# Kaspersky Cybersecurity Services

kaspersky

Weitere Informationen finden Sie unter kaspersky.de
#bringonthefuture

Cyberverbrechen kennen heutzutage keine Grenzen und ihr technisches Potenzial wächst rasant: Jeden Tag erleben wir, wie die Angriffe immer ausgereifter werden. Unser Ziel ist es, alle Arten von Cyberbedrohungen abzuwehren und die digitale Welt unserer Kunden sicherer zu machen. Um dies zu gewährleisten und die Nutzung des Internets sicher zu machen, müssen Bedrohungsinformationen in Echtzeit weitergegeben werden. Ein zeitnaher Zugriff auf Informationen ist für einen effektiven Schutz von Daten und Netzwerken unerlässlich.

Eugene Kaspersky
Chairman und CEO, Kaspersky

# Einleitung

**Jeden Tag entstehen neue Cyberbedrohungen in den unterschiedlichsten Formen und über viele verschiedene Angriffsvektoren.**

**Es gibt keine einzelne Lösung, die vollständigen Schutz bietet. Jedoch besteht selbst in unserer Big Data-Welt ein großer Teil des Kampfes gegen die aktuellen Bedrohungen darin, zu wissen, wo man nach Gefahren suchen soll.**

**Als Geschäftsführer, CIO, CISO oder CTO liegt es in Ihrer Verantwortung, Ihr Unternehmen vor den heutigen Bedrohungen zu schützen und die Gefahren zu prognostizieren, die in den nächsten Jahren auf Sie zukommen. Dazu ist mehr als nur ein zuverlässiger technologischer Schutz vor bekannten Bedrohungen erforderlich. Sie benötigen strategische Sicherheitsinformationen, für deren Erhebung die wenigsten Unternehmen über genügend interne Ressourcen verfügen.**

**Wir bei Kaspersky wissen, dass langfristiger Unternehmenserfolg auf langfristigen Beziehungen beruht.**

**Mit Kaspersky an Ihrer Seite erhalten Sie stets in Echtzeit wichtige Informationen über aktuelle Bedrohungen. Unsere umfassenden Cybersecurity Services helfen Ihrem Security Operation Center (SOC)/IT-Sicherheitsteam dabei, das Unternehmen vor Online-Bedrohungen zu schützen.**

**Selbst wenn Ihr Unternehmen keine Kaspersky-Produkte einsetzt, können Sie von den Kaspersky Cybersecurity Services profitieren.**

**Kaspersky Cybersecurity Services**

- **Kaspersky Threat Intelligence**
- **Kaspersky Threat Hunting**
- **Kaspersky Cybersecurity Training**
- **Kaspersky Incident Response**
- **Kaspersky Security Assessment**

## Sicherheit mit dem entscheidenden Unterschied

**Den aktuellen Bedrohungen mit unseren Security Intelligence Services immer einen Schritt voraus zu sein** – das ist unser Anspruch. Dadurch sind wir in der Lage, einen leistungsstarken Malware-Schutz auf dem Markt bereitzustellen.

**In unserem Unternehmen steht Technologie auf allen Mitarbeiterebenen im Mittelpunkt** – ausgehend von unserem CEO Eugene Kaspersky.

**Unser Global Research and Analysis Team** (GReAT) besteht aus erfahrenen IT-Sicherheitsexperten, die bei der Erkennung einiger der weltweit gefährlichsten Malware-Bedrohungen und gezielten Angriffe federführend waren.

**Viele der weltweit anerkanntesten Sicherheitsunternehmen und Vollzugsbehörden,** darunter INTERPOL, Europol, CERT und die Polizei Londons, haben uns aktiv um Unterstützung gebeten.

**Kaspersky entwickelt alle unternehmenseigenen Kerntechnologien intern,** was die Zuverlässigkeit unserer Produkte und Dienstleistungen erhöht, denn alle unsere Technologien greifen nahtlos ineinander.

**Die renommiertesten Branchenanalysten,** darunter Gartner, Forrester Research und International Data Corporation (IDC), sehen uns in vielen wichtigen IT-Sicherheitskategorien an der Spitzenposition.

**Mehr als 130 OEMs** nutzen unsere Technologien innerhalb ihrer eigenen Produkte und Services, darunter Microsoft, Cisco, Blue Coat, Juniper Networks, Alcatel Lucent und mehr.

# Kaspersky Threat Intelligence

**Die Überwachung, Analyse, Interpretation und Abwehr der sich ständig weiterentwickelnden IT-Sicherheitsbedrohungen ist mit immensem Aufwand verbunden. Unternehmen aus allen Branchen sind für den effektiven Umgang mit IT-Sicherheitsbedrohungen auf aktuelle und relevante Daten angewiesen.**

**Kaspersky Cybersecurity Services**

**Kaspersky Threat Intelligence**

Threat Data Feeds
CyberTrace
APT Intelligence Reporting
Digital Footprint Intelligence
Threat Lookup
Cloud Sandbox

**Kaspersky Threat Hunting**

**Kaspersky Cybersecurity Training**

**Kaspersky Incident Response**

**Kaspersky Security Assessment**

Die Threat Intelligence Services von Kaspersky bieten Ihnen Zugriff auf alle Informationen, die Sie zur Abwehr dieser Bedrohungen benötigen. Sie werden von unserem erfahrenen Team aus Forschern und Analysten zur Verfügung gestellt.

Wissen, Erfahrung und umfassende Erkenntnisse über praktisch jeden Aspekt der Cybersicherheit haben Kaspersky zum vertrauenswürdigen Partner angesehener internationaler Strafverfolgungs- und Regierungsbehörden, darunter Interpol und CERTs, gemacht. Auch Sie können dieses Wissen für Ihr Unternehmen nutzen.

Die Threat Intelligence Services von Kaspersky beinhalten:

- Threat Data Feeds
- CyberTrace
- APT Intelligence Reporting
- Digital Footprint Intelligence
- Threat Lookup
- Cloud Sandbox

## Threat Data Feeds

Cyberangriffe geschehen jeden Tag. Cyberbedrohungen werden immer häufiger, komplexer und schwerer erkennbar. Zuverlässige **Abwehrmaßnahmen zu finden, wird zunehmend schwieriger**. Angreifer nutzen komplizierte **Kill Chains**, kampagnen und angepasste **Taktiken, Techniken und Abläufe (Tactics, Techniques and Procedures, TTPs), um in Systeme einzudringen und Ihre Geschäftsabläufe zu unterbrechen oder Ihren Kunden zu schaden**. Inzwischen ist bekannt, dass Schutz nur über neuartige Methoden bereitgestellt werden kann, die auf Bedrohungsinformationen basieren.

Durch Integration topaktueller Feeds mit Bedrohungsinformationen zu verdächtigen und gefährlichen IPs, URLs und Datei-Hashes in bestehende Sicherheitskontrollen, wie z. B. SIEM-Systeme, können Sicherheitsteams die Ersteinstufung von Warnmeldungen automatisieren. Außerdem bieten 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 Incident Response (IR) Teams übergeben werden müssen.

Andere Sicherheitsanbieter und Unternehmen nutzen Kaspersky Threat Data Feeds, um eigene Sicherheitslösungen zu entwickeln oder **ihr Unternehmen zu schützen.**

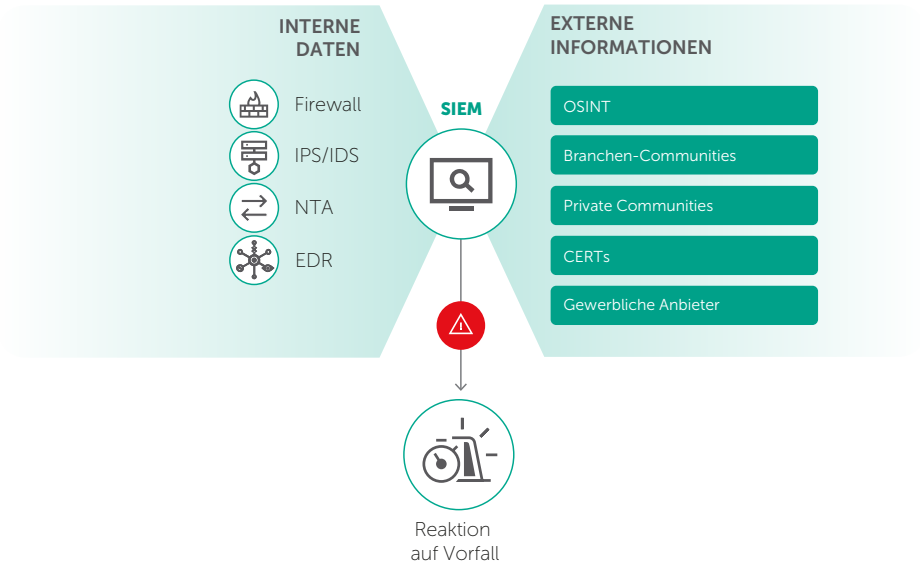



**Abbildung 1. Operationalisierung externer Bedrohungsinformationen**

**Kontextdaten**

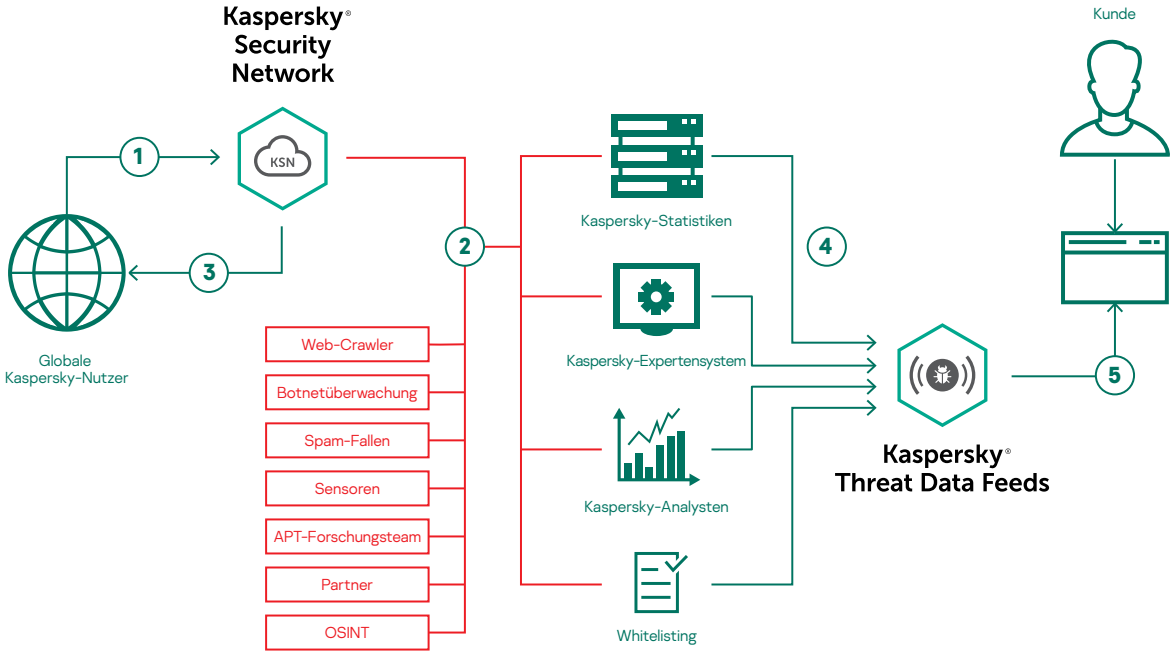
Jeder Datensatz in jedem Data Feed wird mit **umfangreichem Kontext** angereichert (Bezeichnungen von Bedrohungen, Zeitstempel, Geolokalisierungsdaten, aufgelöste IP-Adressen infizierter Webressourcen, Hashes, Beliebtheit usw.). Kontextdaten eröffnen den Blick auf das große Ganze und ermöglichen die weitere Analyse und vielfältige Nutzung der Daten. Wenn die Daten in einen Kontext gesetzt werden, liefern sie schneller Antworten auf die **Fragen „Wer?“, „Was?“, „Wo?“ und „Wann?“**. Außerdem geben sie Aufschluss über Ihre Gegner, sodass Sie rechtzeitig Entscheidungen treffen und die **richtigen Maßnahmen für Ihr Unternehmen** finden können.

# Die Data Feeds

Die Feeds umfassen Folgendes:

- **IP Reputation Feed** – Gruppen von IP-Adressen mit Kontext zu verdächtigen und schädlichen Hosts;
- **Malicious and Phishing URL** – 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, um infizierte Geräte zu erkennen, die mit C&C-Servern kommunizieren;
- **Ransomware URL Feed** – Enthält Links, die Ransomware-Objekte hosten oder auf die Ransomware-Objekte zugreifen;
- **Vulnerability Data Feed** – Eine Reihe von Sicherheitsschwachstellen mit zugehörigen Bedrohungsinformationen (etwa Hashes von anfälligen Programmen/Exploits, Zeitstempel, CVEs und Patches);
- **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;
- **IoT URL Feed** – Enthält Websites, die zum Herunterladen von IoT Malware verwendet wurden;
- **Malicious Hash Feed** – Umfasst die gefährlichste, am weitesten verbreitete und neu aufkommende Malware;
- **ICS Hash-Datenfeeds** – Satz von Hash-Werten mit entsprechendem Kontext zur Erkennung von schädlichen Objekten, die in ICS (Industrial Control Systems) verwendete Geräte befallen;
- **Mobile Malicious Hash Feed** – Unterstützt die Erkennung schädlicher Objekte, die mobile Android- und iOS-Plattformen infizieren;
- **P-SMS Trojan Feed** – Unterstützt die Erkennung von SMS-Trojanern, über die Angreifer SMS-Nachrichten stehlen, löschen oder beantworten und Sondergebühren für mobile Nutzer erheben können;
- **Whitelisting Data Feed** – Versorgt Lösungen und Services von Drittanbietern mit systematischen Informationen zu legitimer Software;
- **Mit Kaspersky Transforms for Maltego** können Sie URLs, Hashes und IP-Adressen mithilfe der Feeds von Kaspersky überprüfen.

