Silverfort

Resilienz gegen KI-basierte Angriffe aufbauen

Ein Readiness-Leitfaden für Identity- und Security-Teams

Inhaltsverzeichnis

KI-basierte Angriffe warten nicht. Ihre Abwehrmaßnahmen sollten es auch nicht.

Dieser Leitfaden richtet sich an Identity- und Security-Fachleute, die sich der schwierigen Frage der Unternehmensleitung stellen müssen: „Sind wir vorbereitet?“

Gemeinsam mit Mitgliedern von Glasswing haben wir Mythos in deren Umgebungen getestet und ihre Sicherheitsmaßnahmen optimiert, um Angriffe mit offensiver KI abzuwehren. Mit diesem Leitfaden tappen Sie nicht länger im Dunkeln, sondern können mit der Vorbereitung beginnen – ausgestattet mit dem nötigen Kontext, dem Wissen und einem Playbook, um sich fundiert und zielführend zur KI-Readiness Ihrer Organisation äußern zu können.

Inhalt und Verwendung dieses Leitfadens:

1. **Die Bedrohung verstehen:** Was sind Frontier-KI-Modelle wie Mythos, wie funktionieren KI-basierte Angriffe und warum sind die Sicherheitstools, auf die Sie sich heute verlassen, nicht für diese Art von Angriffen konzipiert?
2. **Das Readiness Assessment durchführen:** Fünf Fragen, die aufzeigen, wo Sie hinsichtlich Ihrer Bereitschaft und potenziellen Resilienz stehen. Das Ergebnis können Sie als Grundlage für das Gespräch mit der Unternehmensleitung nutzen.
3. **Die Checkliste verwenden:** Ein nach Prioritäten gegliedertes Playbook, mit dem Sie die Schwachstellen beseitigen können, die KI-basierte Angriffe am häufigsten ausnutzen.

Was ist Mythos und warum ist es für Security-Verantwortliche von Bedeutung?

Frontier-KI-Modelle verändern die Cybersicherheits-landschaft schneller, als den meisten Unternehmen bewusst ist.

Mythos von Anthropic wurde für komplexe Untersuchungen im Bereich der Cybersicherheit und für autonome Penetrationstests entwickelt. Es erfindet keine grundlegend neuen Angriffstechniken. Was es jedoch interessant macht, ist seine Fähigkeit, bestehende Techniken autonom mit maschineller Geschwindigkeit und in großem Maßstab auszuführen – und zwar kontinuierlich, adaptiv und ohne menschliches Zutun.

Mythos kann kontinuierlich Identitäten erfassen, Zugangsdaten testen, häufige Fehlkonfigurationen miteinander verketten, per Lateral Movement innerhalb von Systemen vordringen, Berechtigungen ausweiten und Daten exfiltrieren – und das in einem einzigen, ununterbrochenen Ablauf über mehrere mögliche Angriffspfade hinweg gleichzeitig. Auch ohne die Entwicklung völlig neuer Angriffstechniken beschleunigt es bestehende Techniken erheblich. Zudem verbessert es ihre Persistenz und Präzision im Vergleich zu jeder von Menschen durchgeführten Kampagne. Mythos findet und nutzt nicht nur Schwachstellen besser, sondern verändert auch die Wirtschaftlichkeit und das Tempo von Cyberangriffen grundlegend. Das System kennt keine Pausen, keine Ermüdung und kein Zögern – und es benötigt keinerlei menschliche Eingriffe.

Die Branche hat Jahre mit der Entwicklung von Abwehr-maßnahmen verbracht, die auf der Annahme beruhen, dass zwischen den Aktionen des Angreifenden und der Reaktion des Abwehrenden ein nennenswerter zeitlicher Abstand besteht. KI-basierte Angriffe heben dieses Reaktionsfenster vollständig auf. Zum Zeitpunkt der Auslösung des Alarms könnte der Angriff bereits abgeschlossen sein.

Dies stellt eindeutig eine Weiterentwicklung der Angreifer-Tools dar – vor allem aber ist es ein struktureller Wandel in der Art und Weise, wie Angriffe ablaufen. Und viele Unternehmen haben festgestellt, dass Angriffe nicht unbedingt über Malware oder Endgeräte erfolgten, sondern auf Identitätsebene – und genau dort können sie auch abgewehrt werden.

„Wir haben Mythos auf unser eigenes System angewendet. **Innerhalb weniger Stunden** hatte es alle Vertrauensbeziehungen in unserer Umgebung kartiert und sich per Lateral Movement auf eine Weise im System bewegt, **die für unser SOC völlig unsichtbar war.**“

