kaspersky BRING ON THE FUTURE

Kaspersky CyberTrace

Die Anzahl der Sicherheitswarnungen, die Analysten im Bereich Informationssicherheit täglich bearbeiten müssen, wächst exponentiell. Angesichts dieser riesigen Datenmengen ist eine effektive Priorisierung, Auswahl und Validierung der Warnungen fast unmöglich. Permanent zeigen die zahlreichen Sicherheitsprodukte neue Benachrichtigungen an – bis zu dem Punkt, an dem wichtige Alarme in der Masse untergehen und Analysten überfordert sind. SIEM-Systeme, also Tools zur Protokollverwaltung und Sicherheitsanalyse, die Sicherheitsdaten zusammenführen und Beziehungen zwischen den verschiedenen Warnungen finden, können die Anzahl der Sicherheitsbenachrichtigungen, die näher untersucht werden müssen, reduzieren. Doch selbst mit entsprechenden Systemen sind Sicherheitsanalysten oft überfordert.

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.

Effektive Auswahl und Analyse von Sicherheitswarnungen

Durch Integration topaktueller maschinenlesbarer Bedrohungsinformationen in bestehende Systeme, wie z.&B. SIEM-Systeme, können Security Operation Center die Erstauswahl automatisieren. Außerdem bietet sie den Sicherheitsanalysten so ausreichend Kontext, um umgehend ermitteln zu können, welche Warnungen näher untersucht oder zur weiteren Überprüfung und Bearbeitung an die an die Incident Response-Teams übergeben werden müssen. Wegen der steigenden Anzahl von Threat Intelligence Feeds und verfügbaren Bedrohungsinformationen können Unternehmen aber 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.

Kaspersky CyberTrace ist 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. Die Lösung kann jeden Threat Intelligence Feed im JSON-, STIX-, XML- oder CSV-Format integrieren, den Sie verwenden möchten. Hierzu zählen Feeds von Kaspersky, von anderen Anbietern, Open Source-Informationen (Open Source Intelligence, OSINT) sowie benutzerdefinierte Feeds. Darüber hinaus unterstützt CyberTrace zahlreiche SIEM-Lösungen und Protokollquellen ohne Konfigurationsaufwand.

Kaspersky CyberTrace nutzt einen internen Prozess zum Abgleich und zur Analyse der eingehenden Daten, der die Arbeitslast der SIEM-Systeme deutlich reduziert. Das Tool analysiert eingehende Protokolle und Ereignisse, gleicht die entsprechenden Daten schnell mit Feeds ab und erstellt bei Bedrohungen eigene Sicherheitswarnungen. Die übergeordnete Architektur der Lösungsintegration wird in der unten stehenden Abbildung dargestellt:

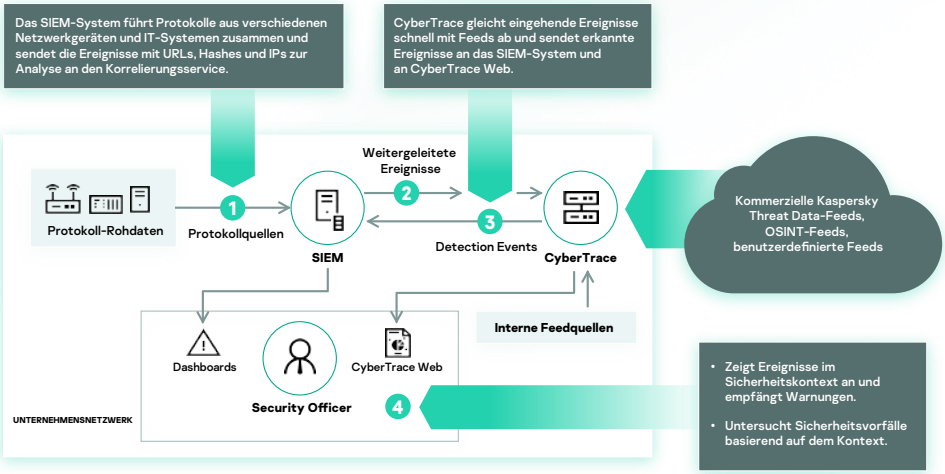

Abbildung 1. Integrationsschema von Kaspersky CyberTrace

Produktmerkmale

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

- 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.
- 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.

