Kaspersky® CyberTrace

Die Anzahl der Sicherheitswarnungen, die Analysten in Security Operations Centers (SOC) täglich bearbeiten müssen, wächst exponentiell an. Angesichts dieser riesigen Datenmenge sind die effektive Priorisierung, Auswahl und Validierung der Warnungen nahezu unmöglich. Permanent zeigen die zahlreichen Sicherheitsprodukte neue Benachrichtigungen an – bis zu dem Punkt, an dem wichtige Alarme in dem Chaos 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. Analysten an vorderster Front – sogenannte Tier 1 Analysts – sind jedoch auch mit entsprechenden Systemen völlig überfordert.

Effektive Auswahl und Analyse von Sicherheitswarnungen

Durch Integration topaktueller maschinenlesbarer Bedrohungsinformationen in bestehende Systeme, wie z. B. SIEM-Systeme, können Security Operation Centers die Erstauswahl automatisieren. Außerdem bietet sie den Tier 1 Analysts so ausreichend Kontext, um umgehend ermitteln zu können, welche Warnungen näher untersucht oder zur weiteren Überprüfung und Bearbeitung an die an die Incident Response (IR) Teams übergeben 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 werden in verschiedenen Formaten bereitgestellt und beinhalten viele Gefährdungsindikatoren (Indicators of Compromise, IoCs), die für SIEM-Systeme oder Sicherheitskontrollen nur schwer zu verarbeiten sind.

Kaspersky CyberTrace ist ein Threat Intelligence Tool zur Zusammenführung und Analyse von Bedrohungsinformationen, das die nahtlose Integration von Threat Intelligence Feeds in SIEM-Lösungen ermöglicht. So können Analysten die Bedrohungsinformationen in ihren bestehenden Sicherheitsworkflows 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 Lab, von anderen Anbietern, Open Source-Informationen (Open Source Intelligence, OSINT) sowie benutzerdefinierte Feeds. Darüber hinaus unterstützt CyberTrace zahlreiche SIEM-Lösungen und Protokollquellen ohne Konfigurationsaufwand. Durch automatische Abstimmung der Protokolle mit den Bedrohungsfeeds bietet Kaspersky CyberTrace zu jedem Zeitpunkt eine Echtzeitübersicht der aktuellen Sicherheitssituation, damit Tier 1 Analysts schneller fundiertere Entscheidungen treffen können.