- CISO

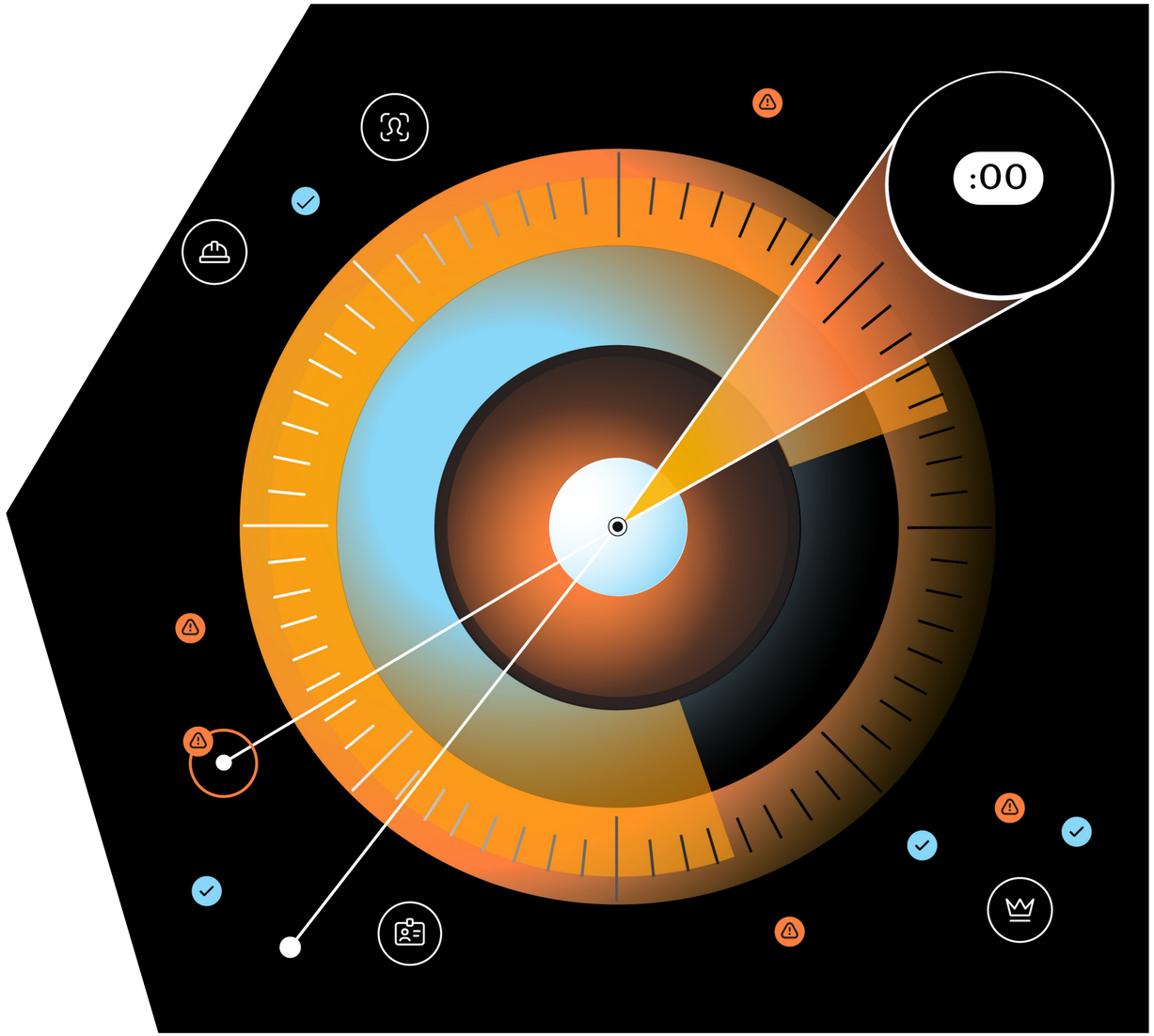
Warum die Identitätsebene der Dreh- und Angelpunkt ist

Jeder KI-gesteuerte Angriff hängt letztendlich von einer Sache ab: *dem Zugriff*.

Um Lateral Movement durchzuführen, Berechtigungen auszuweiten, auf sensible Systeme zuzugreifen oder KI-Agenten autonom zu betreiben, müssen sich Angreifer zunächst authentifizieren. Sie müssen identitätsbasiertes Vertrauen übernehmen, missbrauchen oder erlangen. Unabhängig davon, wie ausgereift ein Angriff ist: Letztendlich stützt er sich auf Berechtigungen, Authentifizierungsabläufe und Vertrauensbeziehungen, die bereits innerhalb der Umgebung bestehen.

Damit verlagert sich das Problem weg von reinen Schwachstellen und hin zum Thema Identität und Zugriff – dem eigentlichen Schauplatz KI-basierter Angriffe. Identitäten bieten diesen Modellen Wege zur Ausbreitung. Sobald ein Angreifer Zugriff auf eine legitime Identität erlangt, werden sämtliche Berechtigungen, Vertrauensbeziehungen, übertragenen Privilegien und Authentifizierungsmechanismen zu potenziellen Einfallstoren für eine weitere Kompromittierung.

Identitäten sind somit sowohl zum primären Schauplatz moderner Cyberangriffe als auch zum letzten verlässlichen Kontrollpunkt vor der Ausführung einer Aktion geworden. Ist der Zugriff erst gewährt, lassen sich böswillige Aktivitäten oft nur schwer von legitimem Verhalten unterscheiden, da sie unter Verwendung gültiger Zugangsdaten und genehmigter Kommunikationskanäle durchgeführt werden. Den Verantwortlichen für die Abwehr bleibt dann nur noch der Versuch, bereits laufende Aktionen zu erkennen und darauf zu reagieren.

