ARCTIC WOLF

CYBERRISIKEN BESEITIGEN

WHITEPAPER

Hybrid-KI ist die effektivste Verteidigung der Cybersecurity-Branche

Die heutige Bedrohungslage ist enorm komplex und entwickelt sich ständig weiter. Deshalb ist es für KI-basierte Lösungen derzeit unmöglich, den menschlichen Faktor in der Schleife zu eliminieren und gleichzeitig ein starkes Sicherheitsniveau aufrechtzuerhalten.

Künstliche Intelligenz (KI) und Machine Learning (ML) werden zunehmend eingesetzt, um die nächste Generation von Cybersecurity-Lösungen zu entwickeln. Diese Lösungen erleichtern es Unternehmen, komplexe Cyberangriffe zu erkennen, und senken gleichzeitig die Kosten für die Verwaltung der Lösungen. Leider haben viele Menschen eine falsche Vorstellung von KI. Sie stellen sich die Maschine als menschenähnliches Gehirn vor, das komplexe Aufgaben bewältigen kann und den Bedarf an Sicherheitsexperten für die Verwaltung der Lösungen reduziert. Das ist nicht der Fall. Die heutige Bedrohungslage ist enorm komplex und entwickelt sich ständig weiter. Deshalb ist es für KI-basierte Lösungen derzeit unmöglich, den menschlichen Faktor in der Schleife zu eliminieren und gleichzeitig ein starkes Sicherheitsniveau aufrechtzuerhalten.

In diesem Whitepaper werden die Cybersecurity-Herausforderungen für den Markt sowie die Grenzen von KI- und Machine-Learning-Lösungen für Cybersecurity erläutert. Es geht darauf ein, warum menschlich unterstütztes Machine Learning erforderlich ist, um diese Herausforderungen zu bewältigen, und wie Arctic Wolf Hybrid-KI und andere unterstützende Funktionen in unserer Cloud-basierten Security-Operations-Plattform einsetzt, um die effektivste Cybersecurity-Abwehr und Incident Response zu bieten.

Cybersecurity-Herausforderungen für den Markt

Sicherheitsverletzungen sorgen fast täglich für Schlagzeilen. Ein bekanntes Beispiel ist die Kreditauskunftei Equifax, bei der durch einen Angriff private Informationen von 143 Millionen Menschen (der Hälfte der US-Bevölkerung) offengelegt wurden. Von Ransomware-Angriffen wie WannaCry und Petya waren Hunderte von Krankenhäusern und Kliniken, Produktionsstätten und Point-of-Sale-Terminals auf der ganzen Welt betroffen. Niemand ist gegen derartige Cyberangriffe immun, und viele Unternehmen stehen denselben Herausforderungen gegenüber:

Zu viele Warnungen, zu viele Daten:

Viele Unternehmen haben Produkte für die Perimeter- und Endgerätesicherheit angeschafft, um sich vor gängigen Cyberbedrohungen zu schützen. Was fehlt, ist eine Lösung, die einen zentralen Überblick über alle Produkte hinweg bietet. Jedes dieser Einzelprodukte produziert täglich Hunderte von Protokolldatensätzen, was bei den begrenzten IT-Mitarbeitern zu Alarmmüdigkeit führt.

Mangel an Cybersecurity-Experten:

Mit der Zunahme von Cyberangriffen steigt auch die Nachfrage nach Sicherheitsexperten. Angesichts des enormen Mangels an Security-Experten in der Branche ist es für viele Unternehmen unmöglich, entsprechende Stellen dauerhaft zu besetzen. Das vorhandene IT-Personal arbeitet an der Belastungsgrenze, und es fehlen die nötigen Sicherheitskenntnisse, um komplexe Bedrohungen zu finden und zu priorisieren sowie Risiken zu mindern.

Mangel an verwertbaren Informationen:

In puncto Cybersecurity mangelt es nicht an Daten in Protokollaufzeichnungen, sondern an kontextbezogenen Informationen über Urheber, Art, Zeitpunkt, Ursprung und Ziel des Angriffs sowie über die erforderlichen Maßnahmen, um das Risiko mindern. Hier machen die neueste Threat Intelligence und menschliches Fachwissen einen großen Unterschied.