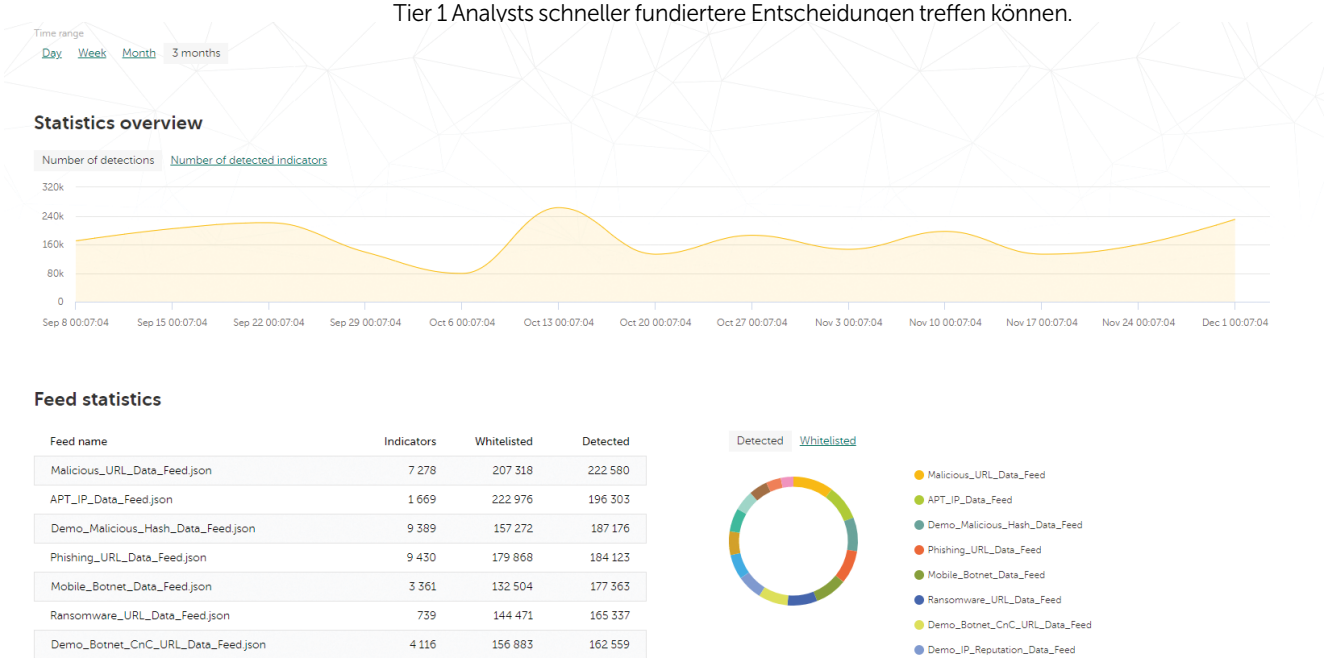


Abbildung 1: Statistiken von Kaspersky CyberTrace

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

- Bereits enthaltene Demo-Bedrohungsfeeds von Kaspersky Lab sowie OSINT-Feeds
- SIEM-Konnektoren für verschiedenste SIEM-Lösungen zur Visualisierung und Verwaltung von Bedrohungsdaten
- Feed-Nutzungsstatistiken zur Messung der Effektivität integrierter Feeds
- On Demand-Suche nach Indikatoren (Hashes, IP-Adressen, Domains, URLs) für eingehende Untersuchungen
- Weboberfläche für Datenvisualisierungen, Konfigurationszugriff sowie zur Verwaltung von Feeds, Syntaxanalyse-Regeln, Blacklists und Whitelists
- Erweiterte Feed-Filter (basierend auf dem Kontext des jeweiligen Indikators, einschließlich Bedrohungstyp, Geostandort, Beliebtheit, Zeitstempel und weiteren Informationen) sowie Protokollereignisse (basierend auf benutzerdefinierten Bedingungen)
- Export von Suchergebnissen aus Datenfeeds im CSV-Format zur Integration in andere Systeme (Firewalls, Netzwerk- und Host-IDS, benutzerdefinierte Tools)
- Batch Scans von Protokollen und Dateien
- Befehlszeilenschnittstelle für Windows- und Linux-Plattformen
- Standalone-Modus, bei dem Kaspersky CyberTrace nicht in ein SIEM-System integriert wird, sondern die Protokolle von verschiedenen Quellen, wie z. B. Netzwerkgeräten, empfängt und analysiert
- Installation in DMZs, die vom Internet isoliert sein müssen

Das Tool nutzt einen internen Prozess zum Abgleich und zur Analyse der eingehenden Daten, der die Arbeitslast der SIEM-Systeme deutlich reduziert. Kaspersky CyberTrace 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:

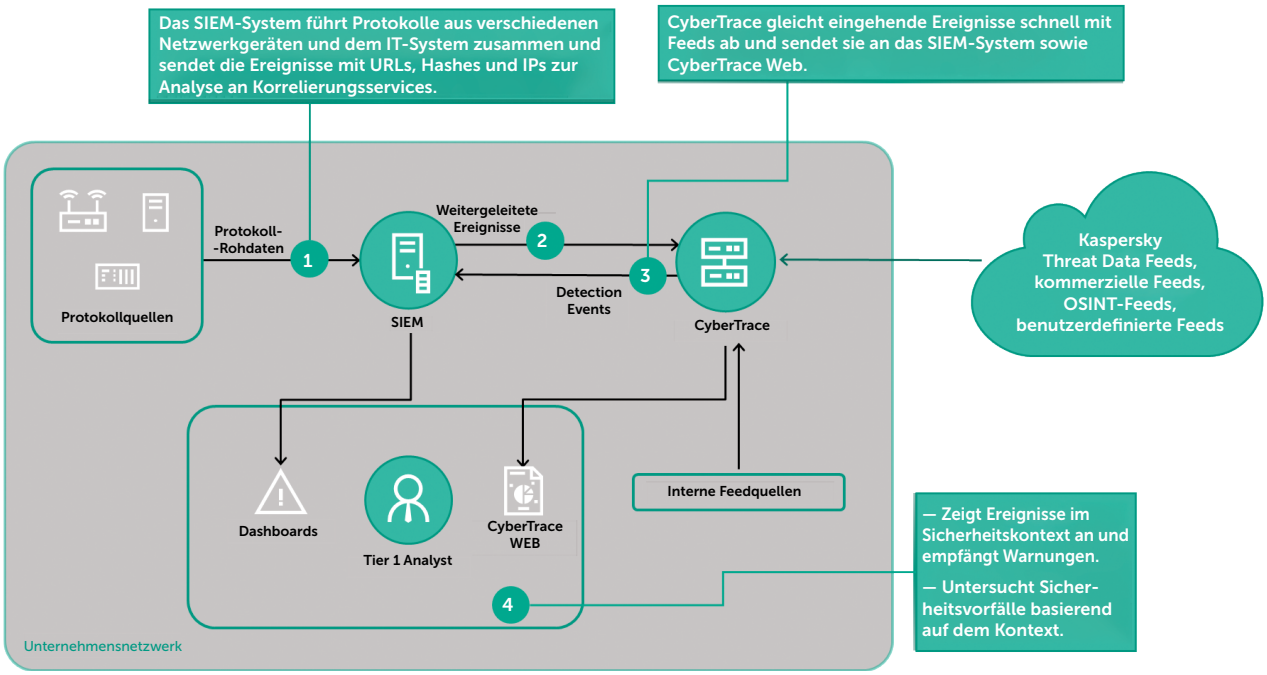


Abbildung 2: Integrationsschema von Kaspersky CyberTrace

Kaspersky Lab bietet darüber hinaus eine Reihe ständig aktualisierter Bedrohungsfeeds, die in Kaspersky CyberTrace integriert werden können. Diese Feeds ermöglichen globale Transparenz, die rechtzeitige Erkennung von Cyberbedrohungen, die Priorisierung von Sicherheitswarnungen und die effektive Reaktion auf Vorfälle bzgl. der Informationssicherheit:

- IP Reputation Feed: Enthält eine Reihe von IP-Adressen mit Kontext zu verschiedenen Kategorien verdächtiger und schädlicher Hosts
- Malicious and Phishing URL Feed: Enthält schädliche bzw. Phishing-Links und -Websites
- Botnet C&C URL Feed: Enthält C&C-Server für Desktop-Botnets sowie zugehörige schädliche Objekte
- Mobile Botnet C&C URL Feed: Enthält C&C-Server für mobile Botnets

- Ransomware URL Feed: Enthält Links, die Ransomware-Objekte hosten oder auf die Ransomware-Objekte zugreifen
- APT IoC Feeds: Enthält schädliche Domains, Hosts, IP-Adressen und Dateien, die Cyberkriminelle bei APT-Angriffen verwenden
- Passive DNS (pDNS) Feed: Eine Reihe von Datensätzen, die die Ergebnisse von DNS-Auflösungen (von der Domain zur entsprechenden IP-Adresse) enthalten[1]
- IoT URL Feed: Enthält Websites, die zum Herunterladen von IoT Malware verwendet wurden[2]
- Malicious Hash Feed: Umfasst die gefährlichste, am weitesten verbreitete sowie neu aufkommende Malware
- Mobile Malicious Hash Feed: Enthält schädliche Objekte, die Android- und iOS-Mobilgeräte infizieren
- P-SMS Trojan Feed: Umfasst SMS-Trojaner, über die Angreifer SMS-Nachrichten stehlen, löschen oder beantworten und Sondergebühren für mobile Nutzer erheben können
- Whitelisting Data Feed: Stellt für Lösungen und Services von Drittanbietern systematische Informationen zu legitimer Software bereit

Datenfeeds werden aus kombinierten, heterogenen und äußerst zuverlässigen Quellen zusammengeführt, darunter das Kaspersky Security Network und seine über 100 Millionen globalen Benutzer, die ihre Daten zu Cyberbedrohungen freiwillig mit uns teilen, unsere eigenen Webcrawler, unser Botnet-Überwachungssystem, das rund um die Uhr alle bekannten Botnets, ihre Ziele und Aktivitäten überwacht, Spam-Fallen, Forschungsteams sowie vertrauenswürdige Partner.

All diese Daten werden dann in Echtzeit sorgfältig untersucht und anhand verschiedener Aufbereitungsverfahren, wie z. B. durch statistische Kriterien, Kaspersky-Expertensysteme (Sandboxes, heuristische Engines, Multi-Scanner, Similaritätstools, Erstellung von Verhaltensprofilen usw.), durch Validierung von Analysten und durch Verifizierung anhand von Whitelists, präzisiert.

Jedem Datensatz in den einzelnen Datenfeeds wird umfangreicher Kontext hinzugefügt (Bedrohungsbewertung, Geostandort, Bedrohungsnamen, Zeitstempel, aufgelöste IP-Adressen infizierter Webressourcen, Hashes, Beliebtheit usw.).