**Abbildung 2. Quellen der Kaspersky Threat Intelligence**



**Service-Highlights**

- Data Feeds mit vielen **False Positives** sind wertlos. Deshalb werden die Feeds vor ihrer Veröffentlichung umfassend getestet und gefiltert, um zu gewährleisten, dass nur überprüfte Daten bereitgestellt werden.
- Die Data Feeds werden automatisch in Echtzeit generiert – basierend auf den weltweit vom Kaspersky Security Network erfassten Daten, die einen Einblick in einen signifikanten Anteil des gesamten Internetdatenverkehrs und alle möglichen Datentypen von Millionen von Endbenutzern in mehr als 213 Ländern gewähren. So werden hohe **Erkennungsraten** garantiert.
- Sämtliche Feeds werden über eine äußerst fehlertolerante Infrastruktur generiert und überwacht, die **dauerhafte Verfügbarkeit** gewährleistet.
- Die Feeds ermöglichen die **umgehende Erkennung von URLs**, die für Phishing, Malware, Exploits, Botnets und andere schädliche Inhalte genutzt werden.
- **Malware** in allen Arten von Datenverkehr (Web, E-Mail, P2P, IM usw.) sowie gezielte mobile Malware kann **sofort erkannt** und identifiziert werden.
- Einfache **Verteilungsformate (JSON, CSV, OpenIOC, STIX)** über **HTTPS** oder Ad-hoc-Bereitstellungsmechanismen ermöglichen die einfache Integration der Daten in Sicherheitslösungen.
- Hunderte von Experten, darunter **Sicherheitsanalyste**n aus der ganzen Welt, weltweit anerkannte **Sicherheitsexperten aus unserem GReAT-Team** und führenden Forschungs- und Entwicklungsteams, tragen gemeinsam zur Bereitstellung dieser Feeds bei. Sicherheitsbeauftragte erhalten kritische, aus zuverlässigen Daten generierte Informationen und Benachrichtigungen, ohne Gefahr zu laufen, von unnötigen Anzeigen und Warnungen überflutet zu werden.
- **Einfache Implementierung**. Dank ergänzender Dokumentation, Beispielen, einem persönlichen technischen Account Manager sowie dem technischen Support von Kaspersky geht die Integration schnell und einfach vonstatten.

## Erfassung und Verarbeitung

Unsere Data Feeds werden aus zusammengeführten, heterogenen und äußerst zuverlässigen Quellen bezogen, darunter das Kaspersky Security Network, unsere eigenen Webcrawler, unser Service zur Botnet-Überwachung (Überwachung von Botnets und ihrer Ziele und Aktivitäten rund um die Uhr, das ganze Jahr) sowie Spam-Fallen, Forschungsteams und Partner.

Dann werden sämtliche zusammengefassten Daten in Echtzeit sorgfältig untersucht und anhand verschiedener Aufbereitungsverfahren präzisiert, z. B. durch statistische Kriterien, Sandboxes, heuristische Engines, Similaritätstools, Erstellung von Verhaltensprofilen, die Validierung durch Analysten und die Verifizierung anhand von Whitelists.

## Vorteile

- **Verstärken Sie Ihre Lösungen zur Netzwerkverteidigung**, einschließlich SIEMs, Firewalls, IPS/IDS, Sicherheits-Proxys, DNS-Lösungen und APT-Abwehr, mit regelmäßig aktualisierten Gefährdungsindikatoren (Indicators of Compromise, IOCs) und praktisch umsetzbarem Kontext. So erhalten Sie Einblicke in Cyberangriffe und können den Zweck, die Funktionen und die Ziele der Angreifer ermitteln. Führende SIEM-Systeme (einschließlich HP ArcSight, IBM QRadar, Splunk usw.) werden vollständig unterstützt;
- Entwickeln oder verbessern Sie den **Malware-Schutz für Geräte am Netzwerkrand** (wie z. B. Router, Gateways und UTM-Appliances);
- **Verbessern und beschleunigen Sie Ihre Vorfallsreaktion und forensischen Fähigkeiten,** indem Sie Ihren Sicherheits- bzw. SOC-Teams Zugriff auf relevante Bedrohungsinformationen sowie globale Erkenntnisse über die Hintergründe gezielter Angriffe bereitstellen. Diagnostizieren und analysieren Sie Sicherheitsvorfälle auf Hosts und im Netzwerk effizienter und wirkungsvoller. Priorisieren Sie Signale von internen Systemen gegenüber unbekannten Bedrohungen, verkürzen Sie so die Vorfallsreaktionszeit, und unterbrechen Sie die Kill Chain, bevor entscheidende Systeme und Daten in Mitleidenschaft gezogen werden;
- **Stellen Sie Unternehmensnutzern Bedrohungsinformationen bereit**. Nutzen Sie Informationen aus erster Hand zu aufkommender Malware und anderen Bedrohungen, **um Ihre Verteidigung präventiv zu stärken und Vorfälle zu vermeiden;**
- **Helfen Sie bei der Abwehr gezielter Angriffe**. Verstärken Sie Ihre Sicherheitsstellung durch taktische und strategische Bedrohungsinformationen, indem Sie Verteidigungsstrategien an die spezifischen Bedrohungen anpassen, mit denen Ihr Unternehmen konfrontiert ist;
- Nutzen Sie Bedrohungsinformationen zur Erkennung **schädlicher Inhalte, die in Ihren Netzwerken und Rechenzentren gehostet werden;**
- **Verhindern Sie die Extraktion vertraulicher Assets und geistigen Eigentums** über infizierte Geräte an Personen außerhalb des Unternehmens. Dank der schnellen Erkennung infizierter Assets vermeiden Sie den Verlust von Wettbewerbsvorteilen und Geschäftschancen und schützen den Ruf Ihres Unternehmens;
- Durchsuchen Sie Gefährdungsindikatoren, wie z. B. C&C-Protokolle, IP-Adressen, schädliche URLs oder Datei-Hashes mit von Experten validiertem Bedrohungskontext. Dieser ermöglicht es Ihnen, Angriffe zu priorisieren, vereinfacht Entscheidungen zu IT-Ausgaben und -Ressourcenverteilung und **unterstützt Sie dabei, sich auf die Abwehr der Bedrohungen zu konzentrieren, die das größte Risiko für Ihr Unternehmen darstellen;**
- Nutzen Sie unsere Expertise und praktisch umsetzbaren Kontextinformationen **zur Verbesserung Ihrer Produkte und Services** , wie z. B. Inhaltsfilterung, Blockierung von Spam/Phishing usw;
- **Erweitern Sie als MSSP** Ihr Business, indem Sie Ihren Kunden branchenführende Bedrohungsinformationen als Premiumservice bieten. **Als CERT** können Sie Ihre Fähigkeiten rund um die Erkennung und Identifizierung von Bedrohungen verbessern und erweitern.

# Kaspersky CyberTrace

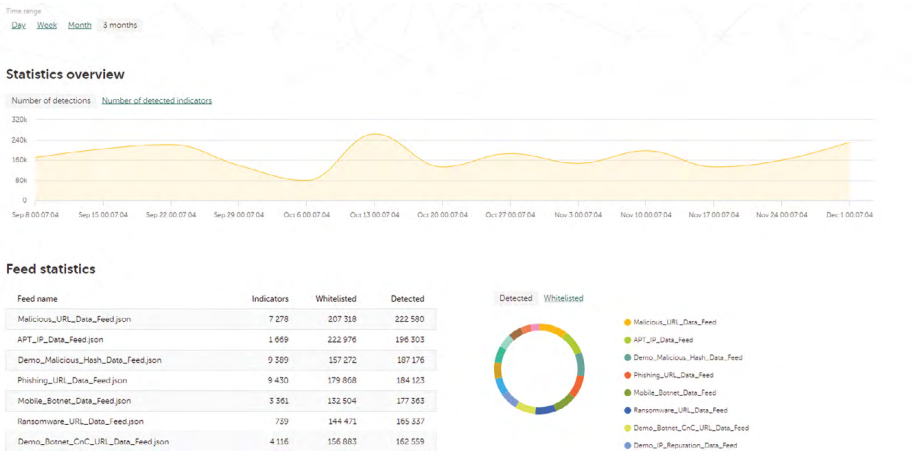
Die Anzahl der Sicherheitswarnungen, die Analysten in Security Operations Centers (SOC) täglich bearbeiten müssen, wächst exponentiell. Angesichts dieser riesigen Datenmengen ist eine effektive Priorisierung, Auswahl und Validierung der Warnungen nahezu unmöglich. Permanent zeigen die zahlreichen Sicherheitsprodukte neue Benachrichtigungen an – bis zu dem Punkt, an dem wichtige Alarme in 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. Analysten an vorderster Front – sogenannte Tier 1 Analysts – sind jedoch auch mit entsprechenden Systemen oft 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, 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 3. Statistiken von Kaspersky CyberTrace**



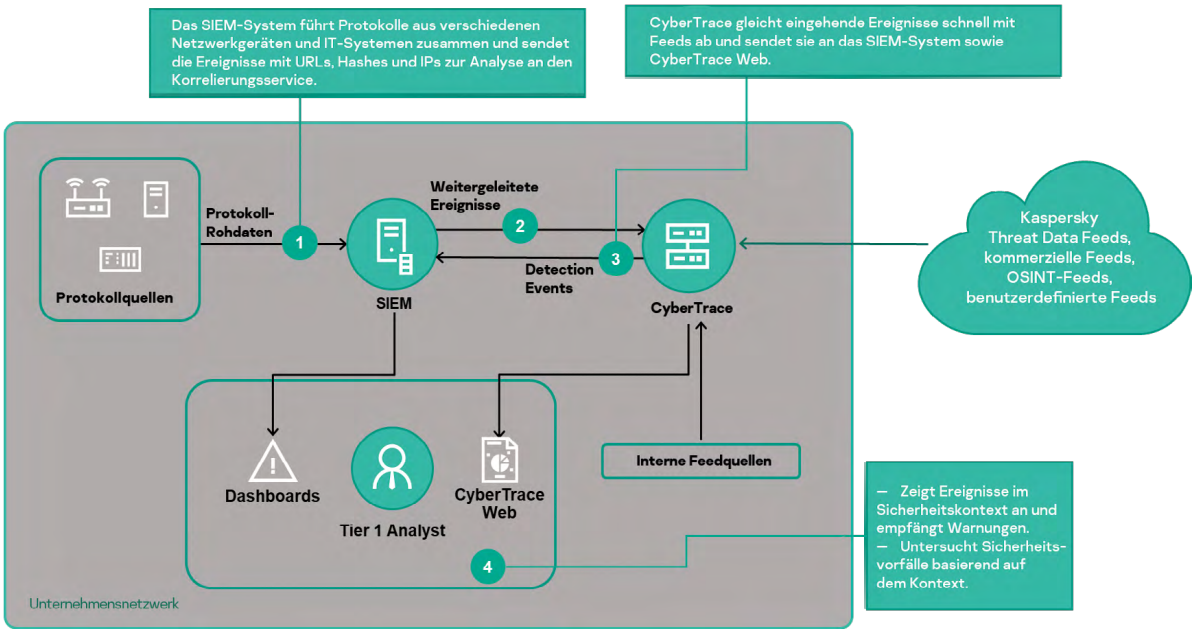

Kaspersky CyberTrace bietet verschiedene Tools, um Bedrohungsinformationen optimal zu nutzen und eine effektive Auswahl von bzw. Reaktion auf Sicherheitswarnungen zu ermöglichen:

- Bereits enthaltene Demo-Bedrohungsfeeds von Kaspersky 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 4: Integrationsschema von Kaspersky CyberTrace**




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 APT Intelligence Reporting bietet Ihnen Folgendes:**

- **Exklusiver Zugriff** auf die technischen Details aktueller Bedrohungen noch während der Untersuchung und vor der Veröffentlichung.
- **Einblicke in nicht öffentliche APTs:** Nicht alle komplexen Bedrohungen werden öffentlich bekannt gemacht. Einige von ihnen werden aufgrund der Angriffsziele, der Vertraulichkeit der Daten, der Art und Weise, auf die die Schwachstellen geschlossen werden, oder der zugehörigen Strafverfolgungsmaßnahmen nie veröffentlicht. Aber die Details werden unseren Kunden mitgeteilt.
- **Detaillierter Zugriff auf technische Daten.** Dies beinhaltet eine umfangreiche Liste von Gefährdungsindikatoren (Indicators of Compromise, IOCs), die in Standardformaten wie OpenIOC oder STIX bereitgestellt werden, sowie Zugriff auf unsere Yara-Regeln.
- **Profile von Bedrohungsakteuren** mit zusammengefassten Informationen zum jeweiligen Bedrohungsakteur, einschließlich vermutetem Herkunftsland und Hauptaktivität, verwendeter Malware-Familien, angegriffener Branchen und Regionen sowie Beschreibungen aller verwendeten HTTP-Adressen und deren Zuordnung zum MITRE ATT&CK-Framework.
- **MITRE ATT&CK.** Alle in den Berichten beschriebenen HTTP-Adressen werden dem MITRE ATT&CK-Framework zugeordnet. Dies ermöglicht eine verbesserte Erkennung und Reaktion durch die Entwicklung und Priorisierung der entsprechenden Anwendungsbereiche der Sicherheitsüberwachung, Schwachstellenanalysen und die Überprüfung der aktuellen Schutzmaßnahmen gegen relevante TTPs.
- **Kontinuierliche Überwachung von APT-Kampagnen:** Zugriff auf praktisch nutzbare Informationen noch während der Untersuchung (Information über die APT-Verteilung, IOCs, C&C-Infrastruktur).
- **Nachträgliche Analyse:** Zugriff auf alle zuvor herausgegebenen privaten Berichte während der Abolaufzeit.
- **RESTful-API** für nahtlose Integration und Automation Ihrer Sicherheitsworkflows.

# APT Intelligence Reporting

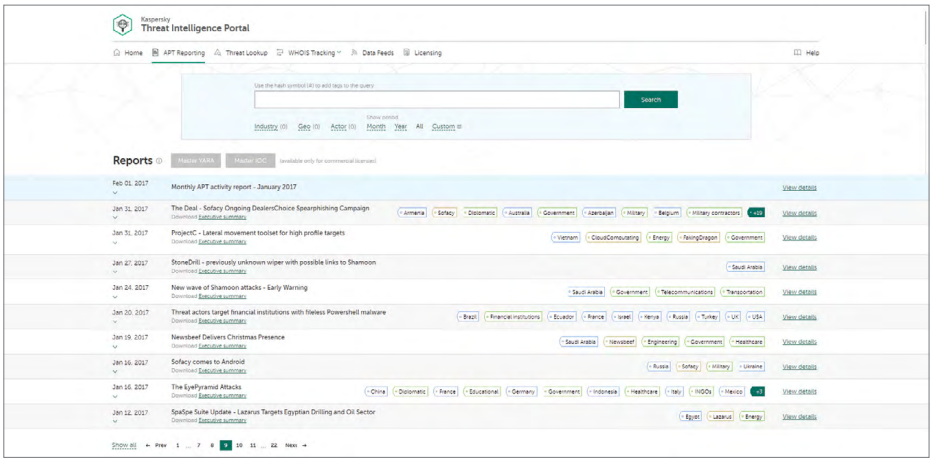
Verbessern Sie das Bewusstsein für und Wissen über hochentwickelte Cyberspionage-Kampagnen durch umfassende, praxisorientierte Berichte von Kaspersky.