Mit menschlicher Interaktion (Human in the Loop, HITL) können Sicherheitsexperten Machine Learning mit Threat Intelligence nutzen, um je nach Modell sowohl bekannte Malware-Stämme als auch Zero-Day-Exploits zu erkennen. Bei den neueren Stämmen sollten Sicherheitsanalysten das Verhalten der gesamten Kill Chain untersuchen und zusätzliche Threat-Intelligence-Parameter ermitteln, um den neuen Malware-Stamm genau zu klassifizieren. Anschließend können sie das Machine-Learning-Modell so optimieren, dass der neue Malware-Stamm in der Zukunft jederzeit automatisch erkannt wird.

Arctic Wolf Security Operations mit Hybrid-KI

Als Marktführer im Bereich Security Operations kennt Arctic Wolf die Grenzen von KI für die Cybersecurity und nutzt Hybrid-KI, um das Beste aus beiden Welten zu vereinen.

Hybrid-KI verbindet menschliche Intelligenz mit der Leistungsfähigkeit von Maschinen, um eine exponentiell bessere Bedrohungserkennung zu bieten, Fehlalarme erheblich zu reduzieren und die Zeit zwischen Erkennung und Reaktion zu verkürzen. Sie überträgt die praktische Erfahrung und Intuition des Concierge Security® Teams bei der Behandlung von Sicherheitsvorfällen auf das Machine Learning, um die Erkennungsfunktionen zu verbessern und zu verfeinern.

Die Rolle von KI für die Cybersecurity

Die benötigte Analysekapazität, um riesige Datenmengen aus Tausenden von Quellen zu verarbeiten, übersteigt bei weitem die kognitiven Fähigkeiten eines einzelnen Menschen. Mit der überlegenen Rechenkapazität von Maschinen lässt sich dieses Problem angehen. Das steigert den Bedarf an KI für Cybersecurity-Lösungen allgemein. KI kann der menschlichen Intelligenz und Intuition jedoch noch nicht das Wasser reichen. CISOs müssen dies berücksichtigen, wenn sie sie als Teil ihrer Security-Operations-Infrastruktur in Betracht ziehen.

Dies sind die beiden wichtigsten Arten von Machine Learning, die in allen KI-Systemen zum Einsatz kommen – je nach Ausrichtung einzeln oder in Kombination.

Beaufsichtigtes Machine Learning: Bei diesem Ansatz wird ein Machine-Learning-Modell durch die Verstärkung positiver Ergebnisse verfeinert. Die Erkennung basiert auf einer gewissen Menge „bekannter“ Bedrohungsdaten, die als Beispiele gekennzeichnet und dem Modell zur Verfügung gestellt werden. Auf dieser Grundlage kann das Modell Bedrohungen klassifizieren und Angriffe genau identifizieren. Dies ist vergleichbar damit, bei einer neuen Gruppe von Patienten anhand von Parametern wie Größe, Gewicht, Alter und Blutzuckerspiegel „bekannter“ Diabetespatienten die Veranlagung für eine Krankheit wie Diabetes zu prognostizieren.

Unbeaufsichtigtes Machine Learning: Bei diesen Modellen basiert die Erkennung auf anomalen Mustern, die automatisch aus großen, nicht gekennzeichneten Datensätzen extrahiert werden. Wenn Sie nicht wissen, nach welchen Bedrohungsparametern Sie suchen sollen, können diese Modelle Muster erkennen, die für Menschen möglicherweise nicht erkennbar wären. In der Lernphase führt dies tendenziell zu viel mehr falsch positiven Meldungen und Warnungen und könnte Alarmmüdigkeit und betriebliche Ineffizienz nach sich ziehen. Dies ist vergleichbar mit der Identifizierung eines neuen Virusstamms (ähnlich einem Zero-Day-Angriff), bei dem die Ursachen der Krankheit noch nicht bekannt sind.

Wie jede moderne Technologie muss sowohl überwachtes als auch unüberwachtes Machine Learning nach der Implementierung gepflegt werden. Cyberkriminelle ändern kontinuierlich ihre Vorgehensweise und finden neue Bereitstellungsmethoden, um bestehende Cyber-Abwehrmaßnahmen mit Machine-Learning-Verfahren zu umgehen. Daher ist menschliches Fachwissen erforderlich, um Fehlalarme herauszufiltern und die Algorithmen mithilfe guter Bedrohungsdaten und Threat Intelligence zu verfeinern.