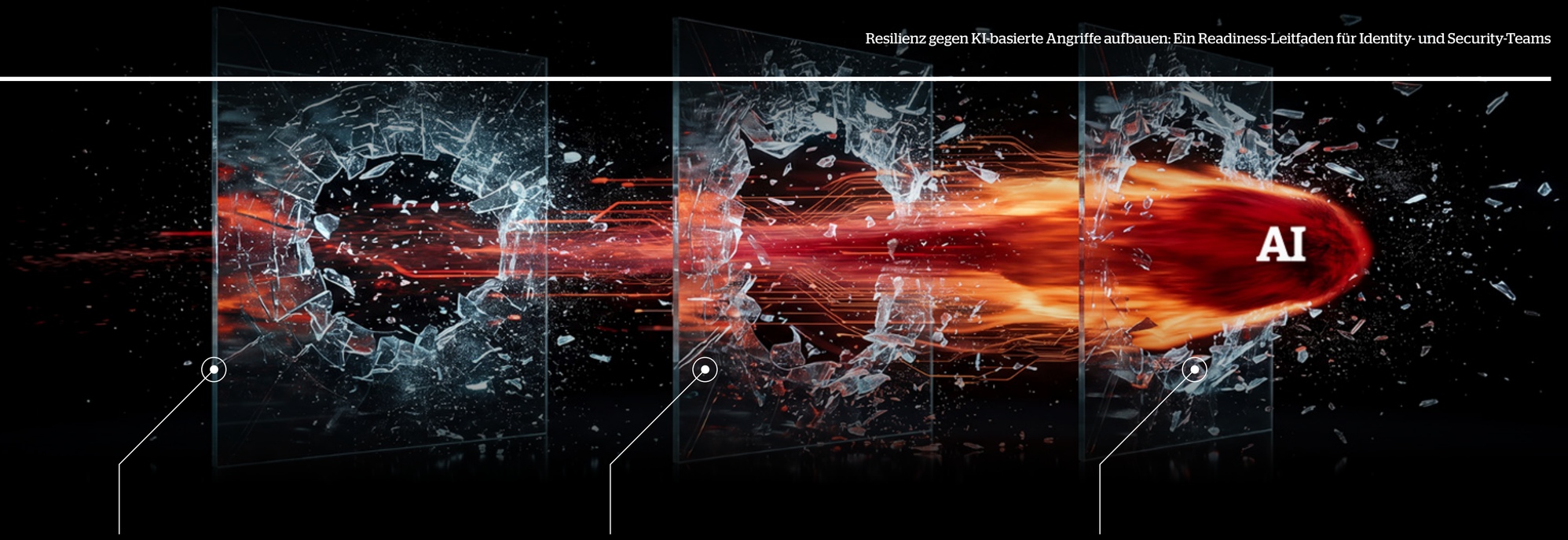


Die Regeln haben sich geändert, die meisten Tools jedoch nicht: Warum herkömmliche Identity-Security-Modelle versagen

Die meisten Bereiche der Identity Security wurden im Hinblick auf Angriffe mit menschlichem Tempo konzipiert, bei denen die Angriffskette unterbrochen werden kann, bevor größerer Schaden entsteht.

KI-basierte Angriffe machen diese Annahmen zunichte. Angriffsketten, die sich früher über Stunden oder Tage erstreckten, können nun innerhalb von Minuten ablaufen.

Dies untergräbt mehrere zentrale Ansätze, auf die sich Organisationen nach wie vor verlassen.



IGA ist zu statisch
Systeme für Identity-Governance und -Verwaltung wurden auf der Grundlage vordefinierter Richtlinien, regelmäßiger Bewertungen und administrativer Workflows entwickelt.

KI-basierte Angriffsketten sind jedoch dynamisch. Sie werden innerhalb von Sekunden entwickelt und ausgeführt.

Statische Richtlinien können nicht alle Lateral-Movement-Routen vorhersehen, die ein KI-Modell in einem komplexen Identitätsgraphen eines Unternehmens aufdecken könnte. Wenn Angreifer innerhalb von Sekunden handeln, verlieren regelmäßige Zugriffsüberprüfungen, die alle paar Monate stattfinden, ihre Relevanz.

Herkömmliches PAM ist zu eng gefasst
PAM schützt eine begrenzte Anzahl bekannter privilegierter Konten durch Vaulting und Sitzungsmanagement.

KI-basierte Angriffe denken jedoch nicht in Kategorien wie „privilegierte Konten“. Sie betrachten die gesamte Unternehmensumgebung als einen zusammenhängenden Vertrauensgraphen.

Service Accounts, delegierte Berechtigungen und implizite Vertrauensbeziehungen werden zu potenziellen Angriffspfaden – viele davon sind von herkömmlichen PAM-Bereitstellungen nicht abgedeckt.

Erkennung und Reaktion erfolgen zu spät
Tools zur Erkennung und Reaktion warnen zwar vor Bedrohungen, werden jedoch meist erst dann aktiv, wenn verdächtiges Verhalten bereits aufgetreten ist.