Mit den Informationen in diesen Berichten können Sie schnell auf neue Bedrohungen und Schwachstellen reagieren, indem Sie Angriffe über bekannte Vektoren abblocken, den durch hoch entwickelte Angriffe angerichteten Schaden reduzieren und Ihre Sicherheitsstrategie oder die Ihrer Kunden erweitern.

Kaspersky hat einige der bedeutendsten APT-Angriffe aller Zeiten entdeckt. Nicht alle neu entdeckten APTs werden jedoch umgehend gemeldet– viele von ihnen werden sogar nie veröffentlicht.

Als Abonnent von Kaspersky APT Intelligence Reporting erhalten Sie exklusiven Zugang zu unseren Forschungsergebnissen und Erkenntnissen, einschließlich der vollständigen technischen Details in unterschiedlichen Formaten zu jedem APT, noch während dieser aufgedeckt wird – inklusive aller Bedrohungen, die nie veröffentlicht werden. Jeder der Berichte enthält Zusammenfassungen, die sich an C-Level-Mitarbeiter richten und einfach verständliche Informationen zum entsprechenden APT enthalten. Der Zusammenfassung folgt eine ausführliche technische Beschreibung des APT mit zugehörigen IOCs und Yara-Regeln. So erhalten Sicherheitsforscher, Malware-Analysten, Sicherheitstechniker, Netzwerkanalysten und APT-Experten praktisch umsetzbare Informationen für eine präzise Reaktion auf entsprechende Bedrohungen.

Unsere Experten, die zu den erfolgreichsten APT-Jägern der Branche zählen, halten Sie zudem über Änderungen in der Taktik von Cyberkriminellen auf dem Laufenden. Außerdem erhalten Sie Zugriff auf unsere vollständige Datenbank mit APT-Berichten – eine weitere effektive Recherche- und Analysequelle, die Sie zur Verteidigung Ihres Unternehmens nutzen können.




# Digital Footprint Intelligence

Ihr Unternehmen wächst. Aber gleichzeitig nimmt auch die Komplexität Ihrer verteilten IT-Umgebung zu; eine große Herausforderung, wenn es darum geht, Ihre weit verteilte digitale Präsenz ohne direkte Kontrolle oder entsprechende Zuständigkeiten zu schützen. Dank dynamischer und verbundener Umgebungen können Unternehmen erheblichen Nutzen aus der Optimierung ihrer Prozesse, erhöhter Produktqualität, einem besseren Kundeneindruck und einer gestärkten Wettbewerbsposition ziehen. Gleichzeitig bietet die wachsende Konnektivität eine immer größer werdende Angriffsfläche. Und da die Angreifer immer raffinierter werden, brauchen Sie nicht nur einen präzisen Einblick in die Online-Präsenz Ihrer Organisation, sondern müssen auch Veränderungen nachverfolgen können und zeitnah über Ihre online zugänglichen digitalen Werte informiert werden.

Auch wenn Organisationen bereits eine breite Palette an Sicherheitstools einsetzen, sind sie noch lange nicht vor jeder digitalen Bedrohung geschützt: Funktionen zur Erkennung und Eindämmung von Insider-Aktivitäten, Pläne und Angriffsszenarien von Cyberkriminellen in Darknet-Foren etc. Damit Sicherheitsanalysten Unternehmensressourcen aus dem Blickwinkel des Gegners betrachten, potentielle Angriffsvektoren schnell erkennen und ihre Verteidigungsstrategie entsprechend ausrichten können, hat Kaspersky die Kaspersky Digital Footprint Intelligence entwickelt.

Was wäre die beste Methode, einen Angriff gegen Ihr Unternehmen zu starten? Wie kann man Ihre Organisation am kostengünstigsten angreifen? Welche Informationen stehen einem Angreifer, der es auf Sie abgesehen hat, zur Verfügung? Ist Ihre Infrastruktur bereits gefährdet?

Unsere Digital Footprint Intelligence beantwortet diese und weitere Fragen. Unsere Experten erstellen dazu ein umfassendes Bild Ihrer aktuellen Gefährdungslage, zeigen Schwachstellen auf, die mit großer Wahrscheinlichkeit genutzt werden, und weisen ggf. bereits stattgefundene bzw. geplante Angriffe nach.

Das Modul wurde auf der Grundlage von OSINT-Techniken in Kombination mit automatisierten und manuellen Analysen des öffentlichen Internets, Deep Web und Dark Web entwickelt. Zusammen mit der internen Kaspersky-Wissensdatenbank bieten die daraus resultierenden maßgeschneiderten Berichte praktisch umsetzbare Einblicke und Handlungsempfehlungen, mit denen Sie die Zahl der potentiellen Angriffsvektoren und das Risiko einer digitalen Gefährdung minimieren können. Dazu zählen:

- Netzwerkperimeter-Bestandsaufnahme ohne Störung des laufenden Betriebs, um zu ermitteln, welche kundenseitigen Netzwerkressourcen und offen zugänglichen Services potentielle Angriffspunkte bieten. Dazu gehören unter anderem versehentlich im Perimeter belassene Verwaltungsschnittflächen oder unzureichend konfigurierte Services, Geräteschnittstellen etc.
- Maßgeschneiderte Analyse der vorhandenen Schwachstellen mit Bewertung und umfassender Risikoeinstufung nach CVSS-Schweregrad, Verfügbarkeit von öffentlichen Exploits, Penetration Testing und Standort von Netzwerkressourcen (Hosting/Infrastruktur).
- Identifizierung, Überwachung und Analyse aller aktiven oder geplanten zielgerichteten Angriffe auf Ihr Unternehmen, Ihre Branche oder Region abzielende APT-Kampagnen.
- Die Erkennung von Bedrohungen, die sich speziell gegen Ihre Kunden, Partner und Abonnenten richten, deren infizierte Systeme dann für Angriffe auf Ihr Unternehmen genutzt werden könnten.
- Diskrete Überwachung von Pastebin-Seiten, öffentlichen Foren, sozialen Netzwerken, Instant-Messaging-Kanälen, im Untergrund tätige, geheime Online-Foren und -Communitys; Ermittlung von möglicherweise gefährdeten Konten, Datenlecks oder Angriffen auf Ihre Organisation, die in diesem Foren geplant und diskutiert werden.

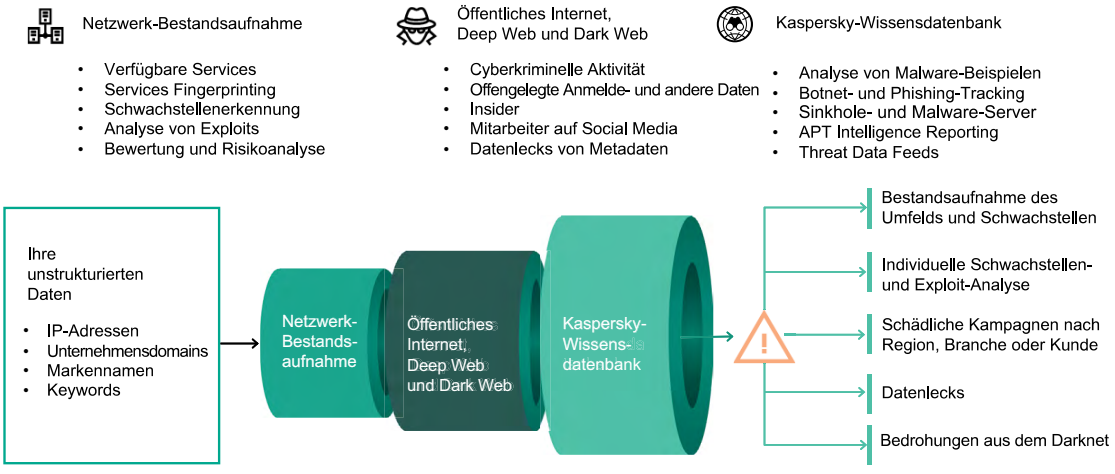
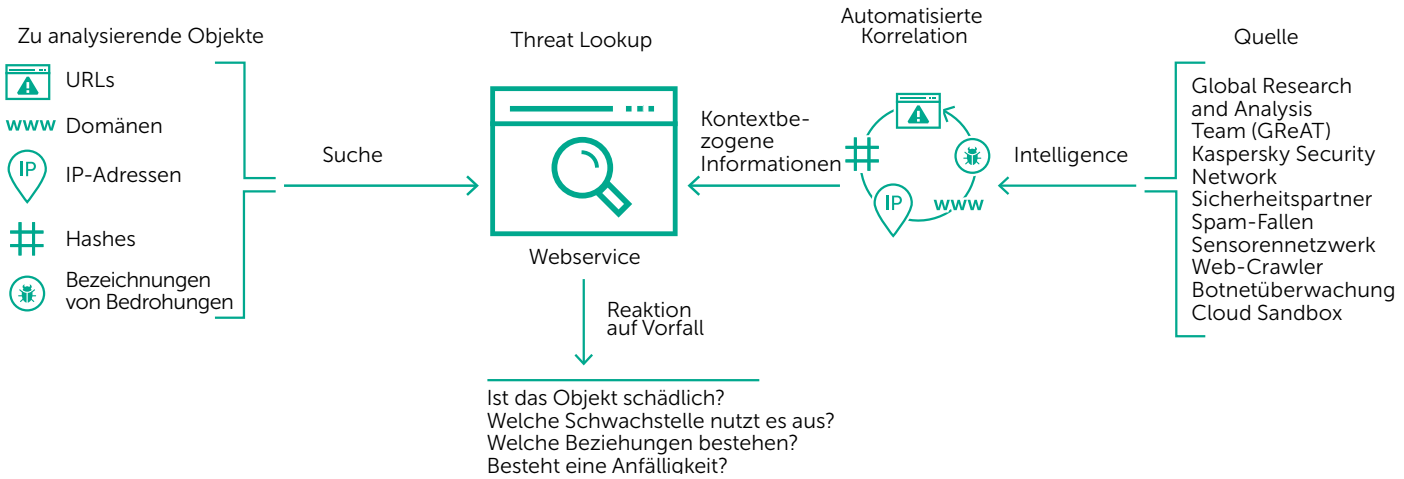



**Abbildung 1. Kaspersky Digital Footprint Intelligence**

## Schneller Einstieg – einfache Anwendung – keine Ressourcen erforderlich

Kaspersky Digital Footprint Intelligence hat keinerlei Auswirkungen auf die Integrität und Verfügbarkeit Ihrer Netzwerkressourcen und -services. Die Berichte werden im Kaspersky Threat Intelligence Portal bereitgestellt, wo wir alle Bedrohungsdaten aus mehr als 20 Jahren gesammelt haben. Darüber hinaus werden Sie sofort benachrichtigt, sobald neue Informationen zur Verfügung stehen. Per API lässt sich Kaspersky Digital Footprint Intelligence auch in die Task Management-Systeme von Drittanbietern integrieren, was den zur Workflow-Verwaltung erforderlichen zeitlichen Aufwand erheblich reduziert.

# Threat Lookup




### Service-Highlights

- **Vertrauenswürdige Informationen:** Ein zentraler Bestandteil von Kaspersky Threat Lookup ist die Zuverlässigkeit unserer Bedrohungsinformationen, die durch einen praktisch umsetzbaren Kontext ergänzt werden. Kaspersky-Produkte zählen zu den führenden bei Anti-Malware-Tests[1]. Die hohen Erkennungsraten mit Fehlalarmquoten, die praktisch gegen Null gehen, zeigen die Zuverlässigkeit unserer Sicherheitsinformationen.
- **Threat Hunting:** Gehen Sie bei der Prävention, Erkennung und Reaktion auf Angriffe proaktiv vor, um deren Auswirkung und Häufigkeit zu minimieren. Erkennen und beenden Sie Angriffe so früh wie möglich. Je früher Sie eine Bedrohung entdecken, umso weniger Schaden entsteht, umso schneller können Korrekturmaßnahmen stattfinden und umso eher kann sich der Netzwerkbetrieb normalisieren.
- **Sandbox-Analyse:** Dabei werden unbekannte Bedrohungen durch die Ausführung von verdächtigen Objekten in einer abgesicherten Umgebung erkannt sowie das gesamte Bedrohungsverhalten mitsamt der Artefakte in leicht verständlichen Berichten überprüft.
- **Breite Pallette an Exportformaten:** Exportieren Sie die Gefährdungsindikatoren (Indicators of Compromise, IOCs) oder den praktisch umsetzbaren Kontext in gängige, strukturiertere und computerlesbare Formate, z. B. STIX, OpenIOC, JSON, Yara, Snort oder sogar CSV, um alle Vorteile von Bedrohungsinformationen nutzen zu können, betriebliche Workflows zu automatisieren oder eine Integration in bestehende Sicherheitskontrollen, z. B. SIEMs, zu ermöglichen.
- **Benutzerfreundliche Weboberfläche oder RESTful API:** Sie können auf diesen Service manuell über eine Web-Oberfläche (über einen Browser) oder über eine einfache RESTful-API zugreifen.

Cyberkriminalität entwickelt sich mit dem technologischen Fortschritt und kennt heute kaum noch Grenzen. Wir beobachten Cyberangriffe, die immer raffinierter werden, und Cyberkriminelle, die für ihre Angriffe zunehmend Ressourcen aus dem Dark Web einsetzen. Cyberbedrohungen werden immer häufiger, komplexer und schwerer erkennbar. Zuverlässige Abwehrmaßnahmen zu finden, wird zunehmend schwieriger. Die Angreifer nutzen dabei komplizierte „Kill Chains" und individuelle Taktiken, Techniken und Abläufe (Tactics, Techniques and Procedures, TTPs), um Ihre Geschäftsabläufe zu stören, Ihre Vermögenswerte zu entwenden oder Ihren Kunden zu schaden.