Hybrid-KI – Das Potenzial von KI für die Cybersecurity ausschöpfen

Sehen wir uns an, warum ein Hybrid-KI-Ansatz mit menschlicher Interaktion unerlässlich ist, um das volle Potenzial von KI auszuschöpfen und neue Ransomware-Stämme genau zu erkennen.

Umgebungen, die sich für die Implementierung von Machine-Learning-Lösungen ohne angemessene menschliche Beteiligung entscheiden, stellen möglicherweise fest, dass diese Tools ihre Sicherheitslage tatsächlich eher beeinträchtigen. Die Implementierung von Machine Learning ohne angemessenes Management könnte dazu führen, dass die Modelle entweder eine hohe Rate an falsch positiven Ergebnissen und Fehlalarmen erzeugen oder die Erkennung gänzlich fehlschlägt. Das ist, als würde man eine Überwachungskamera installieren, ohne darauf zu achten, dass sie scharfe Bilder liefert oder in die richtige Richtung zeigt. Ohne die richtige Abstimmung und Verwaltung vermittelt sie nur ein falsches Sicherheitsgefühl.

Arctic Wolf Concierge Security® Team (CST)

Das CST ist für jeden Kunden von Arctic Wolf der erste Ansprechpartner. Es erweitert Ihr internes Team, kennt Ihre Netzwerkinfrastruktur und Geschäftsrisiken und verfügt über das Sicherheits-Know-how, um komplexe Bedrohungen zu erkennen und Abwehrmaßnahmen vorzuschlagen.

Das CST ist für jeden Kunden von Arctic Wolf der erste Ansprechpartner. Es erweitert Ihr internes Team, kennt Ihre Netzwerkinfrastruktur und Geschäftsrisiken und verfügt über das Sicherheits-Know-how, um komplexe Bedrohungen zu erkennen und Abwehrmaßnahmen vorzuschlagen. Das CST fungiert als Ihr vertrauenswürdiger Berater, berichtet regelmäßig über die Effektivität Ihres Sicherheitsniveaus und führt Geschäftsprüfungen durch, um strategische Einblicke in Ihre Cybersecurity-Investitionen zu liefern.

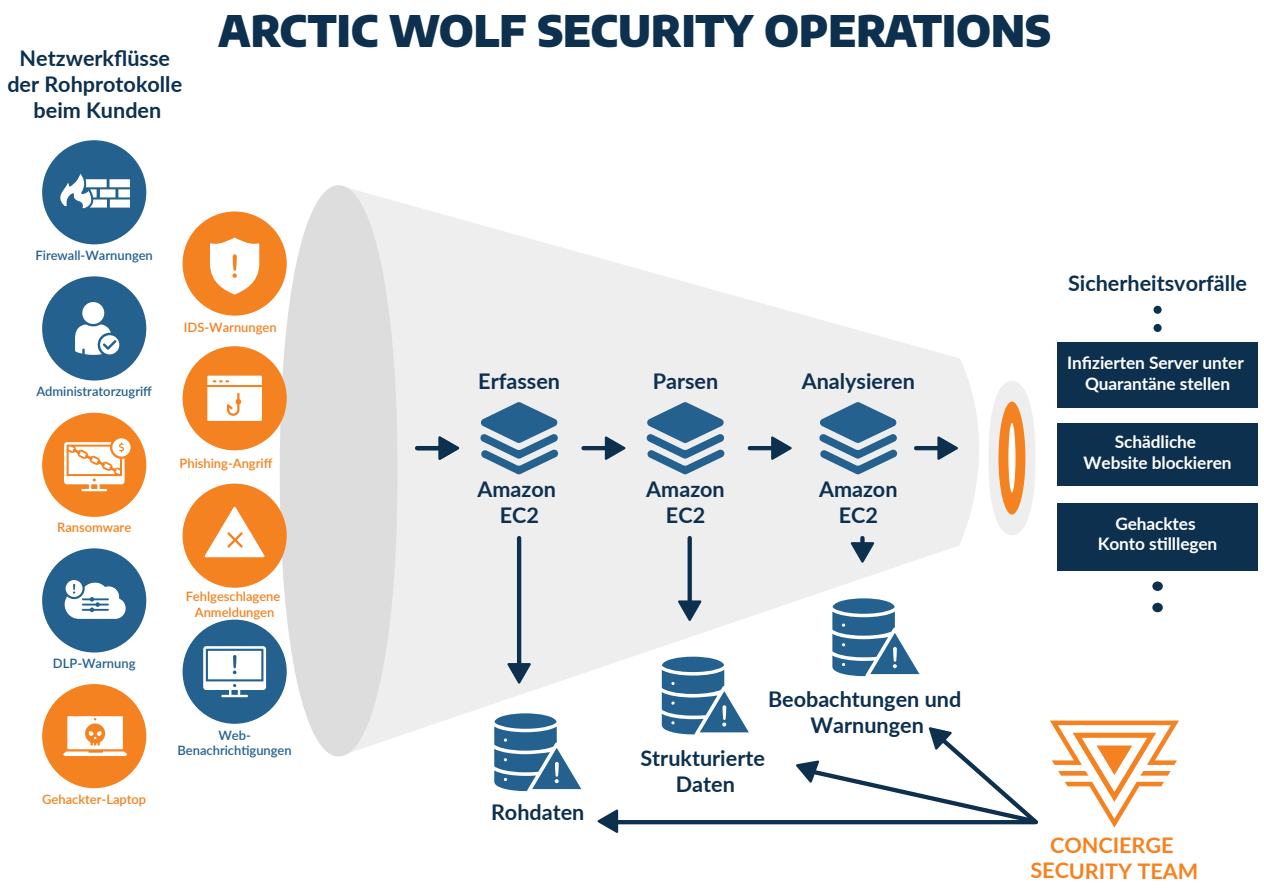
Das CST verwendet die folgenden einzigartigen Funktionen der Arctic Wolf Security Operations Platform, um neue Daten zu integrieren, unerwartete Ereignisse zu verarbeiten und mit zusätzlichem Kontext den branchenweit besten Schutz zu bieten.