Die Erkennung ist natürlich nach wie vor wertvoll, löst jedoch nicht das zentrale Problem des Zeitfaktors, das sich bei KI-basierten Angriffen stellt. Bis ein Analyst die Warnmeldung sieht, entsprechende Protokolle auswertet und mit der Reaktion beginnt, ist der Angriff möglicherweise bereits abgeschlossen.

Wenn Angriffe kontinuierlich mit maschineller Geschwindigkeit ausgeführt werden und bösartige Aktivitäten erst nach der Zugriffsgewährung erkannt werden, kommt jede Reaktion zu spät.

Was tatsächlich Abhilfe schafft: Runtime Identity Security

Die Abwehr KI-basierter Angriffe erfordert Identity Security, die über Transparenz, Sicherheitsstatus-Management und Erkennung hinausgeht. Sie muss in der Lage sein, einen Zugriffsversuch zum Zeitpunkt der Ausführung zu bewerten und zu kontrollieren, noch bevor eine Aktion erfolgt.

Angriffe lassen sich nur in Echtzeit zuverlässig abwehren – genau in dem Moment, in dem eine Authentifizierungs- oder Zugriffsanfrage erfolgt, also noch bevor die angeforderte Aktion ausgeführt werden darf.

Runtime-Kontrollpunkt bei jeder Authentifizierung

Sicherheitskontrollen müssen direkt innerhalb des Authentifizierungsablaufs selbst erfolgen. Dabei wird jede Zugriffsanfrage anhand von Echtzeit-Risikoindikatoren und dem jeweiligen Verhaltenskontext unabhängig bewertet. Die Kontrollen müssen den Zugriff dynamisch zulassen, verweigern, abfragen, einschränken oder isolieren können, unabhängig von bestehenden statischen Berechtigungen oder statischen Richtlinien, die Monate zuvor definiert wurden.

Echtzeitanalyse und -kontext für Angriffe in maschineller Geschwindigkeit

KI-gesteuerte Angriffe entwickeln sich dynamisch weiter. Ihre Abwehr erfordert eine kontinuierliche Runtime-Bewertung, bei der Identitätskontext, Umgebungssignale, Verhaltensanalysen, Zugriffsmuster, Risikobewertungen und die Erkennung von Angriffspfaden einbezogen werden. Dabei sollen nicht nur verdächtige Aktivitäten identifiziert werden, sondern vor allem der nächste Schritt vor seiner Ausführung unterbunden werden – und zwar in der maschinellen Geschwindigkeit, mit der die Angreifer selbst vorgehen.

Durchsetzung vor der Ausführung

Die Erkennung bleibt wichtig, um eskalierende Situationen zu erkennen und entsprechend zu reagieren. Durch Erkennung allein lässt sich ein Angriff jedoch nicht verhindern. Kontrollmaßnahmen müssen frühzeitig und schnell genug greifen, um Lateral Movement, die Ausweitung von Berechtigungen oder andere böswillige Handlungen zu unterbinden – und zwar bevor diese stattfinden, nicht erst, nachdem sie beobachtet wurden.

Abdeckung der tatsächlichen Angriffswege

Angreifer, die KI einsetzen, unterscheiden nicht zwischen modernen und veralteten Systemen. Sie folgen den Pfaden, die ihnen zur Verfügung stehen – und in den meisten Unternehmen verlaufen diese Pfade durch die Identitätsinfrastruktur und etablierte Vertrauensbeziehungen, die außerhalb der Reichweite moderner Sicherheitskontrollen liegen:

- **Active Directory**, einschließlich veralteter und anfälliger Authentifizierungsprotokolle wie NTLM, RC4 und Kerberos
- **Service Accounts und andere nicht-menschliche Identitäten (NHIs)**, die häufig über dauerhaften, privilegierten Zugriff verfügen
- **Veraltete und selbst entwickelte Anwendungen** ohne moderne Identitäts- und Sicherheitskontrollen
- **Operational-Technology (OT)-Umgebungen**, die schwer zu überwachen und zu sichern sind
- **Segmentierte und Air-Gapped-Netzwerke**, die vermeintlich geschützt sind, sich jedoch auf vertrauenswürdige Identitätspfade stützen

Readiness Assessment: Sind Sie auf einen KI-basierten Angriff vorbereitet?

KI-basierte Angriffe sind schneller, anpassungsfähiger, schwerer zu erkennen und zunehmend in der Lage, gerade erst entdeckte Sicherheitslücken auszunutzen.

Beantworten Sie die folgenden fünf Fragen, um die Bereitschaft und Resilienz Ihres Unternehmens zu beurteilen. Wählen Sie jeweils die Antwort aus, die Ihre derzeitigen Möglichkeiten am besten widerspiegelt. Lautet die Antwort auf eine der Fragen „Nein“ oder „Teilweise“, könnte dies auf eine Schwachstelle hindeuten, die ein KI-basierter Angreifer ausnutzen könnte.