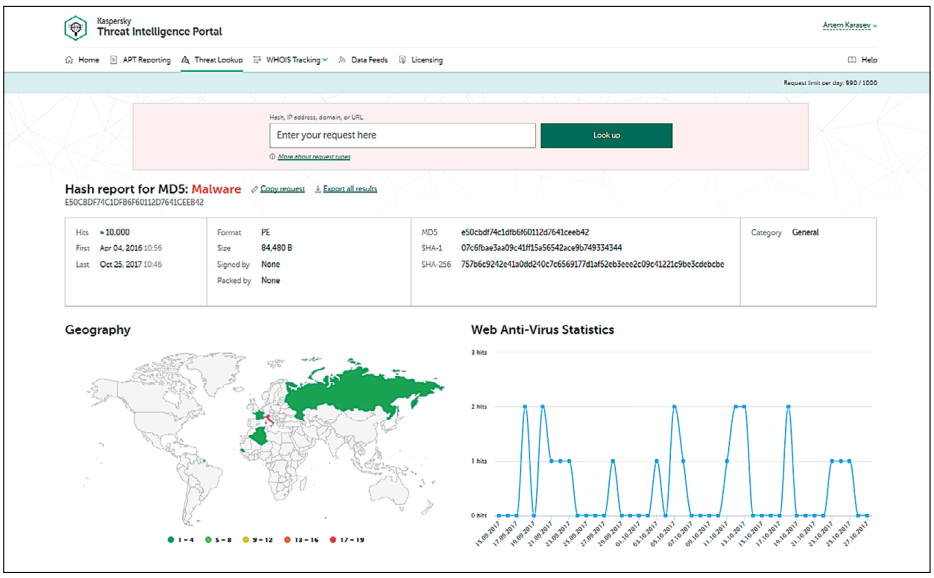
Kaspersky Threat Lookup bietet unser gesamtes Wissen über Cyberbedrohungen und ihre Abhängigkeiten in einem einzigen, leistungsstarken Webservice. Das Ziel ist es, Sie und Ihre Sicherheitsteams mit so vielen Informationen wie möglich zu versorgen, damit Cyberangriffe schon im Vorfeld abgewendet werden können. Die Plattform ruft die neuesten detaillierten Bedrohungsdaten ab zu URLs, Domänen, IP-Adressen, Hash-Werten, Namen von Bedrohungen, statistische/Verhaltensdaten, WHOIS/DNS-Daten, Dateiattribute, geographische Standortdaten, Downloadketten, Zeitstempel etc. Im Ergebnis erhalten Sie eine weltweite Übersicht über neue und sich entwickelnde Bedrohungen, damit Sie Ihre Organisation schützen und die Vorfallsreaktion beschleunigen können.

Die von Kaspersky Threat Lookup bereitgestellten Bedrohungsinformationen werden in Echtzeit über eine äußerst fehlertolerante Infrastruktur generiert und überwacht, die kontinuierliche Verfügbarkeit und ein gleichbleibendes Leistungsniveau gewährleistet. Hunderte von Experten, darunter Sicherheitsanalysten aus der ganzen Welt, weltweit anerkannte Sicherheitsexperten aus unserem GReAT-Team und führende Forschungs- und Entwicklungsteams, tragen gemeinsam zur Bereitstellung von wertvollen und praxisnahen Bedrohungsinformationen bei.

## Hauptvorteile

- **Verbessern und beschleunigen Sie Ihre Vorfallsreaktion und forensischen Funktionen,** indem Sie Ihren Sicherheits-/SOC-Teams Zugriff auf relevante Bedrohungsinformationen sowie globale Erkenntnisse über die Hintergründe von gezielten Angriffen bereitstellen. Diagnostizieren und analysieren Sie Sicherheitsvorfälle auf Hosts und im Netzwerk effizienter und wirkungsvoller. Priorisieren Sie Signale von internen Systemen gegenüber unbekannten Bedrohungen, verkürzen Sie so die Vorfallsreaktionszeit und unterbrechen Sie die Kill Chain, bevor entscheidende Systeme und Daten in Mitleidenschaft gezogen werden.
- **Führen Sie anhand hochzuverlässiger Bedrohungskontexte** detaillierte Suchen innerhalb der Bedrohungsindikatoren aus, z. B. in IP-Adressen, URLs, Domänen oder Datei-Hashes, um Angriffe zu priorisieren, Entscheidungen über Personal- und Ressourcenzuteilungen zu verbessern und sich auf die Abwehr derjenigen Bedrohungen zu konzentrieren, die das größte Risiko für Ihr Unternehmen darstellen.
- **Wehren Sie gezielte Angriffe ab.** Verbessern Sie mithilfe taktischer und strategischer Bedrohungsinformationen Ihre Sicherheitsinfrastruktur, indem Sie die richtigen Verteidigungsstrategien einsetzen.

1 http://www.kaspersky.com/top3




## Jetzt können Sie

- über eine webbasierte Benutzeroberfläche oder die RESTful-API nach Bedrohungsindikatoren suchen.
- nachvollziehen, warum ein Objekt als schädlich eingestuft wird.
- überprüfen, ob ein entdecktes Objekt weit verbreitet ist oder nur vereinzelt vorkommt.
- zusätzliche Details überprüfen, darunter Zertifikate, häufig genutzte Bezeichnungen, Dateipfade oder zugehörige URLs, um neue verdächtige Objekte zu ermitteln.

Dies sind nur einige Beispiele. Es gibt noch eine Vielzahl weiterer Möglichkeiten, diese relevanten und fein abgestuften Sicherheitsinformationen zu nutzen.

Kenne deine Feinde und deine Freunde. Erkennen Sie nachgewiesen unschädliche Dateien, URLs und IP-Adressen und beschleunigen Sie den Untersuchungsvorgang. Wenn jede Sekunde zählt, sollten Sie keine Zeit mit der Analyse von vertrauenswürdigen Objekten verlieren.

Unser Ziel ist es, alle Arten von Cyberbedrohungen abzuwehren und die digitale Welt unserer Kunden sicherer zu machen. Um das zu erreichen und die Nutzung des Internets sicher zu machen, müssen Bedrohungsinformationen in Echtzeit weitergegeben und verwendet werden können. Ein zeitnaher Zugriff auf Informationen ist für einen effektiven Schutz Ihrer Daten und Netzwerke unerlässlich. Jetzt können Sie mit Kaspersky Threat Lookup effizienter und einfacher denn je auf diese Daten zugreifen.

**Wichtige Funktionen**

- Geladene und ausgeführte DLLs
- Erstellte gemeinsame Erweiterungen (Mutexes)
- Geänderte und erstellte Registrierungsschlüssel
- Externe Verbindungen mit Domainnamen und IP-Adressen
- HTTP- und DNS-Anfragen und -Antworten
- Von der ausgeführten Datei erstellte Prozesse
- Erstellte, geänderte und gelöschte Dateien
- Verarbeitete Speicherauszüge und Netzwerkverkehr-Dumps (PCAP)
- Screenshots
- Detaillierte Bedrohungsinformationen mit umsetzbarem Kontext für jeden aufgedeckten Gefährdungsindikator (IOC)
- RESTful-API
- Und vieles mehr

**Hauptvorteile:**

- Fortschrittliche Erkennung von APTs, gezielten und komplexen Bedrohungen
- Ein Workflow, der die Durchführung hocheffektiver und komplexer Vorfallsuntersuchungen ermöglicht
- Skalierbarkeit, ohne dass Sie kostspielige Hardware erwerben oder Systemressourcen verwalten müssen
- Nahtlose Integration und Automatisierung Ihrer Sicherheitsabläufe

# Cloud Sandbox

Herkömmliche Antivirentools reichen heutzutage nicht mehr aus, um gezielte Angriffe zu verhindern. Virenschutz-Engines können nur bekannte Bedrohungen in verschiedenen Varianten abwehren. Versierte Bedrohungsakteure nutzen jedoch alle ihnen zur Verfügung stehenden Mittel, um eine automatische Erkennung zu umgehen. Verluste durch Zwischenfälle in der IT-Sicherheit steigen weiterhin exponentiell. Dadurch gewinnen Funktionen zur sofortigen Erkennung von Bedrohungen an Bedeutung, um eine schnelle Reaktionsfähigkeit aufzubauen und Bedrohungen entgegenzuwirken, bevor erhebliche Schäden entstehen können.

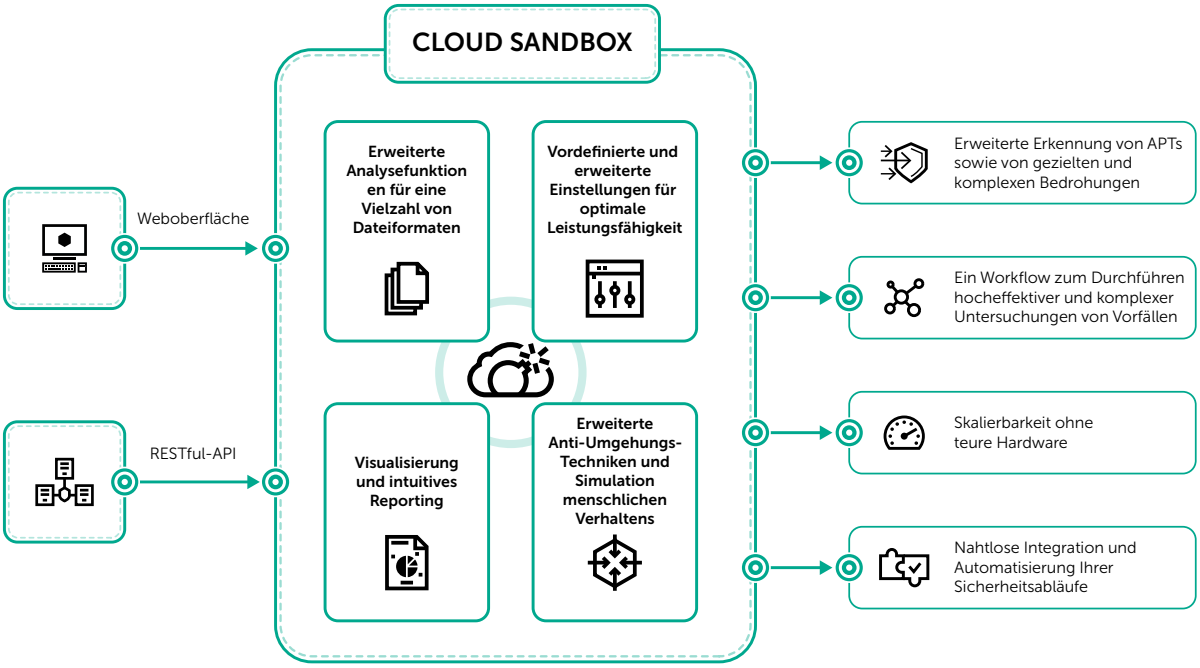
Intelligente Entscheidungen auf Basis von Dateiverhalten zu treffen und zugleich etwa den Prozess-Arbeitsspeicher, die Netzwerkaktivität usw. zu analysieren, ist der optimale Ansatz, um ausgeklügelte, gezielte und maßgeschneiderte Bedrohungen von heute zu erfassen. Während es statistischen Daten häufig an Informationen zu kürzlich modifizierter Malware fehlt, bieten Sandboxing-Technologien leistungsstarke Tools, die die Untersuchung der Herkunft von Dateiproben, die Erfassung von IOCs auf Basis von Verhaltensanalysen sowie die Erkennung schädlicher Objekte ermöglichen, die normalerweise nicht erkannt würden.

## Proaktive Abwehr von Bedrohungen, die Sicherheitsbarrieren umgehen

Heutzutage kommt bei Malware eine Vielzahl von Methoden zum Einsatz, um die Ausführung des eigenen Codes zu vermeiden, wenn dies zur Aufdeckung der schädlichen Aktivität führen könnte. Wenn das System die erforderlichen Parameter nicht erfüllt, zerstört sich das schädliche Programm selbst, ohne Spuren zu hinterlassen. Damit der Schadcode ausgeführt werden kann, muss die Sandboxing-Umgebung daher in der Lage sein, ein normales Nutzerverhalten genau nachzuahmen.

Kaspersky Cloud Sandbox bietet einen hybriden Ansatz und kombiniert dabei Bedrohungsinformationen aus statistischen Daten im Petabyte-Bereich (dank des Kaspersky Security Network und anderen unternehmenseigenen Systemen), Verhaltensanalysen und besonders robuste Anti-Umgehungs-Techniken mit menschlichen Simulationstechnologien wie Auto-Clickern, Dokumentscrolling und Dummy-Prozessen. Das Ergebnis ist eine optimale Umgebung für die Erkennung unbekannter Bedrohungen.

Dieser Service geht unmittelbar aus unserem hauseigenen Sandboxing-Komplex hervor, den wir seit über 10 Jahren stetig weiterentwickeln. Diese Technologie beinhaltet das gesamte Wissen über das Malware-Verhalten, das wir uns während 20 Jahren kontinuierlicher Bedrohungsforschung angeeignet haben. So können wir täglich über 350.000 neue schädliche Objekte erkennen und branchenführende Sicherheitslösungen für unsere Kunden bereitstellen.




Kaspersky Cloud Sandbox ist Teil des Kaspersky Threat Intelligence Portal und ergänzt Ihren Threat Intelligence Workflow. Während Threat Lookup aktuelle, detaillierte Bedrohungsinformationen zu URLs, Domains, IP-Adressen, Datei-Hashes, Bedrohungsnamen, Statistik-/Verhaltensdaten und WHOIS-/DNS-Daten abruft, ermöglicht Cloud Sandbox die Verknüpfung dieses Wissens mit den IOCs, die anhand der analysierten Probe generiert wurden.

Jetzt können Sie hochwirksame und komplexe Vorfalluntersuchungen durchführen, um ein sofortiges Verständnis der Art der Bedrohung zu gewinnen und zusammenhängende Bedrohungsindikatoren aufzudecken.

Untersuchungen können äußerst ressourcenintensiv ausfallen, insbesondere bei mehrstufigen Angriffen. Kaspersky Cloud Sandbox ist ein ideales Tool zur Beschleunigung der Reaktion auf Zwischenfälle sowie forensische Aktivitäten. So profitieren Sie von Skalierbarkeit für die automatische Verarbeitung von Dateien, ohne kostspielige Hardware zu erwerben oder sich Gedanken über Systemressourcen zu machen.