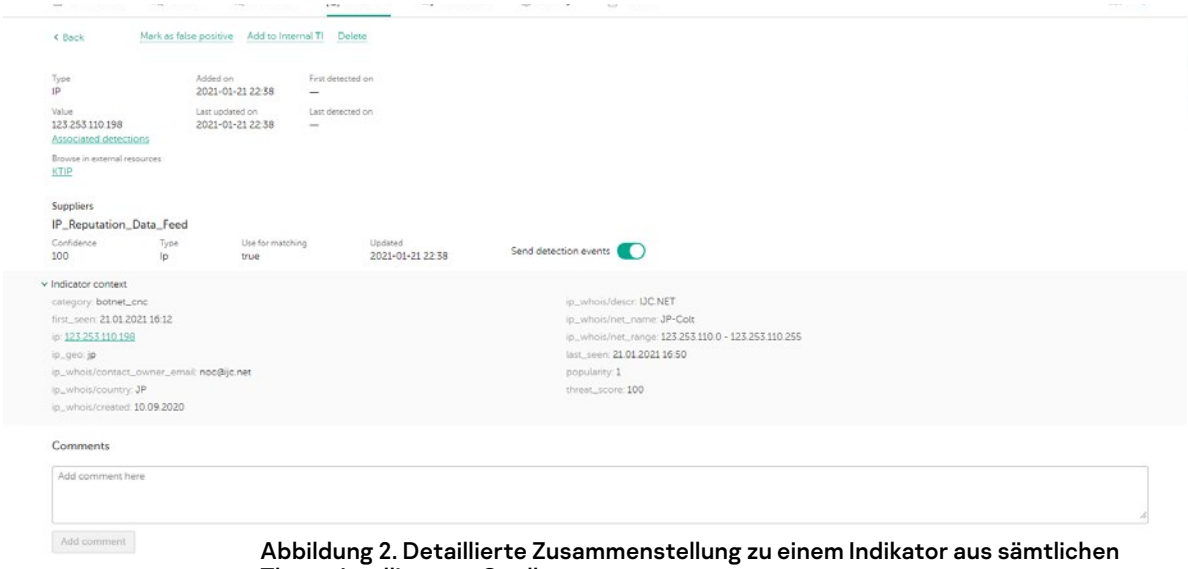

Abbildung 2. Detaillierte Zusammenstellung zu einem Indikator aus sämtlichen Threat Intelligence-Quellen

- Mittels einer Exportfunktion lassen sich Indikatorensätze in Sicherheitssysteme wie Richtlinienlisten (Blocklisten) eintragen. Außerdem können die Daten zwischen Kaspersky CyberTrace-Instanzen oder mit anderen TI-Plattformen geteilt werden.

