

Wenn Sekunden entscheiden, reicht Erkennung allein nicht mehr

Der Alert ist da. Jetzt beginnt die Risikobewertung. KI automatisiert Angriffe, die Zahl exponierter Systeme wächst, Reaktionsfenster schrumpfen. Damit müssen Risiken schneller bewertet werden. Managed Detection & Response verdichtet erkannte Signale zu einer belastbaren Entscheidungsgrundlage für wirksame Cyber Defence.

DER AUTOR

Michael Stampfli
Head of Cyber Defence Services
& Operations, Infoguard

Ein Alarm markiert selten den Anfang eines Angriffs. Meist zeigt er einen Vorfall, der sich längst entwickelt hat. Cyberangriffe passen sich heute innerhalb weniger Stunden an neue Gegebenheiten an. KI automatisiert Angriffsschritte, skaliert Kampagnen und verkürzt die Zeit zwischen Schwachstelle und Ausnutzung. Gleichzeitig erweitern Cloud-Services, digitale Lieferketten und hybride IT-Umgebungen die Angriffsfläche kontinuierlich. Für Security-Teams wächst damit der Druck, Sicherheitsereignisse rasch und richtig einzuordnen.

Managed Detection & Response (MDR) verdichtet Signale zu zusammenhängenden Angriffsmustern, priorisiert Risiken und macht Handlungsbedarf sichtbar. Damit schafft MDR die Basis für fundierte Entscheidungen in der modernen Cyber Defence.

Von der Erkennung zur fundierten Entscheidung

MDR bleibt das Fundament moderner Cyberabwehr. Die Herausforderung besteht darin, aus immer mehr Signalen rasch tragfähige

Entscheidungen abzuleiten. MDR vollzieht den Wandel von der Ereigniserkennung zur kontextbasierten Entscheidungsfähigkeit. Threat Intelligence liefert den Angreiferkontext, XDR verbindet technische Signale über Systeme hinweg, während Zero Trust unkontrollierte Zugriffe und laterale Bewegungen erschwert.

Erst ihr Zusammenspiel schafft die Grundlage, Risiken im Unternehmenskontext richtig einzuordnen und den Handlungsbedarf fundiert zu bewerten. KI korreliert die Ereignisdaten, priorisiert Risiken und verdichtet sie zu einem belastbaren Lagebild. Der Mensch entscheidet. Human-AI-Teaming verbindet die Geschwindigkeit von KI mit menschlichem Urteilsvermögen und Erfahrung. Je stärker KI Entscheidungen unterstützt, desto wichtiger wird die Frage, unter welchen Bedingungen sie arbeitet.

Vertrauenswürdige KI braucht Kontrolle

Sobald KI sicherheitskritische Daten verarbeitet, werden Vertrauen, Transparenz, Kontrolle und Datenhoheit zentral. AI by Design verankert Datenschutz, Governance und Nachvollziehbarkeit von Beginn an in der KI-Architektur. Vertrauenswürdige KI setzt kontrollierte Betriebsbedingungen voraus.

Die LLM-Datenprozessierung richtet sich nach den Anforderungen an Datensouveränität, Governance und Compliance: in der EU, in der Schweiz oder – bei kritischen Infrastrukturen – auf dedizierter KI-Hardware im eigenen Land. So bleiben Datenflüsse kontrolliert und die Verarbeitung nachvollziehbar.

Entscheidungsfähig unter Zeitdruck

Bei einem Cyberangriff zählt jede Minute. MDR hilft, Angriffsmuster schneller zu erkennen, Sicherheitslücken gezielt zu priorisieren und Entscheidungen kontrolliert vorzubereiten. KI verdichtet Analysen und Kontext zu einer verlässlichen Entscheidungsgrundlage. Fachpersonen bewerten die Lage, klare Verantwortlichkeiten machen Entscheidungen nachvollziehbar. So stärkt MDR die Governance und hält Organisationen auch unter Druck handlungsfähig.

Künftig entscheidet die Qualität der Cyberabwehr stärker darüber, wie rasch Organisationen Risiken verstehen, Prioritäten setzen und fundiert handeln können. Dafür führt MDR KI-gestützte Analyse, menschliches Urteilsvermögen und kontrollierte Datenverarbeitung zusammen. So verbindet modernes MDR schnelle Sicherheitsentscheidungen mit Kontrolle und Vertrauen.



BILD: THUNDERTURBO - ADOBE STOCK.COM / GEMINI

« KI verarbeitet Daten, Analysten entscheiden »

KI beschleunigt nicht nur Cyberangriffe, sondern auch deren Abwehr. Im Interview erklärt Michael Stampfli, Head of Cyber Defence Services & Operations bei Infoguard, wie KI Sicherheitsanalysten unterstützt und warum sie den Menschen nicht ersetzt. Interview: Dylan Windhaber



Wie verändert KI die Bedrohungslandschaft?

