Kaspersky Anti Targeted Attack

kaspersky bring on the future

Cyberkriminelle sind Spezialisten in der Entwicklung einzigartiger und immer neuer Methoden, um in Systeme einzudringen und sie zu kompromittieren. Da sich die Bedrohungen ständig weiterentwickeln und immer raffinierter und zerstörerischer werden, ist es von entscheidender Bedeutung, sie schnell zu erkennen und angemessen darauf zu reagieren.

Kaspersky Anti Targeted Attack

Verkürzt die Zeit bis zur Bedrohungserkennung und -reaktion

Vereinfacht die Bedrohungsanalyse und Vorfallsreaktion

Hilft, Sicherheitslücken zu schließen und die „Verweildauer" von Angriffen zu verkürzen

Automatisiert manuelle Aufgaben während Bedrohungserkennung und -reaktion

Entlastet das IT-Sicherheitspersonal für andere Aufgaben

Unterstützt bei der Einhaltung von Compliance

Erstklassige Cybersicherheit: APTs (Advanced Persistent Threats) und raffinierten Bedrohungen immer einen Schritt voraus

Kaspersky Anti Targeted Attack (KATA) hilft Ihnen beim Aufbau einer zuverlässigen Abwehr, die Ihre Unternehmensinfrastruktur vor APT-ähnlichen Bedrohungen und gezielten Angriffen schützt und die Einhaltung gesetzlicher Vorschriften unterstützt, ohne zusätzliche IT-Sicherheitsressourcen zu erfordern. Komplexe Vorfälle werden schnell erkannt, untersucht und abgewehrt. Die Effizienz Ihrer IT-Sicherheit bzw. Ihres SOC-Teams wird gesteigert, indem dieses von manuellen Aufgaben entlastet wird – dank einer einheitlichen Lösung, die den Einsatz von Automatisierung maximiert und die Qualität der Ergebnisse verbessert.

Kaspersky Anti Targeted Attack bietet umfassenden Schutz vor APTs und vor besonders raffinierten Cyberbedrohungen. Sie haben die Wahl zwischen Basis- oder erweiterten NDR-Schutzfunktionen und der Kombination mit einer EDR-Lösung oder nativen XDR-Szenarien. Jetzt verfügen Ihre IT-Sicherheitsspezialisten über alle erforderlichen Tools, um komplexe Bedrohungen zu erkennen, Spitzen-Technologie einzusetzen, effektive Untersuchungen durchzuführen, proaktiv nach Bedrohungen zu suchen und schnell und zentral darauf zu reagieren.

Freie Wahl

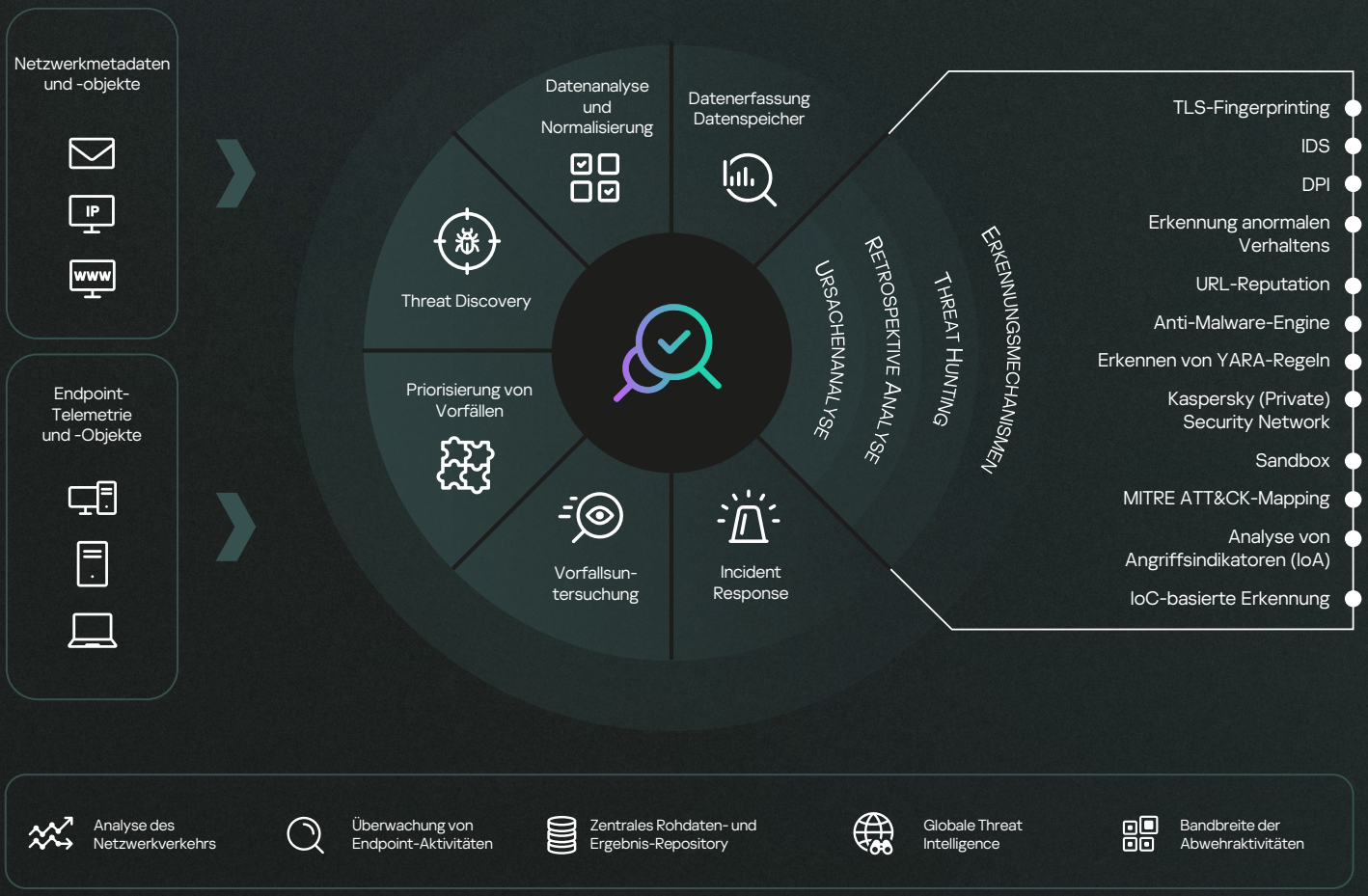
3 Schutzstufen gegen APT:

KATA → KATA NDR Enhanced → KATA Ultra

Vergleichsstudien	KATA	KATA NDR Enhanced	KATA Ultra
Essential NDR-Funktionalität • Überwachung des Datenverkehrs im Netzwerk und fortschrittliche Erkennungs-Engines • TLS-Fingerprinting • PCAP im Zusammenhang mit IDS-Warnhinweisen • URL-Reputationsanalyse • Erkennung von Eindringlingen auf Basis von IDS-Regeln (Nord-Süd) • Anleitung zur Abwehr im Netzwerk • Automatisierte Antwort auf Gateway-Ebene und ICAP-Integration mit Sperrmodus	•	•	•
Fortschrittliches Sandboxing	•	•	•
Kaspersky Threat Intelligence und MITRE ATT&CK-Anreicherung	•	•	•
Verbesserte NDR-Funktionalität • DPI für Protokolldefinition • Erkennung von Eindringlingen auf Basis von IDS-Regeln (Ost-West) • Netzwerksitzungstabelle, Netzwerkkarten, Bestandsmodul für umfassende Transparenz im Netzwerk • Analyse von Telemetriedaten aus dem Netzwerk und Endpoint-Überwachung (EPP Linux, Windows) • Schutz vor Sicherheitsrisiken im Netzwerk (nicht autorisierte Geräte, ARP-Spoofing etc.) • Speicherung und nachträgliche Analyse von Rohdaten (PCAP) • Reaktion auf Netzwerkgeräten über API-Connector • Erkennung anormalen Verhaltens • Erkennung von Schatten-IT		•	•
EDR-Expertenfunktionen			•
Native XDR-Funktionalität			•

Eine neue Dimension der Sicherheit

Kaspersky Anti Targeted Attack ist eine umfassende Schutzlösung vor APT auf Basis unserer Threat Intelligence und in Anlehnung an das Framework von MITRE ATT&CK. Alle potenziellen Angriffspunkte für Bedrohungen – Netzwerk, Web, E-Mail, PCs, Laptops, Server und virtuelle Maschinen – stehen unter Ihrer Kontrolle.



Automatisierung von Aufgaben der Bedrohungserkennung und -abwehr

optimiert die Kosteneffizienz Ihrer Sicherheits-, Incident-Response- und SOC-Teams

Nahtlose und einfache Integration

mit bestehenden Sicherheitsprodukten, Verbesserung des allgemeinen Sicherheitsniveaus und Schutz Ihrer bestehenden Sicherheitsprodukte

Vollständige Einsicht

in die IT-Infrastruktur Ihres Unternehmens

Maximale Flexibilität

für die Bereitstellung in physischen und virtuellen Umgebungen überall dort, wo Transparenz und Kontrolle erforderlich sind

Erweitern Sie Ihre Warnmeldungen mit Kaspersky Threat Intelligence

Kaspersky Threat Intelligence

Nutzen Sie umfassende Informationen, die von mehr als 100 Millionen Sensoren, umfangreichen Repositorien mit bösartigen und legitimen Dateien, dem Dark Web sowie kontinuierlichen Aktivitäten zur Bedrohungssuche und Vorfallsreaktion gesammelt wurden.

Greifen Sie direkt über die KATA-Warnungen auf das Threat Intelligence Portal zu: Analysieren Sie verdächtige Dateien, überprüfen Sie Verbindungen zu anderen Beobachtungswerten und fügen Sie umsetzbare Kontextinformationen hinzu.

Warum Kaspersky?

Globale Präsenz und internationale Anerkennung

Nachgewiesene technologische Effizienz

Transparent und Compliance-orientiert

Einmaliger Erfahrungsschatz und Know-how

Anerkannt in der gesamten IT-Sicherheitsbranche

Ausgezeichneter Kundenschutz seit 28 Jahren

Kaspersky Anti Targeted Attack

Mehr erfahren

www.kaspersky.de

#kaspersky
#bringonthefuture