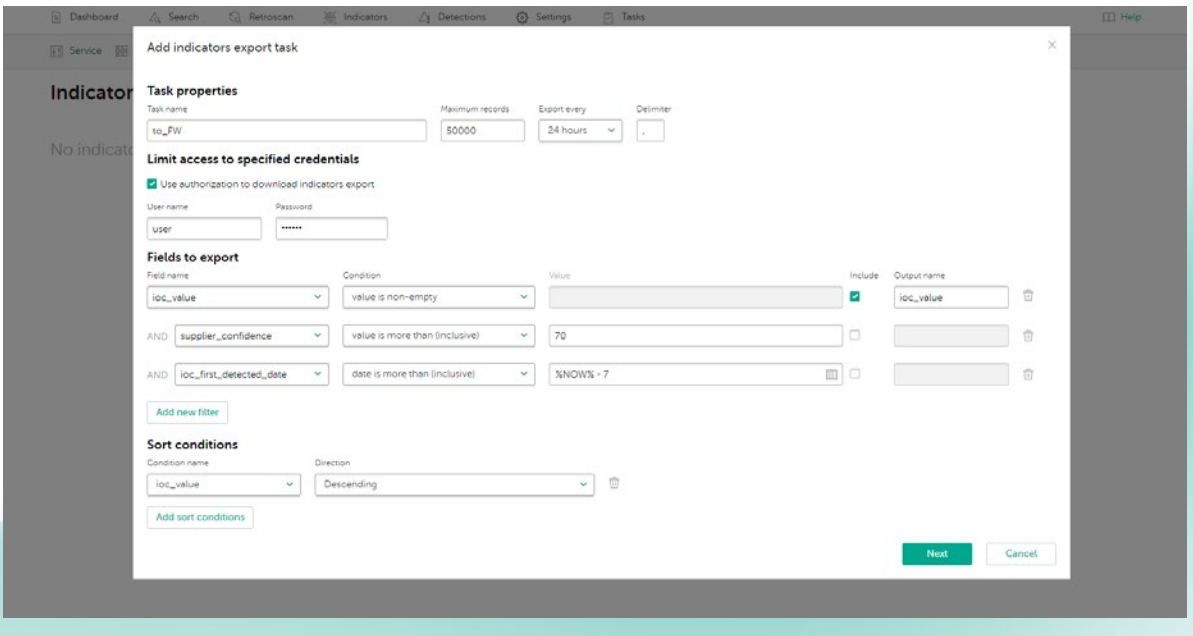

Abbildung 3. Exportieren von Indikatoren

- 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.
- Ein Filter zum Senden von erkannten Ereignissen ("Events") an SIEM-Lösungen entlastet nicht nur diese Systeme, sondern verhindert auch die Alarmermüdung von Analysten. Dadurch werden nur die Events an SIEM weitergeleitet, die wirklich gefährlich sind und als Vorfälle behandelt werden müssen. Alle weiteren Events werden in der internen Datenbank abgelegt und können bei Ursachenanalysen oder beim Threat Hunting eingesetzt werden.
- Mehrmandantenfähigkeit hilft MSSPs oder bei Anwendungsfällen in großen Unternehmen, wenn ein Service Provider Events 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.