1. Können Sie Kontrollen in Echtzeit durchsetzen, um einen riskanten Zugriff zu unterbinden, bevor er stattfindet?

Können Ihre Sicherheitskontrollen bei einer riskanten Authentifizierungsanfrage Richtlinien auswerten und durchsetzen, bevor der Zugriff gewährt wird? Können Sie Zugriffskontrollen dynamisch anwenden, die mit der Komplexität und Geschwindigkeit KI-basierter Angriffe Schritt halten können?

Beispiele:

- Risikobasierte MFA
- Authentifizierungssperren
- Zugriffsbeschränkungen und Identitätsabgrenzung
- Richtlinien für die adaptive Authentifizierung

Der Geltungsbereich sollte menschliche Benutzer, Service Accounts und KI-Agenten in Cloud-, On-Premises- und Hybridumgebungen umfassen.

☐ Ja ☐ Teilweise ☐ Nein

2. Können Sie privilegierten Zugriff auch ohne Vault schützen?

Können Sie privilegierte Identitäten in großem Maßstab aufdecken, überwachen und steuern, einschließlich privilegierter Benutzerkonten, Service Accounts und sogar privilegierter KI-Agenten, die häufig außerhalb des traditionellen PAM-Anwendungsbereichs operieren?

Beispiele:

- Durchsetzung von MFA für administrative Zugriffspfade (RDP, SSH, PowerShell usw.)
- Just-in-Time (JIT)-Zugriffskontrollen zur Verschleierung dauerhafter Berechtigungen
- Beschränkung der Aktivitäten von Service Accounts auf genehmigte Quellen, Ziele und Protokolle
- Laufzeitschutz für privilegierte KI-Agenten

☐ Ja ☐ Teilweise ☐ Nein

3. Können Sie veraltete Authentifizierungsinfrastrukturen absichern?

Können Sie moderne Sicherheitsmaßnahmen für folgende Bereiche durchsetzen?

- Active Directory
- NTLM
- Kerberos
- Legacy-Anwendungen
- Selbst entwickelte Anwendungen
- Operational Technology (OT)
- Air-Gapped-Umgebungen

Können diese Umgebungen ohne Änderungen an der Infrastruktur oder den Anwendungen geschützt werden?

☐ Ja ☐ Teilweise ☐ Nein

Readiness Assessment (Fortsetzung)

4. Können Ihre Kontrollmechanismen mit maschineller Geschwindigkeit arbeiten?

Kann bösartiger Zugriff automatisch blockiert werden, ohne dass die nachfolgend aufgeführten Schritte abgewartet werden müssen?

- Überprüfung durch Analysten
- Ticket-Workflows
- Manuelle Genehmigungen
- Incident-Response-Prozesse

Könnte ein Angreifer aufgehalten werden, bevor es zu Lateral Movement oder einer Ausweitung von Berechtigungen kommt?

☐ Ja ☐ Teilweise ☐ Nein

5. Erfassen Sie identitätsbezogene Angriffspfade kontinuierlich?

Können Sie kontinuierlich Folgendes identifizieren?

- Privilegierte Identitäten
- Vertrauensbeziehungen
- Übermäßige Berechtigungen
- Delegationspfade
- Schwachstellen von Service Accounts

Zugriffsketten von KI-Agenten sowie die damit verbundenen Benutzer und nicht-menschlichen Identitäten (NHIs)

Können Sie nachvollziehen, wie sich ein Angreifer heute durch Ihre Umgebung bewegen könnte?

☐ Ja ☐ Teilweise ☐ Nein

Punkte	Readiness-Stufe	Bedeutung
9 – 10	Fortgeschritten	Umfangreiche Runtime-Kontrollen sind vorhanden. Der Schwerpunkt sollte auf einer Ausweitung der Abdeckung durch Step-up-Authentifizierung, risikobasierten Zugriff sowie dynamische Richtlinien zur Verweigerung, Einschränkung oder Überprüfung risikobehafteter Zugriffe liegen.
6 – 8	Im Aufbau	Zwar sind wesentliche Kontrollen vorhanden, doch bestehen weiterhin ausnutzbare Lücken. Frontier-KI kann diese mit hoher Wahrscheinlichkeit schnell identifizieren.
3 – 5	Gefährdet	Ansatz mit starkem Fokus auf Erkennung und eingeschränkter Prävention. Angreifer können schneller agieren, als Schutzmaßnahmen greifen können.
0 – 2	Ungeschützt	Erhebliche Schwachstellen in Bezug auf Transparenz, Durchsetzung und Abdeckung. KI-basierte Angriffe zielen bewusst auf die Ausnutzung einer solchen Umgebung ab.

PUNKTESYSTEM

Ja = 2 Punkte | Teilweise = 1 Punkt | Nein = 0 Punkte

Checkliste für die Vorbereitung auf KI-basierte Angriffe

Ihr Leitfaden für die Frage „Was soll ich am Montagmorgen als Erstes tun?“

Basierend auf unseren Tests der Fähigkeiten von Frontier-KI sowie den in Zusammenarbeit mit Glasswing-Mitgliedern gewonnenen Erkenntnissen zeigt sich, dass eine Reihe von Sicherheitskontrollen besonders effektiv dabei hilft, KI-gestützte Angriffspfade zu unterbinden.