# Kaspersky Threat Hunting

**Sicherheitsteams in allen Branchen arbeiten kontinuierlich daran, Systeme aufzubauen, die umfassenden Schutz vor sich immer schneller entwickelnden Cyberbedrohungen bieten. Die meisten dieser Systeme nutzen jedoch einen reaktiven „Benachrichtigungsansatz" bei Cybersicherheitsvorfällen: 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 ermittelt 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.**

**Kaspersky Cybersecurity Services**

- **Kaspersky Threat Intelligence**
- **Kaspersky Threat Hunting**
  Kaspersky Managed Protection
  Targeted Attack Discovery
- **Kaspersky Cybersecurity Training**
- **Kaspersky Incident Response**
- **Kaspersky Security Assessment**

## Kaspersky Managed Protection

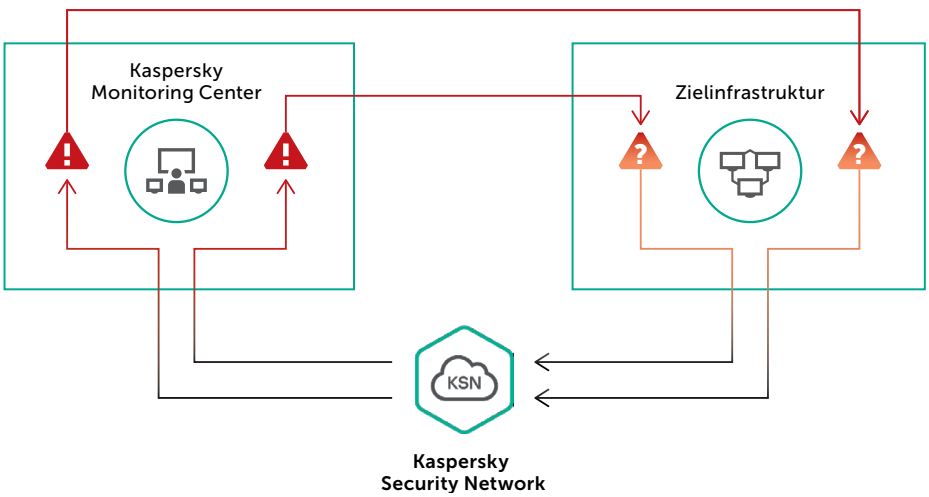
Kaspersky Managed Protection bietet Nutzern von Kaspersky Endpoint Security und Kaspersky Anti Targeted Attack Platform einen vollständig verwalteten Service, der eine einzigartige Kombination aus Technologien zur Erkennung und Vermeidung gezielter Angriffe bietet. Der Service umfasst die Überwachung 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 Non-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 Bedrohungsuntersuchung, einschließlich der von den Angreifern gegen Ihr Unternehmen eingesetzten Methoden und Technologien.
- Integrierter Ansatz – das Portfolio von Kaspersky beinhaltet sämtliche Technologien und Services, die Sie für die Implementierung eines vollständigen Zyklus für den Schutz vor gezielten Angriffen benötigen:

**Servicevorteile**

- Schnellere und effektivere Abwehr dank umgehender und effizienter Erkennung.
- Keine Zeitverschwendung 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.



### Der Service im Detail

Die Erkennung gezielter Angriffe von Kaspersky umfasst die folgenden Maßnahmen:

**Sammeln und Analysieren von Daten zu Angriffen mit externem Ursprung.** Das Ziel dieser Phase ist es, eine Momentaufnahme der Schwachstellen von Unternehmen zu erhalten, die von Eindringlingen angegriffen werden oder zuvor angegriffen wurden. Zu diesem Zweck greifen wir auf verschiedene Informationsquellen zu, darunter Untergrund-Communities von Cyberkriminellen, und überwachen Ihre Umgebung mithilfe von internen Kaspersky-Überwachungssystemen. Durch die Analyse dieser Informationen können wir Schwachstellen in der Infrastruktur eines Unternehmens identifizieren, über die Cyberkriminelle Konten hacken, Daten stehlen und vieles mehr tun können.

**Datenerfassung vor Ort.** In dieser Phase werden Daten von Workstations, Servern, SIEM-Systemen und anderen Geräten in der Infrastruktur des Kunden erfasst. Einige der Daten werden mithilfe von Software erfasst, die dem Kunden im Rahmen des Service bereitgestellt wird.

**Datenanalyse.** Die Experten von Kaspersky verwenden die in der vorherigen Phase gesammelten Daten zur Identifizierung von Vorfällen im Unternehmensnetzwerk. Der Hauptzweck dieser Phase besteht darin, die Art des Vorfalls zu bestimmen und dessen Auswirkungen auf die Infrastruktur zu bewerten, um entsprechende Abhilfemaßnahmen zu implementieren. Zu diesem Zeitpunkt werden Daten aus Workstation-Protokollen, Netzwerkaktivitätsdaten und andere kontextbezogene und Verlaufsdaten verwendet. Es werden keine zusätzlichen Daten direkt von kompromittierten Systemen gesammelt.

**Frühzeitige Incident Response.** Zu diesem Zeitpunkt stellen wir erste Empfehlungen für die anfängliche Vorfallsreaktion bereit. In einigen Fällen benötigen die Kaspersky-Experten zur Bestätigung und Klassifizierung eines Vorfalls zusätzliche Daten, etwa verschiedene Dateien von Betriebssystemen, Programmen und Netzwerkgeräten, Netzwerkverkehr-Dumps, Festplatten-Images, Speicherauszüge oder andere Datentypen. Der Kunde wird möglicherweise gebeten, zusätzliche Daten bereitzustellen (per E-Mail oder über verschiedene Netzwerkressourcen, je nach Art und Menge der angeforderten Daten).

**Berichterstellung.** Die im Rahmen des Service durchgeführten Arbeiten werden in einem Abschlussbericht gemeinsam erfasst. Dieser enthält die Ergebnisse der Datenanalyse aus externen Quellen sowie Beschreibungen erkannter Angriffe auf der Grundlage der Analyse der in der Infrastruktur des Kunden erfassten Daten. Zudem enthält der Bericht Empfehlungen für die Behebung der erkannten Angriffe.

### Zusätzliche Services

Unsere Experten unterstützen Sie auch dabei, die Symptome eines Vorfalls zu analysieren, tief greifende digitale Analysen für bestimmte Systeme 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.

# Targeted Attack Discovery

Experten von Kaspersky 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 so erhalten Sie folgende Informationen:

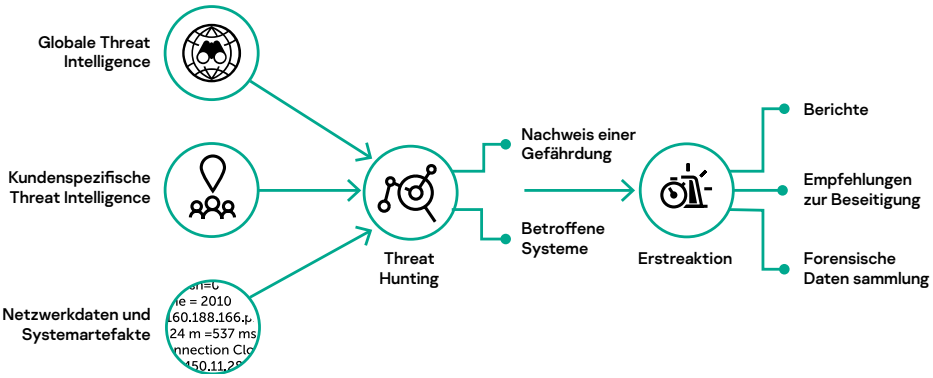
- Ob, wie und von wem Sie derzeit angegriffen werden
- Wie sich dieser Angriff auf Ihre Systeme auswirkt, und wie Sie sich wehren können
- Wie Sie zukünftige Angriffe vermeiden

## Und so funktioniert es

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
- Analysieren von aktuellen 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:

- **Allgemeine Informationen,** die bestätigen, dass Ihr Netzwerk gefährdet wurde, oder Anzeichen dafür;
- **Analyse der gesammelten Informationen** zu Bedrohungen und Gefährdungsindikatoren (IOC);
- **Beschreibung möglicher Angriffsquellen** und gefährdeter Netzwerkkomponenten;
- **Empfehlung von Abhilfemaßnahmen,** um Auswirkungen durch Zwischenfälle entgegenzuwirken und um Ihre Ressourcen in Zukunft vor ähnlichen Angriffen zu schützen.

# Kaspersky Cybersecurity Training

**Sicherheitsschulungen sind angesichts der zunehmenden Bedrohungslage für Unternehmen unerlässlich. Sicherheitsmitarbeiter müssen in den erweiterten Sicherheitstechniken ausgebildet werden, die eine wichtige Komponente des effektiven Bedrohungsmanagements und der Strategien zur Risikominimierung im Unternehmen bilden.**

**Kaspersky Cybersecurity Services**

- **Kaspersky Threat Intelligence**
- **Kaspersky Threat Hunting**
- **Kaspersky Cybersecurity Training**
  - Windows Digital Forensics
  - Malware-Analyse und Reverse Engineering
  - Advanced Windows Digital Forensics
  - Erweiterte Malware-Analyse und Reverse Engineering
  - Windows Incident Response
  - Effiziente Bedrohungserkennung mit Yara
- **Kaspersky Incident Response**
- **Kaspersky Security Assessment**

Diese Kurse umfassen eine breite Auswahl von Cybersicherheitsthemen und -techniken mit Assessments von der Einsteiger- bis zur Expertenebene. Alle Kurse werden am Kundenstandort oder ggf. in einer lokalen oder regionalen Niederlassung von Kaspersky angeboten.

Die Kurse umfassen sowohl theoretische Lektionen als auch praktische Übungen. Nach Abschluss jedes Kurses können die Teilnehmer ihr Wissen in einem Test prüfen.

## Servicevorteile

### Windows Digital Forensics und Advanced Windows Digital Forensics

Vertieft das Fachwissen Ihres internen Teams für digitale Forensik und Vorfallsreaktion. Teilnehmer dieses Kurses können Erfahrungslücken schließen und ihre praktischen Fertigkeiten bei der Suche nach digitalen Spuren von Cyberkriminalität sowie bei der Analyse verschiedener Datentypen zur Ermittlung des zeitlichen Ablaufs und der Quellen des Angriffs entwickeln und verbessern. Nach Abschluss dieses Kurses können Teilnehmer Computervorfälle erfolgreich untersuchen und die Sicherheit des Unternehmens verbessern.

### Malware-Analyse und Reverse Engineering und Erweiterte Malware-Analyse und Reverse Engineering

Diese Kurse richten sich an Sicherheitsforscher und Vorfallsreaktionsteams, an Malware-Analysten, Sicherheitstechniker, Netzwerksicherheitsanalysten, APT Threat Hunter und IT-Sicherheitsmitarbeiter. Die Teilnehmer erhalten eine Einführung in Reverse Engineering-Programme, Assembly-Sprache, entsprechende Tools, gängige Techniken von Malware-Autoren, um persistent zu bleiben, Erkennungssysteme zu umgehen und in Speicher von Systemprozessen einzudringen etc. Im weiterführenden Kurs geht es darum, wie man ein modernes APT-Toolkit analysiert, vom Erhalt der ersten Probe bis hin zur Erstellung einer weitreichenden technischen Beschreibung mit IOCs.

### Windows Incident Response

Der Kurs führt Ihr Team durch sämtliche Phasen der Vorfallsreaktion und stattet sie mit dem umfassenden Wissen aus, das für eine erfolgreiche Wiederherstellung nach Vorfällen erforderlich ist.

### Effiziente Bedrohungserkennung mit Yara

In diesem Kurs erfahren Sie, wie Sie effektive Yara-Regeln schreiben, testen und so verbessern können, dass sie Bedrohungen finden, die bisher unbekannt blieben.

### Praktische Erfahrung

Von einem der führenden Sicherheitsanbieter, gemeinsames Arbeiten und Lernen zusammen mit unseren globalen Experten, die die Teilnehmer durch ihre eigene Erfahrung im alltäglichen Kampf gegen die Cyberkriminalität inspirieren.