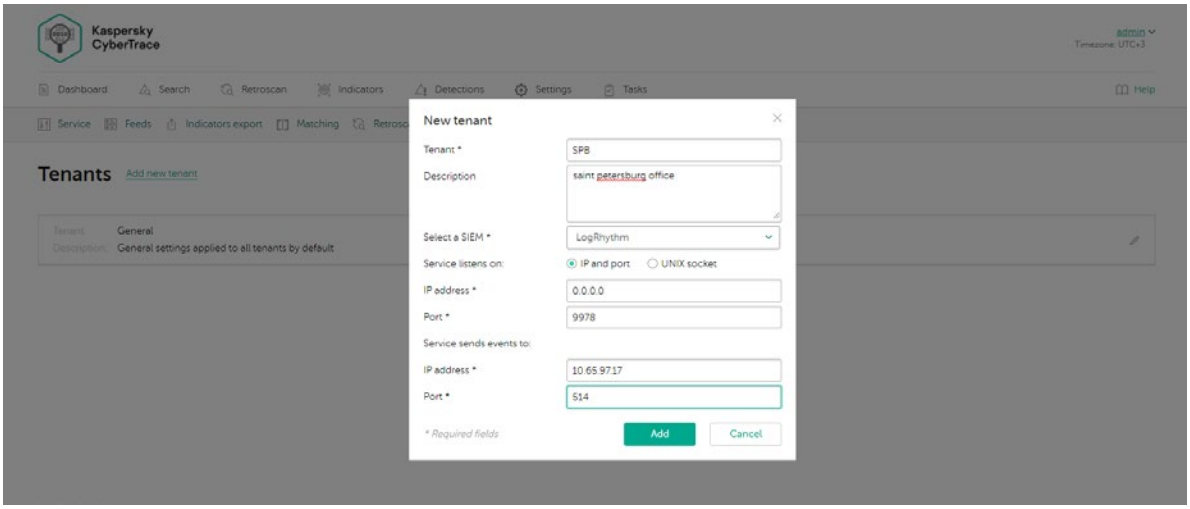

Abbildung 4. Erstellen neuer Mandanten

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

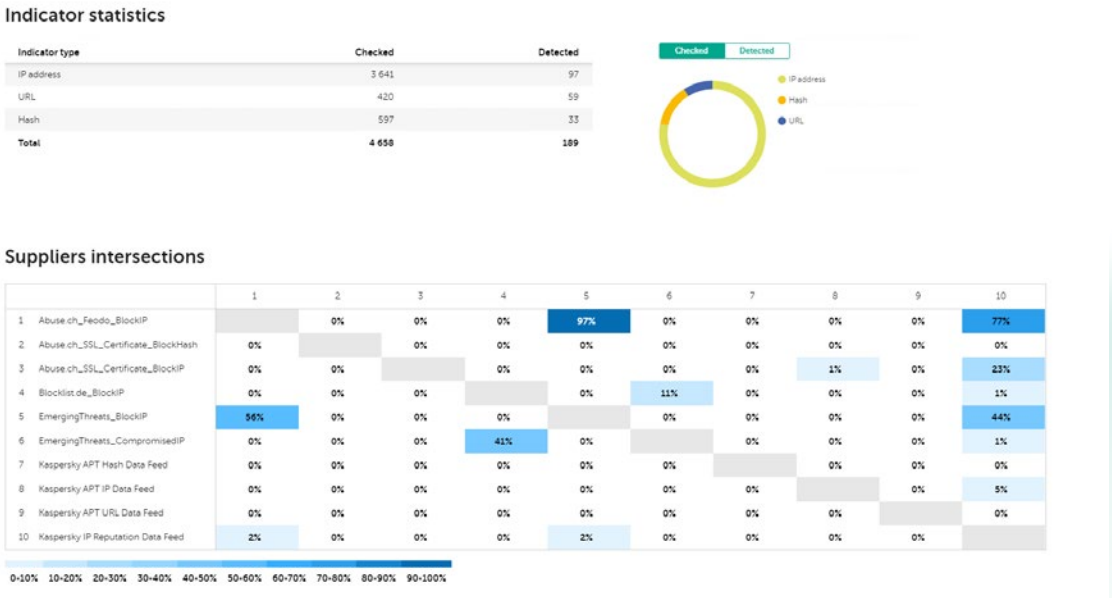

Abbildung 5. Indikatorenstatistik und Feed-Überschneidungsmatrix

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

- Mit der HTTP Rest-API können Sie Bedrohungsdaten abrufen und verwalten. Denn über die Rest-API lässt sich Kaspersky CyberTrace zur vereinfachten Automatisierung und Orchestrierung mühelos in komplexe Umgebungen integrieren.
- Integration mit der Kaspersky Unified Monitoring and Analysis-Plattform (KUMA), einschließlich Web UI-Integration (einzelne Weboberfläche), wird ebenfalls unterstützt.

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
- Geringere Arbeitsbelastung für Analysten
- Umgehende Erkennung kritischer Warnungen und fundiertere Entscheidungen hinsichtlich der Eskalation von Warnungen an Incident Response-Teams
- Aufbau einer vorausschauenden informationsbasierten Abwehr

Neues über Cyberbedrohungen: de.securelist.com
IT Security News: www.kaspersky.de/blog/b2b
IT-Sicherheit für KMU: kaspersky.de/business
IT-Sicherheit für Großunternehmen: kaspersky.de/enterprise
Threat Intelligence-Portal: opentip.kaspersky.de

www.kaspersky.de

Beständigkeit, Unabhängigkeit und Transparenz – das zeichnet uns aus. Wir möchten eine sichere Welt schaffen, in der Technologien uns das Leben erleichtern. Deshalb schützen wir diese Technologien, damit Menschen auf der ganzen Welt die unzähligen Möglichkeiten nutzen können, die Technologien mit sich bringen. Wir tragen mit Cybersicherheit zu einer sicheren Zukunft bei.

Weitere Informationen finden Sie hier:
kaspersky.com/transparency

Proven.
Transparent.
Independent.