Michael Stampfli: KI beschleunigt, skaliert und verfeinert bekannte Angriffsmethoden wie Phishing und Social Engineering. Für unser Cyber Defence Center bedeutet das mehr relevante Signale, professionellere Täuschungsversuche und weniger Zeit für ihre Einordnung.

Welche Rolle spielt MDR?

MDR verknüpft Ereignisse, priorisiert Risiken und liefert früh Handlungsempfehlungen. So schafft Verdichtung eine belastbare Entscheidungsgrundlage, damit Unternehmen früher und fundierter handeln können.

Was macht aus einem Alert eine Entscheidung?

Ein Alert signalisiert zunächst nur eine Auffälligkeit. Entscheidend sind Einordnung und Reaktion. Im Alltag zählen drei Fragen: Was ist passiert? Wie relevant ist das Ereignis? Was ist zu tun? Antworten entstehen erst, wenn Signale aus Endpoint-, Identitäts-, Netzwerk-, Cloud- und E-Mail-Daten zusammenfliessen. KI reichert Daten an, gruppiert Alerts, priorisiert Ereignisse, erstellt Attack Stories und schlägt Analyseschritte vor. Im Zusammenspiel mit unseren Analystinnen und Analysten entsteht daraus Human-AI-Teaming: KI verarbeitet Daten, unsere Fachpersonen entscheiden. Sie bewerten Hypothesen im Kundenkontext und steuern die Response.

Wie bleibt KI unter Kontrolle?

Kontrolle beginnt mit klaren Vorgaben. Gerade Security-Telemetrie

ist besonders sensibel, da sie Rückschlüsse auf Identitäten, Berechtigungen, Schwachstellen und kritische Geschäftsprozesse erlaubt. Deshalb müssen Unternehmen bestimmen, wie und wo Daten verarbeitet werden. Je nach Anforderungen geschieht dies in der Schweiz, in der EU oder in isolierten Umgebungen. Kritische Infrastrukturen können verlangen, dass ihre Security-Telemetrie die Schweiz nie verlässt. Dabei muss nachvollziehbar sein, wozu und wie lange Daten verarbeitet werden. AI by Design sorgt dabei für Datenminimierung, sichere Datenflüsse und vollständige Nachvollziehbarkeit.

Was bleibt die Aufgabe des Menschen?

Der Mensch behält die Verantwortung. Kritische Response-Massnahmen erfolgen entweder nach menschlicher Freigabe oder innerhalb klar definierter Regeln. So verbindet Human-AI-Teaming die Geschwindigkeit von KI mit menschlichem Urteilsvermögen.

Was bedeutet das konkret?

Das Team konzentriert sich stärker auf Validierung, Kontextbewertung, Qualitätssicherung und Kundenkommunikation. KI übernimmt dafür Aufgaben wie Konsolenwechsel und Datenaufbereitung, verdichtet Einzelsignale zu Attack Stories und macht Beziehungen zwischen Identitäten, Endgeräten und Cloud-Ressourcen sichtbar. Reasoning-Komponenten erkennen Informationslücken, weitere Prüfungen schlägt die KI vor. Verantwortung und Entscheidung bleiben beim Menschen – die Ergebnisse nachvollziehbar.

Was macht Cyber Defence mit KI resilient?

An erster Stelle steht eine verlässliche Datenbasis. Unternehmen müssen ihre kritischen Assets, Identitäten und Geschäftsprozesse kennen und deren Telemetrie verknüpfen können. Ebenso zentral ist eine verbindliche KI-Governance. Sie definiert Daten, Modelle, Verarbeitungsorte, Automatisierungen und Freigaben.

Was heisst das für Ihr Team?

Das Team muss lernen, KI zu nutzen, ohne ihr blind zu vertrauen. Sie prüfen Ergebnisse anhand der Evidenz, erkennen Grenzen und hinterfragen Einschätzungen. Playbooks, Eskalationswege und Übungen übersetzen Erkenntnisse rasch in wirksames Handeln. Resiliente Unternehmen begrenzen Auswirkungen und lernen aus Vorfällen. Entscheidend sind Transparenz, klare Regeln und KI dort einzusetzen, wo sie Entscheidungen verbessert.

« Das Team muss lernen, KI zu nutzen, ohne ihr blind zu vertrauen. »

Michael Stampfli, Head of Cyber Defence Services & Operations, Infoguard



Das Dossier
finden Sie auch
online
netzwoche.ch