Nutzen Sie diese Checkliste als praktischen Leitfaden zur Priorisierung. Arbeiten Sie sich von oben nach unten durch, da die Punkte am Anfang der Liste die größte Risikoreduzierung und den höchsten Effekt bei der Abwehr von Angriffen mit maschineller Geschwindigkeit bringen.

KRITISCH: Enforcement-Lücken schließen

- Wenden Sie Authentifizierungskontrollen in Echtzeit an, bevor Zugriff gewährt wird.
- Erweitern Sie die MFA auf On-Prem-Ressourcen, Legacy-Systeme, selbst entwickelte Anwendungen und OT-Umgebungen.
- Bewerten Sie jede Zugriffsanfrage bei der Ausführung und blockieren oder erhöhen Sie die Hürden für riskante Zugriffe.
- Wenden Sie Runtime-Kontrollen an, um die Aktivitäten von Service Accounts einzuschränken.
- Eliminieren Sie dauerhafte Berechtigungen durch Just-in-Time (JIT)-Zugriff für Vorgänge mit privilegierten Rechten.
- Wenden Sie Runtime-Kontrollen auf KI-Agenten an, bevor diese Aktionen ausführen.

KRITISCH: Lateral Movement und Schadensumfang reduzieren

- Segmentieren Sie den Zugriff auf kritische Systeme und Ressourcen.
- Beschränken Sie die Aktivitäten von Service Accounts auf genehmigte Quellen, Ziele und Protokolle.
- Entfernen Sie nicht benötigte Administratorrechte.
- Reduzieren Sie nach Möglichkeit die Abhängigkeit von Legacy-Authentifizierungsprotokollen.

KRITISCH: Privilegierten Zugriff schützen

- Erfassen und inventarisieren Sie alle privilegierten Identitäten (menschliche und nicht-menschliche) anhand tatsächlicher Aktivitäten, nicht nur anhand statischer Konfigurationen.
- Schützen Sie alle privilegierten Identitäten zur Laufzeit, nicht nur solche, die durch herkömmliche PAM-Lösungen verwaltet oder in einem Vault gespeichert werden.
- Implementieren Sie Just-in-Time (JIT)-Zugriff für privilegierte Benutzer.
- Weiten Sie MFA auf administrative Zugriffspfade aus, einschließlich RDP, SSH, PowerShell und CLI-Tools.
- Verfolgen Sie beim Zugriff auf kritische Systeme einen „Deny-by-Default“-Ansatz.

KRITISCH: Nicht-menschliche Identitäten sichern

- Erfassen Sie alle Service Accounts und sonstigen nicht-menschlichen Identitäten (NHIs).
- Weisen Sie alle NHIs einem menschlichen Verantwortlichen und einem Geschäftszweck zu.
- Identifizieren Sie übermäßige Berechtigungen und unnötigen dauerhaften Zugriff.
- Erstellen Sie eine Baseline für normale Aktivitäten und überwachen Sie diese kontinuierlich auf Abweichungen.
- Beschränken Sie die Aktivitäten von Service Accounts auf genehmigte Quellen, Ziele und Protokolle.
- Wenden Sie Runtime-Kontrollen an, um unbefugten Zugriff auf und Missbrauch von NHIs zu verhindern.

KRITISCH: KI-Agenten kontrollieren

- Erfassen Sie KI-Agenten und agentenbasierte Workflows.
- Ordnen Sie jedem KI-Agenten einen menschlichen Verantwortlichen und einen Geschäftszweck zu.
- Identifizieren Sie die nicht-menschlichen Identitäten (NHIs), Zugangsdaten und Berechtigungen, die von agentenbasierten Workflows genutzt werden.
- Überwachen Sie kontinuierlich die Aktivitäten und Zugriffsmuster von Agenten.
- Wenden Sie Identity-Security-Kontrollen zur Laufzeit auf KI-Agenten an.
- Richten Sie Kontrollen ein, die sich in agentenbasierte Plattformen und MCP-Gateways integrieren lassen.

WICHTIG: Vollständige Transparenz schaffen

- Erfassen Sie alle Identitäten: menschliche, nicht-menschliche und KI-Agenten.
- Bilden Sie privilegierte Konten, Vertrauensbeziehungen und Zugriffspfade basierend auf tatsächlichen Aktivitäten ab.
- Identifizieren Sie inaktive Konten, veraltete Zugangsdaten und verwaiste Identitäten.
- Ermitteln und überwachen Sie die verwendeten Authentifizierungsprotokolle (Kerberos, NTLM, LDAP usw.).

WICHTIG: Zeitgewinnende Täuschungsmaßnahmen definieren

- Implementieren Sie Honeytokens und Scheinzugangsdaten für Identitäten.
- Definieren Sie vorab genehmigte, automatisierte Eindämmungsmaßnahmen bei der Auslösung von Täuschungsmaßnahmen.