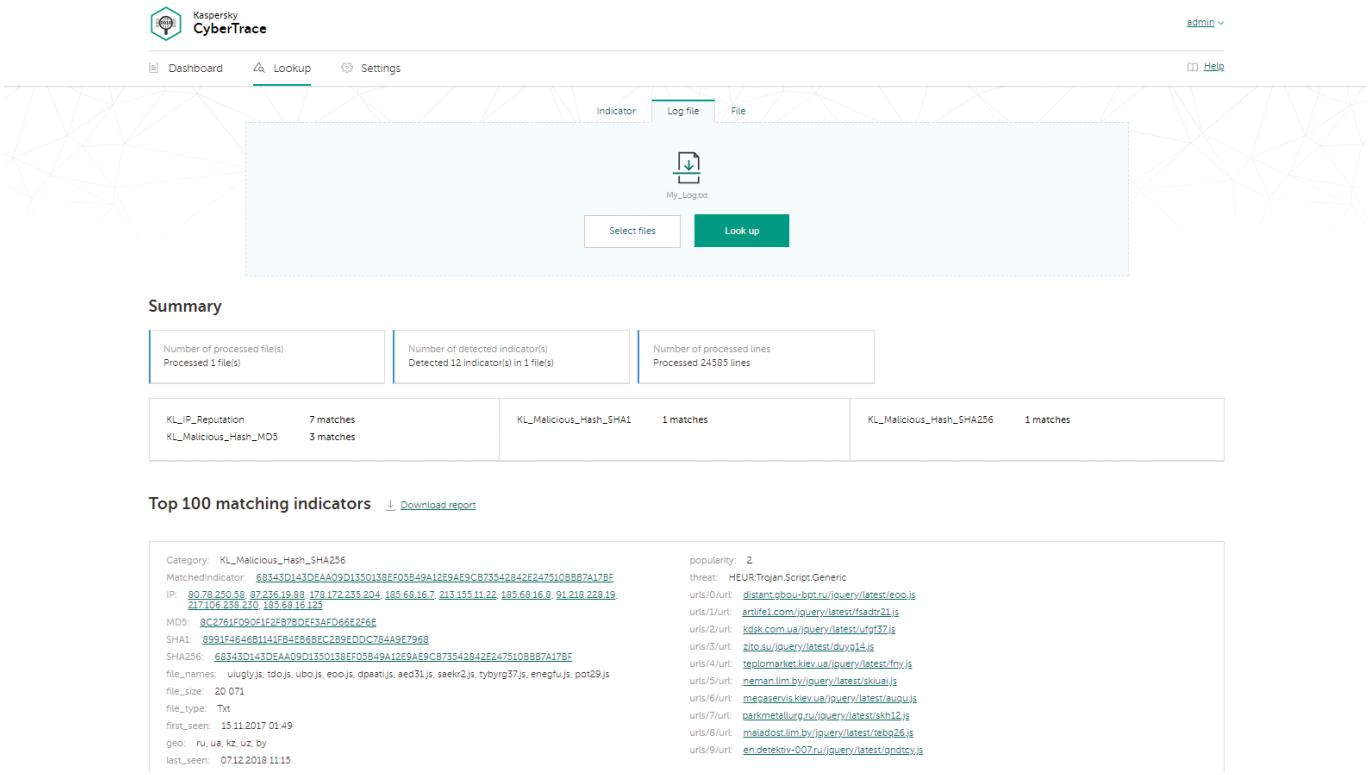


Abbildung 3: Kontext der Kaspersky Threat Data Feeds

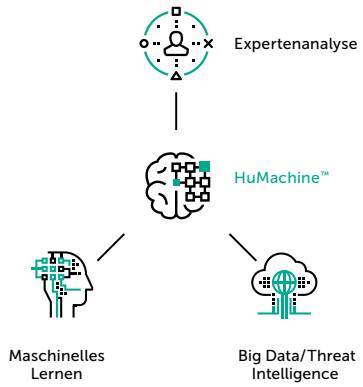
1 Die Integration wird noch 2019 unterstützt.

2 Die Integration wird noch 2019 unterstützt.

Die Kontextdaten eröffnen den Blick auf das große Ganze und ermöglichen die weitere Analyse und vielfältige Nutzung der Daten. Mit dem richtigen Kontext lassen sich mit den Daten schnell die wichtigsten Fragen beantworten: Wer, was, wo und wann? So sind die Cyberkriminellen hinter der aktuellen Bedrohung schnell gefunden und Experten können fundierte Entscheidungen zur Bedrohungsreaktion treffen.

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 die Kaspersky Threat Data Feeds bieten SOC-Analysten folgende Vorteile:

- Effektive Analyse und Priorisierung von Unmengen an Sicherheitswarnungen
- Verbesserung und Beschleunigung der Auswahl und Erstreaktion
- Umgehende Erkennung kritischer Warnungen und fundiertere Entscheidungen hinsichtlich der Eskalation von Warnungen an Vorfallsreaktionsteams
- Vorausschauende informationsbasierte Abwehr



Kaspersky Lab
Cybersicherheit für Unternehmen: **www.kaspersky.de/enterprise**
Neues über Cyberbedrohungen: **https://de.securelist.com**
IT-Sicherheitsnachrichten: **https://www.kaspersky.de/blog/b2b/**

#truecybersecurity
#HuMachine

www.kaspersky.de

© 2019 Kaspersky Labs GmbH. Alle Rechte vorbehalten. Eingetragene Markenzeichen und Handelsmarken sind das Eigentum ihrer jeweiligen Rechtsinhaber.