Sicherheitsoptimierte Datenarchitektur

Die Security-Operations-Plattform von Arctic Wolf ist Cloud-basiert und beruht auf einer hoch skalierbaren, mandantenfähigen Architektur, die für die Verarbeitung von Sicherheitsereignissen optimiert ist. Sie erfasst über 65 Milliarden Ereignisse pro Tag, die sie analysiert und anschließend zu strukturierten Beobachtungen aggregiert.

Die Daten werden dann mithilfe von Verhaltensanalysen und Cyberbedrohungs-Informationen analysiert, um nur die schwerwiegendsten Vorfälle für alle Kunden zu eskalieren. Dies führt zu einer 99,9997%igen Reduzierung der Anzahl von Vorfällen, die ein Eingreifen des Kunden erfordern – auf im Durchschnitt weniger als einen Sicherheitsvorfall pro Woche und Kunde.

Wie in der Abbildung unten gezeigt, nutzt die Arctic Wolf® Platform die Cloud-Infrastruktur von Amazon Web Services (AWS), um Computing- und Speicherressourcen mithilfe von AWS Elastic Computing (EC2) und Simple Storage Services (S3) dynamisch zu skalieren. Dadurch kann Arctic Wolf unbegrenzte Mengen an Rohprotokollen von mehreren Kunden aufnehmen, parsen und analysieren und dem CST dennoch schnellen Zugriff auf sicherheitsrelevante Daten auf jeder Ebene gewähren – roh, strukturiert oder Beobachtungen/Warnungen.



Mehrere Schleifen für Machine Learning

Der Hybrid-KI-Ansatz kann eine zehnmal höhere Genauigkeit als die normale KI-basierte Technologie bieten, da er mehrere Lernschleifen verwendet, um Sicherheitsvorfälle zu verfeinern und Fehlalarme in jeder Phase des Erfassungs-, Parsing- und Analyseprozesses herauszufiltern.

Mensch-zu-Mensch-Lernschleife:

Das CST interagiert während des Onboardings mit dem Kunden, kennt die Geschäftsrisiken des Kunden und entwickelt eine Baseline für den normalen Betrieb. Dies ermöglicht die Erkennung von Anomalien innerhalb der Kundentelemetrie. Das CST bietet regelmäßige Updates und Berichte zum Sicherheitsniveau eines Kunden und eskaliert Sicherheitsvorfälle nur dann, wenn Maßnahmen zur Minderung/Behebung geschäftskritischer Probleme erforderlich sind.

