AI POWERED

HORNETSECURITY

FACT SHEET

ADVANCED THREAT PROTECTION

KI-gestützter, erweiterter Schutz von E-Mails und Daten, selbst vor den raffiniertesten Bedrohungen.

Cyberkriminelle arbeiten unermüdlich an der Entwicklung neuer Cyberbedrohungen, was es für Sicherheitssoftware schwierig macht, mitzuhalten und Benutzer vor neu aufkommenden Angriffsmethoden zu schützen. Ransomware, CEO-Betrug, Spear-Phishing und Blended Attacks sind nur Beispiele für die Gefahren, die im Cyberspace lauern.

Mit dem Aufkommen weithin verfügbarer KI-Tools können Cyberkriminelle mühelos makellos aussehende Phishing-E-Mails erstellen und sogar Sicherheitsvorkehrungen umgehen und KI-Textgenerierungstools verwenden, um bösartige Codes zu erstellen.

Mit Advanced Threat Protection müssen Sie sich um nichts von dem oben genannten Sorgen machen. Advanced Threat Protection nutzt KI zu seinem Vorteil, schützt Sie vor Zero-Day-Angriffen und selbst den raffiniertesten Bedrohungen und sorgt dafür, dass Sie Cyberkriminellen immer einen Schritt voraus sind.

Was ist betroffen?

E-Mail Kommunikation

Wie kann Ihnen Advanced Threat Protection helfen?

KI-basierte zielgerichtete Forensik

Erkennen Sie brandneue und selbst die raffiniertesten Bedrohungen.

Sandbox-Engine

Testet E-Mail-Anhänge in einer kontrollierten Umgebung auf bösartige Dateien.

Reporting

Verschaffen Sie sich einen umfassenden Überblick über alle Angriffsversuche, Sicherheitswarnungen, ATP-Berichte und forensische Informationen.

Was verbessert sich?

Sichere E-Mail-Postfächer

FILETYPES	BINARY ANALYTICS	SANDBOX 500+ BEHAVIOURAL ANALYSIS SENSORS	REPORTING AND DATA ANALYTICS
EXE	MACRO	ANTI VM EVASION DETECTION	LIVE THREAT MONITOR
PDF	OBFUSCATION	MACHINE LEARNING ENGINE	SECURITY ALERTS
OFFICE	URL	FILESYSTEM MONITOR	ATP-REPORTS
ARCHIVE	OBJECTS	NETWORK TRAFFIC ANALYSIS	FORENSIC INFORMATION
	METADATA	PROCESS- AND REGISTRY MONITOR	
	JAVASCRIPT	FORENSIC MEMORY ANALYSIS	
	HEURISTIC		
	STATIC ANALYSIS		
	ZERO HOUR THREAT OUTBREAK DETECION		

Advanced Threat Protection Sandbox vs. Ransomware & Polymorphe Viren

HORNETSECURITY

FACT SHEET

ATP-Engines	Funktionsweise und Vorteile
Sandbox Engine	Dateianhänge werden in einer Vielzahl verschiedener Systemumgebungen ausgeführt und ihr Verhalten analysiert. Stellt sich heraus, dass es sich um Malware handelt, werden Sie benachrichtigt. Schützt vor Ransomware und Blended Attacks.
Secure Links	Kein riskantes Anklicken von Links in E-Mails mehr. Secure Links ersetzt den ursprünglichen Link durch eine umgeschriebene Version, die über das sichere Web-Gateway von Hornetsecurity führt. Secure Links nutzt künstliche Intelligenz, einschließlich Machine Learning und Deep Learning, um fortschrittlichen Schutz vor Phishing zu bieten, selbst bei kurzfristigen, sehr gezielten Angriffen.Überwachte und unüberwachte Machine-Learning-Algorithmen analysieren mehr als 47 Merkmale von URLs und Webseiten und scannen nach bösartigen Verhaltensweisen, Verschleierungstechniken und URL-Weiterleitungen. Zeitgleich analysieren Computer-Vision-Modelle Bilder, um relevante Merkmale, häufig genutzt bei Phishing-Angriffen, zu extrahieren, einschließlich Markenlogos, QR-Codes und verdächtigem Textinhalt eingebettet in Bildern.
URL Scanning	An eine E-Mail angehängte Dokumente (z.B. PDF, Microsoft Office) können Links enthalten. Diese lassen sich jedoch nicht ersetzen, da dies die Integrität des Dokumentes verletzen würde. Die URL Scanning Engine belässt das Dokument in seiner Originalform und prüft ausschließlich das Ziel dieser Links.
Freezing	Nicht sofort eindeutig klassifizierbare, aber verdächtige E-Mails werden per Freezing über einen kurzen Zeitraum zurückgehalten. Anschließend erfolgt eine weitere Prüfung mit aktualisierten Signaturen. Schützt vor Ransomware, Blended Attacks und Phishing-Angriffen.
Malicious Document Decryption	Verschlüsselte E-Mail Anhänge werden durch passende Textbausteine innerhalb einer E-Mail entschlüsselt. Das entschlüsselte Dokument wird schließlich einer tiefergehenden Virenüberprüfung unterzogen.
KI-unterstützte Targeted Fraud Forensics	**Fraud attempt analysis:** Prüft die Authentizität und Integrität von Metadaten und Mailinhalten. **Identity spoofing recognition:** Erkennung und Blockierung gefälschter Absender-Identitäten. **Intention recognition system:** Alarmierung bei Inhaltsmustern, die auf bösartige Absichten schließen lassen. **Spy-out detection:** Spionageabwehr von Attacken zur Erlangung schützenswerter Informationen. **Feign facts identification:** Inhaltsanalyse von Nachrichten auf Basis von Vorspiegelung fingierter Tatsachen. **Targeted attack detection:** Erkennung gezielter Angriffe auf einzelne Personen.
QR Code Analyzer	Der QR-Code-Analyzer von Hornetsecurity kann QR-Codes erkennen, die direkt in eine E-Mail oder ein Bild eingebettet sind. Alle QR-Codes werden erkannt und mit Lichtgeschwindigkeit auf bösartige Inhalte gescannt. Der QR-Code-Analyzer unterstützt alle gängigen Bildtypen wie GIF, JPEG, PNG und BMP.