbeitsbelastung für Analysten

Erkennen Sie kritische Alarme sofort und treffen Sie fundiertere Entscheidungen über die Eskalation an Teams für Vorfallsreaktion.

Aufbau einer vorausschauenden informationsbasierten Abwehr

Kaspersky CyberTrace

Mehr erfahren

www.kaspersky.de

#kaspersky
#bringonthefuture