Mensch-zu-Maschine-Lernschleife:

Das CST legt anpassbare Sicherheitsrichtlinien in der Arctic Wolf Platform fest, um unsere Customizable Rules Engine (CRulE) zu verfeinern und falsch positive Meldungen zu eliminieren sowie komplexe Bedrohungen mithilfe konfigurierbarer Richtlinien zu erkennen. Diese konfigurierbaren Richtlinien können allgemein auf alle Kunden angewendet und dennoch an die speziellen Bedürfnisse eines bestimmten Kunden angepasst werden.

Maschine-zu-Maschine-Lernschleife:

Die Plattform verwendet Threat Intelligence und Verhaltensanalysen in Korrelation mit Regeln, um die neuesten Bedrohungen genau zu identifizieren. Sie nutzt eine Vielzahl von Threat-Intelligence-Daten wie Software-Schwachstellen, komplexe Malware, neue Netzwerkbedrohungen und webbasierte Bedrohungen.

Anpassbare Sicherheitsrichtlinien

Das CST verwendet die Customizable Rules Engine (CRulE), um benutzerdefinierte Sicherheitsrichtlinien zu definieren und:

Fehlalarme zu eliminieren:

Diese benutzerdefinierten Regeln filtern selektiv Ereignisse heraus, die Fehlalarme verursachen und kein echtes kundenspezifisches Sicherheitsrisiko darstellen, und ermöglichen die Eliminierung von Fehlalarmen.

bekannte Bedrohungen zu erkennen:

Diese Regeln identifizieren Cyberangriffe, die von bekannten bösartigen IP-Adressen und Websites/URLs ausgehen, oder mutmaßliche Ransomware-Angriffe, die bekannte Command-and-Control-Server für den Austausch von Verschlüsselungsschlüsseln verwenden.

unbekannte Bedrohungen zu erkennen:

Diese Regeln identifizieren sich entwickelnde und schwer zu identifizierende Angriffe – z. B. neue Phishing-Versuche oder die Kompromittierung von Anmeldeinformationen –, wenn die Arctic Wolf Platform ungewöhnliches Verhalten erkennt. Dies kann ungewöhnliche Aktivitäten privilegierter Benutzer oder häufige fehlgeschlagene Anmeldeversuche bei Active Directory umfassen.

Das Beste aus beiden Welten

Die Einbindung von Menschen kann die Ergebnisse von KI und Machine Learning erheblich verbessern.

Maschinen und Algorithmen eignen sich hervorragend zur Automatisierung bekannter Mengen, doch die korrekte Kategorisierung neuer Bedrohungsdaten erfordert oft menschliches Eingreifen. Die Verwendung von Machine Learning zur Klassifizierung bösartiger und harmloser Aktivitäten, während sich der Mensch auf die Grauzonen konzentriert, ist die effektivste Kombination, um die heutige Bedrohungslage mit ständig weiterentwickelten Cyberangriffen zu bekämpfen.

Arctic Wolf Security Operations mit Hybrid-KI verbindet die Vorteile von KI mit dem Know-how des CST, um unseren Kunden das Beste aus beiden Welten zu bieten. Die Verbindung von menschlicher Intelligenz mit maschinellen Skalierungsmöglichkeiten ergibt eine erfolgreiche Kombination, die es CISOs ermöglicht, KI für erstklassige Security Operations zu nutzen.

Über Arctic Wolf

Arctic Wolf® ist Marktführer im Bereich Security Operations. Mit der Cloud-nativen Arctic Wolf® Platform unterstützen wir Unternehmen dabei, Cyberrisiken abzuwehren, indem wir Security Operations als Concierge-Service anbieten. Hochqualifizierte Concierge Security® Experten arbeiten als Erweiterung Ihres Teams rund um die Uhr an der Überwachung, Erkennung und Abwehr sowie an kontinuierlichem Risiko-Management, um Systeme und Daten proaktiv zu schützen und gleichzeitig Ihr Sicherheitsniveau kontinuierlich zu stärken. Wir bieten jetzt auch Managed Security Awareness-Schulungen an, um Ihre Mitarbeiter besser über sicherheitsrelevante Best Practices und effektive Reaktionen auf Social-Engineering-Angriffe zu informieren und sie entsprechend vorzubereiten.

Weitere Informationen über Arctic Wolf finden Sie unter arcticwolf.com

Kontakt

arcticwolf.com
1.888.272.8429
ask@arcticwolf.com