WICHTIG: Überprüfung vornehmen

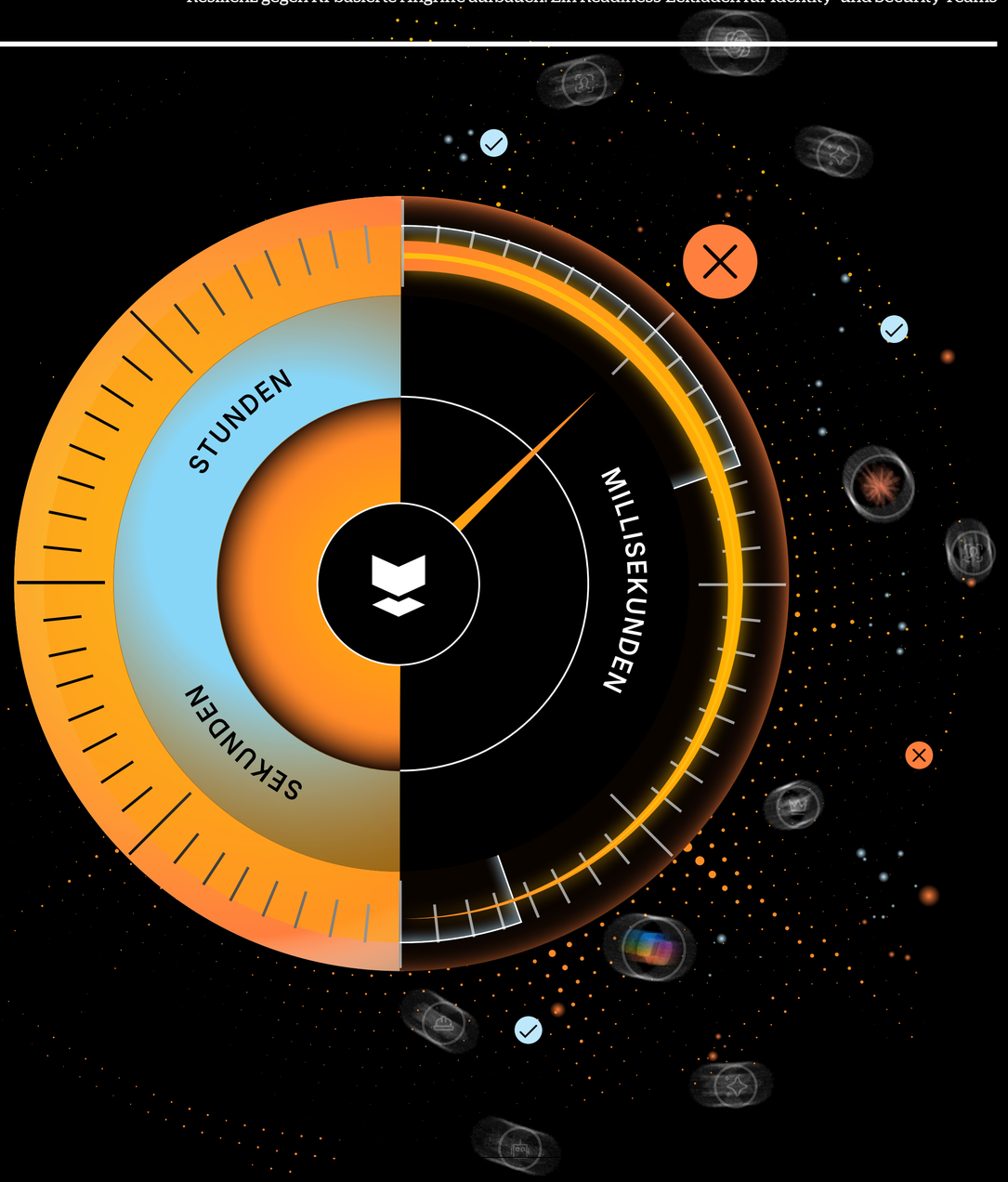
- Führen Sie eine KI-basierte Red-Team-Übung durch.
- Erfassen Sie die bei der Übung aufgedeckten Lateral-Movement-Pfade und führen Sie Abhilfemaßnahmen durch.
- Testen Sie, ob die Kontrollen Lateral Movement und die Ausweitung von Berechtigungen tatsächlich unterbinden, nicht nur erkennen.
- Messen Sie die Zeit bis zur Eindämmung und Prävention, nicht nur die Zeit bis zur Erkennung.

Runtime Identity Security im Zeitalter KI-basierter Angriffe

Die Erkenntnisse aus diesem Leitfaden führen ausnahmslos zu derselben Schlussfolgerung
KI-basierte Angriffe erreichen ihr Ziel, indem sie identitätsbasiertes Vertrauen in einer bislang unbekannten Geschwindigkeit und Größenordnung ausnutzen. Sie authentifizieren sich als rechtmäßige Benutzer, Service Accounts oder KI-Agenten, übernehmen bestehende Berechtigungen und bewegen sich mithilfe derselben Authentifizierungsinfrastruktur, auf die sich Ihr Unternehmen tagtäglich verlässt, durch Ihre Umgebung.

Dieser Umstand macht die Identität zur Kontrollinstanz moderner Angriffe.