# Programmbeschreibung

| Themen | Dauer | Erlernte Fertigkeiten |
|---|---|---|
| **Windows Digital Forensics** | | |
| Im Rahmen eines realitätsgetreuen simulierten Angriffs aus dem Internet werden folgende Themen behandelt:<br>· Einführung in die digitale Forensik<br>· Live-Reaktion und Erfassung von Beweisen<br>· Post-Mortem-Analyse von Windows-Systemen<br>· Details der Windows-Registrierung<br>· Windows-Ereignisse<br>· Windows-Artefaktanalyse<br>· Browserartefakte in der Forensik<br>· E-Mail-Analyse<br>· Forensische Herausforderungen durch SSD-Festplatten<br>· Empfehlungen für den Aufbau eines digitalen forensischen Labors<br>· Erprobung der neu erworbenen Fähigkeiten mit einer praktischen Herausforderung unter Verwendung verschiedener Windows-Artefakte | 4 Tage | · Beschaffung verschiedener digitaler Beweismittel und Umgang damit in forensischen Umgebungen<br>· Auffinden von Spuren vorfallsbezogener schädlicher Aktivitäten anhand von Artefakten aus dem Windows-Betriebssystem<br>· Verwenden von Zeitstempeln aus verschiedenen Windows-Artefakten zur Rekonstruktion von Vorfallszenarien<br>· Ermitteln und Analysieren von Browser- und E-Mail-Verläufen<br>· Anwenden von Tools und Instrumenten der digitalen Forensik<br>· Prozess zur Erstellung eines digitalen forensischen Labors |
| **Malware-Analyse und Reverse Engineering** | | |
| · Grundlegende Analyse mit IDA Pro<br>· Dynamische Analyse mit gängigen Virtualisierungslösungen und Debuggern<br>· Analyse schadhafter Dokumente<br>· Entpacken<br>· Entschlüsseln<br>· Analyse von Shellcodes<br>· Analyse von Exploits<br>· Tipps und Tricks zum Reverse Engineering | 4 Tage | · Informieren Sie sich grundlegend über Betriebssystem und Assemblersprache.<br>· Führen Sie statische und dynamische Malware-Analysen durch, um ein umfassendes Verständnis des Verhaltens und der Funktionen von Malware zu erlangen.<br>· Kontern Sie Malware-Techniken zur Anti-Analyse, zum Selbstschutz und zur Umgehung von Sicherheitssoftware.<br>· Führen Sie Identifikation und Reverse Engineering von eigenständigen und Embedded Shellcodes durch.<br>· Erfahren Sie, wie Sie PDF-Exploits von Grund auf analysieren. |
| **Advanced Windows Digital Forensics** | | |
| Im Rahmen eines realitätsnahen simulierten Angriffs aus dem Internet werden folgende Themen behandelt:<br>· Numerische Systeme<br>· FAT-Dateisystem<br>· NTFS-Dateisystem<br>· Umfassende Windows-Forensik<br>· Daten- und Dateiwiederherstellung aus Dateisystem, Schattenkopien und Verwendung von File Carving<br>· Forensische Herausforderungen im Cloud Computing<br>· Speicherforensik<br>· Netzwerkforensik<br>· Timeline- und SuperTimeline-Analyse im Vergleich<br>· Überprüfen der neu erworbenen Fähigkeiten im Rahmen einer praktischen Herausforderung durch erfasste digitale Beweismittel | 4 Tage | · Durchführen einer umfassenden Dateisystemanalyse<br>· Identifizieren und Wiederherstellen gelöschter Dateien mithilfe verschiedener Techniken<br>· Analyse des Netzwerkverkehrs mit verschiedenen Tools<br>· Identifizieren und Verfolgen schädlicher Aktivitäten in Speicherauszügen<br>· Identifizieren und Extrahieren interessanter Daten aus dem Arbeitsspeicher zur weiteren Analyse<br>· Rekonstruieren des Vorfallablaufs mit Dateisystem-Zeitstempeln<br>· Erstellen eines Zeitplans für alle Windows-Betriebssystemartefakte für ein besseres Verständnis des Vorfallszenarios |
| **Erweiterte Malware-Analyse und Reverse Engineering** | | |
| · Entpacken<br>· Entschlüsseln<br>· Entwicklung eigener Entschlüsselungstools für gängige Szenarien<br>· Dekompilieren des Bytecodes<br>· Codezerlegung<br>· Disassembly<br>· Rekonstruktion moderner APT-Architekturen<br>· Erkennen typischer Codekonstrukte<br>· Identifizieren von Verschlüsselungs- und Komprimierungsalgorithmen<br>· Klassifizieren und Zuordnen basierend auf Code und Daten<br>· Klassen- und Strukturrekonstruktion<br>· APT-Plugin-Architekturen (basierend auf aktuellen APT-Beispielen) | 4 Tage | · Sie können ein modernes APT-Toolkit analysieren, vom Erhalt der ersten Probe bis hin zur Erstellung einer technischen Beschreibung der TTPs des Angreifers über IOCs.<br>· Erstellen Sie statische Entschlüsselungstools für reale Szenarien und führen Sie anschließend eine detaillierte Analyse des schädlichen Codes durch.<br>· Lernen Sie, schädliche Dokumente zu analysieren, die in der Regel für die Bereitstellung der ersten Payload verwendet werden, und erfahren Sie, wie diese extrahiert werden können.<br>· Gewährleisten Sie, dass die Schadensbewertung und die Maßnahmen zur Reaktion auf Vorfälle korrekt und effektiv sind. |
| **Windows Incident Response** | | |
| In einer realitätsnahen simulierten Umgebung findet ein Zwischenfall statt und im Kurs werden die folgenden Themen zu diesem Szenario behandelt:<br>· Einführung in den Prozess der Vorfallsreaktion mitsamt Abläufen<br>· Erläuterung des Unterschieds zwischen normalen Bedrohungen und APTs<br>· Erläuterung der APT Cyber Kill Chain<br>· Anwendung der Vorfallsreaktion auf verschiedene Szenarien<br>· Anwendung der Cyber Kill Chain auf die simulierte Umgebung<br>· Anwendung von Live-Analysen auf betroffenen Geräten bei der Erstreaktion<br>· Forensische Techniken zum Erfassen von Beweismitteln<br>· Einführung in Post-Mortem-Analysen und digitale Forensik<br>· Einführung in Speicherforensik<br>· Protokolldateianalyse mit regulären Ausdrücken und ELK<br>· Einführung in Bedrohungsinformationen<br>· Erstellung von Gefährdungsindikatoren (IOCs) mithilfe von YARA und SNORT<br>· Einführung in Malware-Analyse und Sandboxing<br>· Einführung in die Forensik des Netzwerkverkehrs<br>· Reporting zur Vorfallanalyse und Empfehlungen zum Aufbau von CSIRT<br>· Überprüfung der neu erworbenen Fähigkeiten mit einer praktischen Übung im Rahmen eines weiteren simulierten Szenarios | 4 Tage | · Einführung in die Phasen der Vorfallsreaktion<br>· Faktoren, die Sie bei der Reaktion auf einen Cybervorfall beachten sollten<br>· Erkennen der verschiedenen Angriffstechniken und des Aufbaus gezielter Angriffe durch die Cyber Kill Chain<br>· Reaktion auf verschiedene Vorfälle mit entsprechenden Maßnahmen<br>· Unterscheiden von APTs von anderen Bedrohungen<br>· Bestätigung von Cybervorfällen mithilfe von Live-Analysetools<br>· Unterschied zwischen Live- und Post-Mortem-Analyse und wann diese anzuwenden sind<br>· Identifizierung digitaler Beweismittel, etwa Festplatten- und Speicherdaten sowie Netzwerkverkehr, mit einer Einführung in die forensische Analyse<br>· Schreiben von YARA- und SNORT-IOCs für den erkannten Angriff<br>· Protokolldateianalyse<br>· Einführung in den Aufbau von IR-Teams |
| **Effiziente Bedrohungserkennung mit Yara** | | |
| · Kurze Einführung in die Yara-Syntax<br>· Tipps und Tricks zur Erstellung schneller und effektiver Regeln<br>· Yara-Generatoren<br>· Testen von Yara-Regeln auf Fehlalarme (False Positives)<br>· Aufspüren neuer, unentdeckter Proben auf VT<br>· Verwenden externer Module innerhalb von Yara zum effektiven Aufspüren von Bedrohungen<br>· Suche nach Anomalien<br>· Zahlreiche (!) Beispiele aus dem echten Leben<br>· Übungen zur Vertiefung der Yara-Kenntnisse | 4 Tage | · Erstellen effektiver Yara-Regeln<br>· Testen von Yara-Regeln<br>· Verbessern der Regeln, bis sie Bedrohungen feststellen, die sonst niemand findet |

# Kaspersky Incident Response

**Obwohl Ihre IT- und Sicherheitsmitarbeiter ihr Bestes geben, um sicherzustellen, dass jede der Netzwerkkomponenten gut geschützt ist und jederzeit für legitime Benutzer verfügbar bleibt, kann eine einzige Schwachstelle zum Einfallstor für Kriminelle werden, die Zugriff auf Ihre Informationssysteme erhalten wollen. Niemand ist immun. Egal, wie effektiv Ihre Sicherheitskontrollen sind – Sie können schnell zum Opfer werden.**

**IT-Sicherheitsvorfälle zu vermeiden wird zunehmend schwieriger. Doch selbst wenn es nicht immer möglich ist, einen Angriff zu stoppen, bevor er in Ihr Netzwerk eindringt, sind wir in der Lage, den entstehenden Schaden zu beschränken und eine weitere Ausbreitung des Angriffs zu verhindern.**

**Kaspersky Cybersecurity Services**

- **Kaspersky Threat Intelligence**
- **Kaspersky Threat Hunting**
- **Kaspersky Cybersecurity Training**
- **Kaspersky Incident Response**
  Reaktion auf Vorfall
  Malware-Analyse
  Digital Forensics
- **Kaspersky Security Assessment**

Das wichtigste Ziel der Vorfallsreaktion ist die Reduzierung der Auswirkungen einer Sicherheitsverletzung oder eines Angriffs auf Ihre IT-Umgebung. Der Service deckt den gesamten Zyklus der Vorfallsuntersuchung ab – von der Erfassung von Beweisen vor Ort über die Identifizierung zusätzlicher Gefährdungsindikatoren und die Vorbereitung eines Abhilfemaßnahmenplans bis hin zur vollständigen Beseitigung der Bedrohung aus Ihrem Unternehmen.

Dies erfolgt auf folgende Weise:

- Identifizierung angegriffener Ressourcen.
- Isolierung der Bedrohung.
- Verhinderung einer weiteren Ausbreitung des Angriffs.
- Suchen und Erfassen von Beweisen.
- Analyse der Beweise und Rekonstruktion der Chronologie und Logik des Vorfalls.
- Analyse der für den Angriff verwendeten Malware (falls diese gefunden wird).
- Aufdecken der Angriffsquellen und anderer potentiell gefährdeter Systeme (falls möglich).
- Durchführung toolgestützter Scans Ihrer IT-Infrastruktur zur Aufdeckung möglicher Gefährdungshinweise.
- Analyse ausgehender Verbindungen zu externen Ressourcen (z. B. mögliche Command-and-Control-Server) zur Ermittelung verdächtigen Verhaltens.
- Beseitigung der Bedrohung.
- Empfehlung weiterer möglicher Abhilfemaßnahmen.

Abhängig davon, ob Sie ein internes Vorfallsreaktionsteam haben oder nicht, können Sie unsere Experten damit beauftragen, eine vollständige Untersuchung durchzuführen. Diese beinhaltet die Identifizierung und Isolierung angegriffener Computer sowie das Verhindern einer Ausbreitung der Bedrohung. Zudem kann eine Malware-Analyse oder Digitale Forensik durchgeführt werden.

Die Incident Response Services von Kaspersky werden von erfahrenen Experten auf dem Gebiet der Analyse von Cyberbedrohungen sowie von Malware-Forensikern erbracht. Wir setzen unser gesamtes Wissen und unsere globale Erfahrung in den Bereichen digitale Forensik und Malware-Analyse für die Behebung Ihres Sicherheitsvorfalls ein.

# Malware-Analyse

Die Malware-Analyse liefert ein vollständiges Bild des Verhaltens und der Ziele bestimmter Malware-Dateien, die es auf Ihr Unternehmen abgesehen haben. Die Experten von Kaspersky führen eine detaillierte Analyse der von Ihrem Unternehmen bereitgestellten Malware-Probe durch und erstellen einen ausführlichen Bericht, der Folgendes enthält:

- **Probeneigenschaften:** Eine kurze Beschreibung der Probe und eine Einschätzung zur Malware-Klassifizierung.
- **Detaillierte Malware-Beschreibung:** Eine umfassende Analyse der Funktionen der Malware-Probe, des Verhaltens und der Ziele der Bedrohung (inkl. IOCs), um Ihnen die erforderlichen Informationen zur Neutralisierung ihrer Aktivitäten zu liefern.
- **Abhilfeszenario:** Der Bericht schlägt Schritte zur vollständigen Sicherung Ihres Unternehmens vor dieser Bedrohung vor.

# Digital Forensics

Die digitale Forensik kann eine Malware-Analyse umfassen, wie oben gezeigt, falls Malware während der Untersuchung festgestellt wurde. Unsere Experten setzen die Beweise zusammen, um genau zu verstehen, was vor sich geht, darunter Festplatten-Images, Speicherauszüge und Netzwerk-Traces. Das Ergebnis ist eine detaillierte Aufklärung des Vorfalls. Sie als Kunde leiten diesen Vorgang ein, indem Sie Beweise sammeln und einen Abriss des Vorfalls bereitstellen. Daraufhin analysieren die Experten von Kaspersky die Symptome des Zwischenfalls, identifizieren den Malware-Binärcode (falls vorhanden) und führen die Malware-Analyse durch, um einen detaillierten Bericht inklusive empfohlener Korrekturmaßnahmen bereitzustellen.

# Bereitstellungsoptionen

Die Incident Response Services von Kaspersky sind wie folgt erhältlich:

- als Abonnement
- als Reaktion auf einen einzelnen Vorfall

Beide Optionen werden nach Aufwand unserer Experten für die Aufklärung eines Vorfalls berechnet. Dies wird vor der Unterzeichnung des Vertrags mit Ihnen verhandelt. Sie können die gewünschte Anzahl an Stunden, die wir aufwenden sollen, festlegen oder Sie folgen den Empfehlungen unserer Experten, die sich nach Ihrem speziellen Vorfall und Ihren individuellen Anforderungen richten.

# Kaspersky Security Assessment

**Bei den Security Assessment Services von Kaspersky handelt es sich um die Services unserer internen Experten. Viele von ihnen sind international anerkannte Experten auf ihrem Gebiet und von fundamentaler Bedeutung für die Entwicklung unserer Security Intelligence.**

**Da keine zwei IT-Infrastrukturen exakt gleich und die gefährlichsten Cyberbedrohungen individuell auf die Schwachstellen von Unternehmen zugeschnitten sind, sind auch unsere Expertenservices ein maßgeschneidertes Angebot. Die auf den folgenden Seiten beschriebenen Services sind Teil unseres professionellen Toolkits – sie kommen während der Zusammenarbeit mit Ihnen selektiv bzw. teilweise oder vollständig zum Einsatz.**

**Unser vorrangiges Ziel besteht darin, individuell als Berater für Sie tätig zu werden, Ihr Risiko zu bewerten, Ihre Sicherheitsmaßnahmen zu verschärfen und Sie vor zukünftigen Bedrohungen zu schützen.**

**Security Assessment Services beinhalten Folgendes:**

- **Penetrationstests**
- **Red Teaming**
- **Application Security Assessment**
- **ATM/POS Security Assessment**

**Kaspersky Cybersecurity Services**

- **Kaspersky Threat Intelligence**
- **Kaspersky Threat Hunting**
- **Kaspersky Cybersecurity Training**
- **Kaspersky Incident Response**
- **Kaspersky Security Assessment**
  - Penetrationstests
  - Red Teaming
  - Application Security Assessment
  - ATM/POS Security Assessment

## Penetrationstests

Jedes Unternehmen muss laufend sicherstellen, dass die IT-Infrastruktur umfassend vor potentiellen Cyberattacken geschützt ist. Dies ist eine besondere Herausforderung für Großunternehmen mit Tausenden von Mitarbeitern, Hunderten von Informationssystemen und einer Vielzahl von Standorten weltweit.

Ein Penetrationstest ist eine praktische Demonstration möglicher Angriffsszenarien, in denen versucht wird, die Sicherheitskontrollen Ihres Unternehmensnetzwerks zu umgehen und Zugriff auf wichtige Systeme zu erlangen.

Unsere Penetrationstests vermitteln Ihnen ein genaues Verständnis der Sicherheitslücken in Ihrer Infrastruktur, indem wir die möglichen Konsequenzen unterschiedlicher Angriffsarten analysieren, die Effektivität Ihrer aktuellen Sicherheitsmaßnahmen bewerten und Abhilfe- und Verbesserungsmaßnahmen vorschlagen.

Dank unserer Penetrationstests können Sie:

- **Schwachpunkte in Ihrem Netzwerk identifizieren,** eine fundierte Entscheidung darüber zu treffen, wie finanzielle Mittel am besten einzusetzen sind, um das Risiko in Zukunft zu verringern.
- **Finanzielle und betriebliche Verluste sowie Rufschädigungen durch Cyberangriffe** vermeiden, indem Sie diese durch frühzeitige Erkennung und Schließen von Schwachstellen verhindern.
- **Behördliche Auflagen und Branchen- bzw. unternehmensinterne Normen** erfüllen, die diese Art von Sicherheitsprüfung vorschreiben (z. B. der Datensicherungsstandard für Kreditkartentransaktionen, PCI-DSS).