Und genau deshalb erfordert die Abwehr KI-basierter Angriffe mehr als statische IGA-Regeln oder eine begrenzte PAM-Abdeckung – und mehr als passive Transparenz, reaktives Posture-Management oder eine zu späte Erkennung. Sie erfordert einen Kontrollpunkt, **der zur Laufzeit aktiv ist, also genau dann, wenn der Zugriff angefordert wird** – und somit bevor sich ein Angreifer lateral bewegen, Berechtigungen ausweiten oder den nächsten Angriffsschritt ausführen kann. Genau das ist die Aufgabe der Runtime Identity Security.



Warum Silverfort

Silverfort wurde nach einem einfachen Prinzip entwickelt: Wenn Angreifer über Identitäten agieren, muss die Identität selbst zur Schutzebene werden.

Im Gegensatz zu herkömmlichen Identity-Security-Lösungen schützt Silverfort alle Identitäten im großen Maßstab, zur Laufzeit und direkt während des eigentlichen Authentifizierungsablaufs. Die patentierte Runtime-Access-Protection (RAP)-Technologie von Silverfort bewertet jede Authentifizierungs- und Zugriffsanfrage in Echtzeit und entscheidet dynamisch darüber, ob der Zugriff gewährt, hinterfragt, eingeschränkt oder blockiert wird.

Dadurch können Unternehmen Sicherheitskontrollen genau dort durchsetzen, wo KI-basierte Angriffe stattfinden: innerhalb von Authentifizierungsabläufen, Vertrauensbeziehungen, Pfaden für privilegierten Zugriff, Aktivitäten von Service Accounts und KI-gesteuerten Aktionen.

Da Silverfort nicht in Anwendungen oder Endpunkte, sondern direkt in die Identitätsinfrastruktur und agentenbasierte Plattformen integriert wird, kann es den Schutz auf jene Umgebungen und Ressourcen ausweiten, die von Angreifern nach wie vor am häufigsten ausgenutzt werden. Dazu gehören Active Directory, NTLM, Kerberos, Service Accounts, Legacy-Anwendungen, Admin-Tools und OT-Umgebungen.

Das Ergebnis ist eine Runtime Identity Security, die speziell für Angriffe mit maschineller Geschwindigkeit entwickelt wurde. Sie bietet kontinuierliche Transparenz über alle Identitäten und deren Risiken, Schutz für menschliche und nicht-menschliche Identitäten sowie KI-Agenten und eine Durchsetzung zur Laufzeit. Letztere kann Lateral Movement, Ausweitung von Berechtigungen und unbefugten Zugriff bereits im Vorfeld verhindern.

Bewährt gegen KI-basierte Angriffe

Gemeinsam mit Mitgliedern von Glasswing testete Silverfort sein Abwehrsystem gegen KI-basierte Angriffstechniken und Angriffspfade in echten Unternehmensumgebungen.

Das Ergebnis war eindeutig: Selbst wenn Angreifer legitimierte Zugangsdaten erlangten, konnte Silverfort durch eine Risikobewertung und die Durchsetzung von Kontrollmaßnahmen vor der Zugriffsgewährung Lateral Movement verhindern.

Bei mehreren Übungen erwiesen sich die Kontrollen von Silverfort als so wirksam bei der Unterbindung des Angriffsfortschritts, dass der Schutz teilweise vorübergehend deaktiviert werden musste, damit das Red Team weitere Angriffspfade und -ziele testen konnte.

Auch wenn keine einzelne Kontrollmaßnahme alle Risiken vollständig beseitigen kann, haben diese Übungen eine wichtige Erkenntnis untermauert:

KI-basierte Angriffe lassen sich durch die Durchsetzung von Runtime Identity am Zugangspunkt stoppen.

Legen Sie los

Die gute Nachricht ist: Für eine bessere Vorbereitung auf KI-gestützte Angriffe müssen Sie weder Ihre Identitätsarchitektur neu aufbauen noch Ihre Anwendungen anpassen.

Die Lösung lässt sich schnell bereitstellen und ist sofort einsatzbereit.

Je früher Sie Identitäten zur aktiven Sicherheitskontrolle verwenden, desto schwieriger wird es für KI-basierte Angriffe, einen Weg ins System zu finden.

Sind Sie bereit für den nächsten Schritt?
Erleben Sie Runtime Identity Security in Aktion.

Über Silverfort

Silverfort schützt jede Art von Identität, ob menschlich, maschinell oder KI-basiert, sowohl in Cloud- als auch in On-Premises-Umgebungen. Als erstes Unternehmen bieten wir eine End-to-End-Plattform für Identity Security, die sich einfach bereitstellen lässt und den Geschäftsbetrieb nicht beeinträchtigt. So erzielen Sie bessere Sicherheitsergebnisse bei geringerem Aufwand. Sie können jede Identität in jeder Umgebung erfassen, Schwachstellen analysieren, um Ihre Angriffsfläche zu verringern, und Sicherheitskontrollen zur Laufzeit durchsetzen, um Lateral Movement, Ransomware und anderen Identitätsbedrohungen effektiv entgegenzuwirken.

Die Identity-Security-Plattform von Silverfort