**Ergebnisse der Penetrationstests**
Penetrationstests sollen Sicherheitslücken aufdecken, die ausgenutzt werden könnten, um Zugriff auf wichtige Netzwerkkomponenten zu erlangen. Dies beinhaltet u. a.:

- Anfällige Netzwerkarchitektur, unzureichender Netzwerkschutz
- Schwachstellen, die das Abfangen und Umleiten des Netzwerkverkehrs ermöglichen
- Unzureichende Authentifizierungs- und Autorisierungsmechanismen von unterschiedlichen Diensten
- Schwache Benutzeranmeldedaten
- Konfigurationsfehler inklusive zu umfangreicher Benutzerberechtigungen
- Schwachstellen durch Fehler im Programmcode (Code-Injektionen, Manipulation von Pfadangaben, Schwachstellen auf Clientseite usw.)
- Schwachstellen durch veraltete Hardware und Software ohne aktuelle Sicherheitsupdates
- Bereitstellung der Ergebnisse

Die Ergebnisse werden in einem abschließenden Bericht zusammengefasst, einschließlich detaillierter technischer Informationen zum Testvorgang, Ergebnissen, den entdeckten Schwachstellen und Empfehlungen für Korrekturmaßnahmen sowie einer Kurzübersicht über die Testergebnisse und die möglichen Angriffsvektoren. Auf Anfrage können auch Videos und Präsentationen für Ihre technische Abteilung und die Geschäftsführung bereitgestellt werden.

## Serviceumfang und Optionen

Abhängig von Ihren Anforderungen und der bestehenden IT-Infrastruktur können Sie beliebige oder alle der folgenden Services in Anspruch nehmen:

- **Externer Penetrationstest:** Über das Internet vorgetragene Sicherheitsprüfung durch einen „Angreifer" ohne Vorkenntnisse über Ihr System.
- **Interner Penetrationstest:** Szenarien mit einem internen Angreifer, z. B. einem Besucher, der nur physischen Zugang zu Ihren Büroräumen hat, oder einem Dienstleister, der nur eingeschränkten Zugriff auf Ihre Systeme hat.
- **Social-Engineering-Test:** Prüfung des Sicherheitsbewusstseins unter Ihren Mitarbeitern durch Simulation von Social-Engineering-Attacken, z. B. Phishing, schädlichen Links in E-Mails, verdächtige Anhänge usw.
- **Sicherheitsprüfung für WiFi-Netzwerke:** Unsere Experten besuchen Ihren Standort und analysieren die vorhandenen WiFi-Sicherheitskontrollen.

Welche Teile Ihrer IT-Infrastruktur Sie testen lassen, bleibt Ihnen überlassen, wir empfehlen jedoch, entweder das gesamte Netzwerk oder zumindest die größten Segmente einzubeziehen, da die Testergebnisse aussagekräftiger sind, wenn unsere Experten unter denselben Bedingungen arbeiten wie potentielle Eindringlinge.

## Die Vorgehensweise von Kaspersky bei Penetrationstests

Obwohl bei Penetrationstests echte Hacker-Angriffe simuliert werden, werden diese Tests streng kontrolliert. Sie werden von Kaspersky-Sicherheitsexperten unter vollständiger Wahrung von Vertraulichkeit, Integrität und Verfügbarkeit Ihrer Systeme ausgeführt und halten sich streng an internationale Normen und Best Practices, darunter:

- Penetration Testing Execution Standard (PTES)
- NIST Special Publications 800-115 „Technical Guide to Information Security Testing and Assessment"
- Open Source Security Testing Methodology Manual (OSSTMM)
- Information Systems Security Assessment Framework (ISSAF)
- Web Application Security Consortium (WASC) Threat Classification
- Open Web Application Security Project (OWASP) Testing Guide
- Common Vulnerability Scoring System (CVSS)

Bei den Mitgliedern des Projektteams handelt es sich um erfahrene Profis mit einem tiefgreifenden und aktuellen Praxiswissen auf diesem Gebiet, die als Sicherheitsberater von Branchenführern wie Oracle, Google, Apple, Microsoft, Facebook, PayPal, Siemens und SAP anerkannt sind.

## Bereitstellungsoptionen

Je nach Art des gewünschten Sicherheitsassessments und ihrer speziellen Systembedingungen und Arbeitsabläufe können die Services entweder per Fernzugriff oder am Standort geleistet werden. Die meisten Services lassen sich per Fernzugriff ausführen und selbst die internen Penetrationstests können per VPN-Zugriff durchgeführt werden. Einige Services (z. B. WLAN-Sicherheits-Assessments) können jedoch nur vor Ort ausgeführt werden.

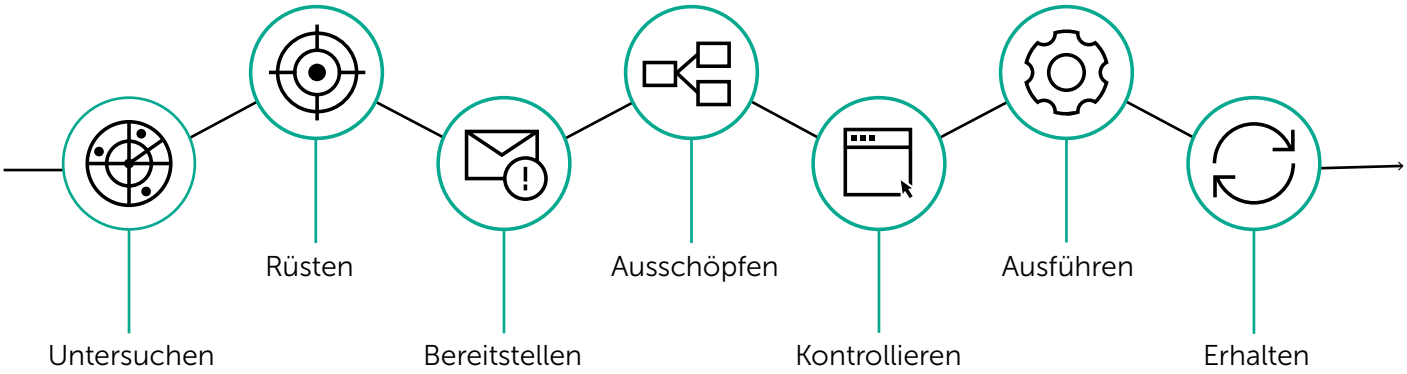
# Red Teaming

Der Service umfasst Folgendes:

- **Threat Intelligence.** Der Service beginnt mit einer Erörterung der bekannten Bedrohungen des Kunden und der Erfahrung des Blue Teams. Ziel ist es, die wichtigsten geschäftlichen Ressourcen zu identifizieren und zu ermitteln, wie Projektergebnisse auf die TTPs zugeschnitten werden können, die von der Unternehmensverteidigung verwendet werden. Während dieser Erörterungen fordert Kaspersky jedoch keine Informationen über die Zielressourcen an, da das Red Team sich auch unabhängig Informationen verschafft, genau, wie ein echter Gegner es tun würde. Die Phase der Informationsbeschaffung umfasst sowohl die Analyse öffentlich zugänglicher Informationen (Open-Source-Informationen) als auch die Analyse von über Untergrund-Communitys verfügbaren Daten.

- **Gegnersimulation.** Diese Phase beginnt mit der Vorbereitung von Angriffsszenarien und Tools, wobei die Ergebnisse der Threat Intelligence-Phase genutzt werden. Die Vorbereitung kann ein genaues Studium der in der Umgebung des Kunden verwendeten Systeme umfassen, um neue Schwachstellen aufzudecken, kann aber auch die Entwicklung von benutzerdefinierten Tools zur Umgehung der Sicherheitssysteme des Kunden oder die Vorbereitung von Spear-Phishing-Angriffen beinhalten. Nach Abschluss der Vorbereitung führt Kaspersky die aktive Phase der Gegnersimulation durch. Diese Tests können Folgendes umfassen:

  - Passive Informationsbeschaffung,
  - Aktive Informationsbeschaffung (Netzwerkerkennung), einschließlich Portscans, Ermittlung verfügbarer Dienste und manuelle Anfragen an bestimmte Dienste (DNS, E-Mail),
  - Scans externer Schwachstellen und deren Analyse
  - Untersuchung der Sicherheit von Webprogrammen (mit automatisierten und manuellen Ansätzen) zur Identifizierung der folgenden Arten von Schwachstellen:
    - Code-Injektion (SQL-Injektion, OS-Commanding usw.)
    - Schwachstellen auf Clientseite (Cross-Site-Scripting, Cross-Site Request Forgery usw.)
    - Fehler bei der Authentifizierung und Autorisierung
    - Unsichere Speicherung von Daten
    - Weitere Schwachstellen, die zu den in der WASC Threat Classification v2.0 und in den OWASP Top Ten aufgeführten Bedrohungen führen können
  - Manuelle Schwachstellenanalyse, einschließlich Ermittlung von Ressourcen ohne Authentifizierung, wichtige öffentlich zugängliche Informationen, mangelhafte Zugriffskontrolle
  - Erraten von Anmeldedaten
  - Social Engineering-Test
  - Ausnutzung einer oder mehrerer der gefundenen Schwachstellen und Berechtigungserweiterung (wenn möglich)
  - Entwickeln Sie einen Angriff mit den oben aufgeführten erlangten Berechtigungen und Techniken, bis der Dienstanbieter auf das LAN oder wichtige Netzwerkressourcen zugreifen kann (z. B. Active Directory-Domaincontroller, Geschäftssysteme, DBMSs) oder bis alle während des Tests verfügbaren Angriffsmethoden ausgeschöpft sind.




Die oben genannten Tests werden entsprechend den vorbereiteten kundenspezifischen Szenarien und unter Einsatz spezieller Techniken durchgeführt, um eine Erkennung durch das Blue Team zu vermeiden. Sobald das Red Team alle Ziele erreicht hat, werden Aktivitäten durchgeführt, um die Vorfallserkennung und Reaktion des Blue Teams auszulösen und das Blue Team an der Übung zu beteiligen.

- **Berichterstellung.** In dieser Phase analysiert Kaspersky die Ergebnisse der Gegnersimulation, erstellt einen Bericht mit einer detaillierten Beschreibung der Angriffe (einschließlich Zeitstempel und Gefährdungsindikatoren) und Empfehlungen.
- **Übersicht der Testergebnisse.** Ein Workshop zur anschließenden Beurteilung mit dem Blue Team des Unternehmens kann arrangiert werden, um die Projektergebnisse, Gründe für nicht erkannte oder nicht verhinderte Elemente und mögliche weitere Verbesserungen der Abwehr zu besprechen.

## Ansatz und Methodik

Das Red Team nutzt Methoden, die echten Hackerangriffen stark ähneln, und ermöglicht dadurch eine Effektivitätsbewertung der Schutzmaßnahmen. Im Gegensatz zu einem Hackerangriff wird der Service jedoch von erfahrenen Kaspersky-Sicherheitsexperten durchgeführt, die Vertraulichkeit, Integrität und Verfügbarkeit des Systems gewährleisten und dabei die folgenden **internationalen Standards und Best Practices strikt einhalten:**

- Penetration Testing Execution Standard (PTES)
- NIST Special Publications 800-115 „Technical Guide to Information Security Testing and Assessment"
- Open Source Security Testing Methodology Manual (OSSTMM)
- Information Systems Security Assessment Framework (ISSAF)
- Web Application Security Consortium (WASC)
- Threat Classification Open Web Application Security Project (OWASP)
- Testing Guide Common Vulnerability Scoring System (CVSS)
- Und weitere Standards, die von der Branche und dem Standort Ihres Unternehmens abhängen

Die Analyse wird sowohl mit automatisierten Tools als auch manuell von Experten durchgeführt.
Die folgenden Tools zur Sicherheitsbewertung können verwendet werden:

- Tools zur Informationserfassung (etwa Maltego und theHarvester)
- Verschiedene allgemeine und spezialisierte Scanner (NMap, MaxPatrol, Nessus, Acunetics WVS, nbtscan und andere)
- Komplexe Lösungen zur Sicherheitsbewertung (Kali Linux)
- Tools zum Erraten von Anmeldedaten (Hydra, ncrack, Bruter und andere)
- Spezielle Lösungen für die Sicherheitsbewertung von Webprogrammen (OWASP dirbuster, BurpSuite, ProxyStrike und verschiedene Plugins für Mozilla Firefox)
- Tools zur Analyse des Netzwerkverkehrs (Wireshark, Cain and Abel)
- Tools zur Extraktion und Verwaltung von Anmeldedaten (Mimikatz, WCE, pwdump und andere)
- Spezialisierte Tools für verschiedene Arten von Angriffen (Yersinia, Loki, Responder, SIPVicious und andere)
- Tools für Disassembly und Debugging (IDA Pro, OllyDbg)
- Weitere Elemente, darunter Exploits mit eingeschränktem Zugriff und benutzerdefinierte Exploit-Tools, die vom Serviceanbieter entwickelt wurden.

Damit das Red Team rechtmäßig und sicher vorgehen kann, muss der Kunde einen Ansprechpartner (einen Vertreter) für die gesamte Projektkommunikation bereitstellen, einschließlich der Umfangsverhandlungen und der Lösung von Zugriffsproblemen sowie der Bestätigung aktiver Arbeiten. Der Vertreter muss ein offizieller Mitarbeiter des Kunden mit einer E-Mail-Adresse sein, die zur Domain des Kunden gehört (kein externer Vermittler).

**Die Vertraulichkeit, Integrität und Verfügbarkeit Ihrer IR-Ressourcen haben für uns höchste Priorität.** Die Experten von Kaspersky ergreifen alle erforderlichen Vorsichtsmaßnahmen, um Schäden an Ihrer IT-Umgebung zu vermeiden. Alle vertraulichen technischen Informationen zum Projekt (wichtige Daten, Anmeldedaten, Bewertungsergebnisse usw.) werden mit starker Verschlüsselung gespeichert und übertragen und können nach Abschluss des Projekts auf Wunsch gelöscht werden.

**Unsere Teammitglieder sind erfahrene Experten** in der Sicherheitsbewertung, verfügen über umfassende Kenntnisse in diesem Bereich und entwickeln ihre Fähigkeiten kontinuierlich weiter. Sie wurden für ihre Sicherheitsforschung von Branchenführern wie Oracle, Google, Apple, Microsoft, Facebook, PayPal, Siemens, SAP und anderen anerkannt (eine Beschreibung des Projektteams finden Sie in Abschnitt 7). Lebensläufe der Mitglieder des Projektteams finden Sie im Anhang zu diesem Angebot.

## Ergebnis

Im Anschluss an die Servicebereitstellung erhalten Kunden einen Bericht mit den folgenden Informationen:

- Grundlegende Schlussfolgerungen zu den identifizierten Verteidigungsfähigkeiten und Empfehlungen zu deren Verbesserung;
- Genaue Beschreibung der erkannten Schwachstellen, darunter Schweregrad, Komplexität der Ausnutzung, mögliche Auswirkungen für das anfällige System, Nachweis über die Existenz der Schwachstelle (wo möglich);
- Detaillierte Beschreibung der Aktivitäten (einschließlich Zeitstempel und Gefährdungsindikatoren) zur Analyse und Verbesserung des Verteidigungsteams;
- Empfehlungen zur Beseitigung von Schwachstellen;
- Empfehlungen zur Verbesserung der Vorfallsreaktionsprozesse;
- Empfehlungen zur Behebung erkannter Probleme bei Prävention und Erkennung.

Mit dem Red Team Testing Service von Kaspersky können Sie die Effektivität Ihrer Überwachungsfunktionen und der Verfahren zur Vorfallsreaktion bewerten.

# Application Security Assessment

Egal, ob Sie Ihre Unternehmensprogramme intern entwickeln oder diese extern einkaufen: Sie wissen, dass ein einziger Fehler im Code zu einer Schwachstelle führen kann, die bei Angriffen erhebliche finanzielle Verluste und Imageschäden nach sich ziehen könnte. Während des Programm-Lebenszyklus können außerdem weitere Schwachstellen hinzukommen, etwa durch Softwareupdates oder eine unsichere Konfiguration der Komponenten bzw. durch neue Angriffsmethoden.

Unsere Application Security Assessments decken Schwachstellen in beliebigen Programmtypen auf: von umfangreichen Cloud-basierten Lösungen, ERP-Systemen, Online-Banking und anderen speziellen Geschäftsprogrammen bis hin zu integrierten Anwendungen und Apps auf unterschiedlichen Plattformen (iOS, Android und andere).

Dank einer Kombination aus Praxiswissen und Erfahrung mit international anerkannten Best Practices entdecken unsere Experten Sicherheitslücken, die Ihr Unternehmen anfällig für unterschiedliche Angriffstypen machen könnten, u. a.:

- Abschöpfen vertraulicher Daten
- Infiltration und Manipulation von Daten und Systemen
- DoS-Attacken
- Betrügerische Aktivitäten

Auf Grundlage unserer Empfehlungen lassen sich die in den Programmen entdeckten Schwachstellen beheben und die aufgeführten Angriffstypen vermeiden.

## Servicevorteile

Die Application Security Assessments von Kaspersky bieten den Programmeigentümern und -entwicklern folgende Vorteile:

- **Keine finanziellen und betrieblichen Verluste** sowie Imageschäden durch frühzeitige Erkennung und Behebung von Schwachstellen, die für Angriffe genutzt werden könnten
- **Keine Beseitigungskosten,** da Programmschwachstellen noch während der Entwicklung identifiziert werden, bevor sie die Produktionsumgebung erreichen, wo die Behebung meist mit erheblichen Störungen und Kosten verbunden ist.
- **Unterstützung des Secure Software Development Lifecycle** (S-SDLC) für Entwicklung und Betrieb sicherer Softwareprogramme.
- **Einhaltung von Verordnungen sowie von Branchen- und internationalen Unternehmensstandards** zur Programmsicherheit, z.B. PCI DSS oder HIPAA

## Serviceumfang und Optionen

Zu den getesteten Programmen gehören u.a. offizielle Webseiten und Unternehmensprogramme (herkömmlich oder Cloud-basiert), darunter auch integrierte oder mobile Programme.

Die Tests werden an Ihre Bedürfnisse und die Besonderheiten der zu testenden Software angepasst. Zu den Services gehören u. a.:

- **Black-Box-Tests** zur Simulation eines externen Angreifers
- **Grey-Box-Tests** zur Simulation von autorisierten Benutzern mit verschiedenen Profilen
- **White-Box-Tests** zur Analyse mit umfassendem Zugriff auf die Anwendung, einschließlich des Quellcodes. Dieser Ansatz ist am effektivsten, wenn es darum geht, möglichst viele Schwachstellen zu entdecken.
- **Application Firewall Effectiveness Assessment:** Programme werden mit und ohne Firewall-Schutz getestet, um Schwachstellen zu ermitteln und festzustellen, ob potentielle Exploits geblockt werden

## Ergebnisse

Die Ergebnisse werden in einem abschließenden Bericht zusammengefasst. Dieser umfasst auch detaillierte technische Informationen zu Testvorgang, Ergebnissen, entdeckten Schwachstellen und Empfehlungen für Korrekturmaßnahmen sowie eine Kurzübersicht, in der mögliche Folgen für die Geschäftsführung beschrieben werden. Auf Anfrage können auch Videos und Präsentationen für Ihre technische Abteilung und die Geschäftsführung bereitgestellt werden.

**Durch die Software ermittelte Schwachstellen:**

- Fehler bei Authentifizierung und Autorisierung, inklusive Multifaktor-Authentifizierung
- Code-Injektion (SQL-Injektion, OS-Commanding usw.)
- Logische Schwachstellen, die Betrugsversuche begünstigen
- Schwachstellen auf Clientseite (Cross-Site-Scripting, Cross-Site Request Forgery usw.)
- Schwache Kryptografie
- Schwachstellen in Client-Server-Verbindungen
- Unsicheres Speichern und Übertragen von Daten, z. B. fehlende PAN-Maskierung in Bezahlsystemen
- Konfigurationsfehler, z. B. Fehler, die zu Attacken auf Sitzungen führen
- Offenlegung vertraulicher Informationen
- Weitere Schwachstellen, die zu den im Bericht „WASC Threat Classification v2.0“ und in den „OWASP Top Ten“ aufgeführten Bedrohungen führen können

## Unsere Vorgehensweise beim Application Security Assessment

Das Application Security Assessment wird von unseren Sicherheitsexperten sowohl manuell als auch mithilfe automatisierter Tools ausgeführt. Hierbei kommt dem Schutz von Vertraulichkeit, Integrität und Verfügbarkeit Ihrer Systeme sowie der strengen Einhaltung u. a. der folgenden internationalen Normen und Best Practices besondere Bedeutung zu:

- Web Application Security Consortium (WASC) Threat Classification
- Open Web Application Security Project (OWASP) Testing Guide
- OWASP Mobile Security Testing Guide
- Weitere Standards, abhängig von der Branche und dem Standort Ihres Unternehmens

Bei den Mitgliedern des Projektteams handelt es sich um erfahrene Profis mit einem tiefgreifenden und aktuellen Praxiswissen auf diesem Gebiet, inklusive der verschiedenen Plattformen, Programmiersprachen, Frameworks, Schwachstellen und Angriffsmethoden. Sie treten als Redner bei wichtigen internationalen Konferenzen auf und arbeiten als Sicherheitsberater für führende Software- und Cloud-Service-Anbieter, darunter Oracle, Google, Apple, Facebook und PayPal.

## Bereitstellungsoptionen

Je nach Art des gewünschten Security Assessments und ihren speziellen Systembedingungen und Anforderungen an die Arbeitsbedingungen können die Services entweder per Fernzugriff oder am Standort geleistet werden. Die meisten der Services lassen sich per Fernzugriff ausführen.

# ATM/POS Security Assessment

Geldautomaten und Kassensysteme sind nicht mehr allein physischen Angriffen wie Aufbrechen oder Kartenbetrug ausgesetzt. Mit zunehmender Ausgereiftheit der Schutzmaßnahmen für Geldautomaten/Kassensysteme von Banken und Herstellern werden auch die Angriffe auf diese Geräte immer raffinierter. Hacker nutzen Schwachstellen in der Infrastruktur, Architektur und den Programmen von Geldautomaten und Kassensystemen (ATM/POS) aus und entwickeln Malware, die speziell auf diese Systeme zugeschnitten ist. ATM/POS Security Assessments von Kaspersky unterstützen Sie bei der Erkennung von Sicherheitslücken in Ihren Geldautomaten/Kassensystemen und somit bei der Abwehr von Angriffen.

Es gibt keine einzelne Lösung, die vollständigen Schutz bietet. Als Geschäftsführer, CIO, CISO oder CTO liegt es in Ihrer Verantwortung, Ihr Unternehmen vor den heutigen Bedrohungen zu schützen und die Gefahren zu prognostizieren, die in den nächsten Jahren auf Sie zukommen. Dazu ist mehr als nur ein zuverlässiger technologischer Schutz vor bekannten Bedrohungen erforderlich. Sie benötigen strategische Sicherheitsinformationen, für deren Erhebung die wenigsten Unternehmen über genügend interne Ressourcen verfügen.

Bei den Security Assessment Services von Kaspersky handelt es sich um die Services unserer interner Experten. Viele von ihnen sind international anerkannte Experten auf ihrem Gebiet und von fundamentaler Bedeutung für die Entwicklung unserer Security Intelligence.

**ATM/POS Security Assessment**
Umfassende Analyse von Geldautomaten und Kassensystemen,speziell zur Erkennung von Schwachstellen entwickelt,die von Angreifern wie folgt ausgenutzt werden können:

- Abheben von Geld ohne Autorisierung
- Durchführen unbefugter Transaktionen
- Abfangen der Karteninformationen Ihrer Kunden
- Initiieren eines DoS-Angriffs

**Was passiert, wenn Betrüger eindringen?**
Jeder Geldautomat besteht aus 4 Kassetten mit bis zu 3.000 Scheinen pro Kassette. Im schlimmsten Fall können Kriminelle bis zu 255.000 US-Dollar erhalten. Im Mai 2016 kam es zu einem Vorfall, bei dem Auszahlungen über Geldautomaten vorgenommen wurden. Dabei koordinierten Kriminelle den Zugriff auf 1400 Geldautomaten in einem Zeitfenster von nur wenigen Stunden. Bei einem Vorfall in Taiwan im Juli 2016 wurde Schadsoftware auf mehreren Geldautomaten installiert, wodurch Kriminelle zwei Millionen US-Dollar über 20 der Geldautomaten abheben konnten. Kriminelle sind dazu imstande, Geldautomaten anzugreifen. Schließen Sie die Sicherheitslücken.

**Wer wir sind**
Mitglieder des Projektteams sind Experten, die über umfassende praktische Erfahrung im Sicherheitsbereich sowie fundierte Kenntnisse im Außendienst verfügen und ihre Fähigkeiten ständig verbessern. Sie bieten regelmäßig Sicherheitsberatungen für ATM-/POS-Anbieter und präsentieren die Ergebnisse unserer ATM-/POS-Sicherheitsrecherchen auf führenden Sicherheitskonferenzen, einschließlich Black Hat, Hack in Paris, Positive Hack Days, Security Analyst Summit, Nuit Du Hack, HITB GSEC, DefCamp, ATMIA Events, Chaos Communication Congress und viele andere.

Folgen Sie unseren Experten unter
de.securelist.com

Weitere Informationen erhalten Sie unter
www.kaspersky.de

## Argumente für diese Lösung

ATM/POS Security Assessments von Kaspersky ermöglichen Anbietern und Finanzdienstleistern Folgendes:

- Erkennen der Schwachstellen in ihren Geldautomaten/Kassensysteme und Verbessern der entsprechenden Sicherheitsverfahren
- Vermeiden der durch einen Angriff möglichen finanziellen und betrieblichen Verluste sowie von Rufschädigungen durch schnelle Erkennung und Behebung der Schwachstellen, die von Angreifern ausgenutzt werden könnten.
- Compliance mit behördlichen, Branchen- oder Unternehmensstandards, wie z. B. PCI DSS (Payment Card Industry Data Security Standard), die die Durchführung von Sicherheits-Assessments vorsehen

## Das testen wir

Der Service umfasst eine umfassende Analyse von Geldautomaten und Kassensystemen einschließlich Bewertung von Softwarekomponenten, Hardwaregeräten und Netzwerkkommunikation. Dieser Service kann auf einem einzelnen Geldautomaten/Kassensystem oder in einem Netzwerk mit mehreren Geräten durchgeführt werden. Sie sollten für das Assessment entweder den Geldautomaten-/Kassensystemtyp, den Sie auch am häufigsten in Ihrem Unternehmen einsetzen, oder den am meisten gefährdeten Gerätetyp (der z. B. bereits Opfer eines Angriffs wurde) mit typischen Konfigurationen verwenden.

## So gehen wir vor

Bei der Analyse suchen unsere Experten nicht nur nach Konfigurationsfehlern und Schwachstellen in veralteten Softwareversionen, sondern führen auch eine umfangreiche Analyse der zugrunde liegenden Logik eines Geldautomaten/Kassensystems durch. Die Sicherheitsanalyse hat das Ziel, neue Schwachstellen (Zero-Day) auf Komponentenebene zu finden. Wenn wir Schwachstellen finden, die ein Angreifer ausnutzen könnte (z. B. in Form einer unberechtigten Barabhebung), können unsere Experten mögliche Angriffsszenarien mithilfe von speziell entwickelten Automatisierungstools oder -geräten nachstellen.

Unsere ATM/POS Security Assessments sind absolut sicher und nicht invasiv, auch wenn sie die Simulation des Angriffsverhaltensechter Hacker beinhalten, um die Effektivität Ihrer Verteidigungsstrategie in der Praxis zu beurteilen.

## Bedrohungen im Finanzsektor

Weil Banken, Aktienmärkte und andere Finanzdienstleister stets interessante Ziele für Cyberkriminelle darstellen, müssen sie im Bereich der Cybersicherheit immer einen Schritt voraus sein, um finanzielle Verluste und Rufschäden zu vermeiden. Kaspersky bietet eine Reihe proaktiver Threat Intelligence Services für Finanzdienstleister, die ihren Sicherheitsbetrieb verbessern und einen proaktiven Ansatz im Hinblick auf fortschrittliche Bedrohungen verwenden möchten:

- Security Assessment Services (Penetrationstests, Application Security Assessment, ATM/POS Security Assessment)
- Threat Intelligence Reports (APT Intelligence Reports, kundenspezifische Threat Intelligence Reports)
- Cyber-Attack Readiness Testing
- Überwachung von Botnet-Bedrohungen
- Threat Data Feeds
- Malware-Analyse und digitale Forensik
- Schulung: Bedrohungsanalyse, Forensik und Untersuchung

Weitere Informationen finden Sie unter www.kaspersky.de/enterprise.

Cyber Threats News:
https://de.securelist.com/
IT Security News:
https://www.kaspersky.de/blog/category/business/
IT-Sicherheit für KMUs:
kaspersky.de/business
IT-Sicherheit für Großunternehmen:
kaspersky.de/enterprise

**www.kaspersky.de**



**Beständigkeit, Unabhängigkeit und Transparenz – das zeichnet uns aus. Wir wollen eine sichere Umgebung schaffen, in der Technologie unser Leben verbessert. Deshalb schützen wir diese Technologie. Damit Menschen auf der ganzen Welt die unzähligen technologischen Möglichkeiten nutzen können. Wir tragen mit Cybersicherheit zu einer sicheren Zukunft bei.**

**Erfahren Sie mehr unter kaspersky.de/transparency**

Proven.
Transparent.
Independent.