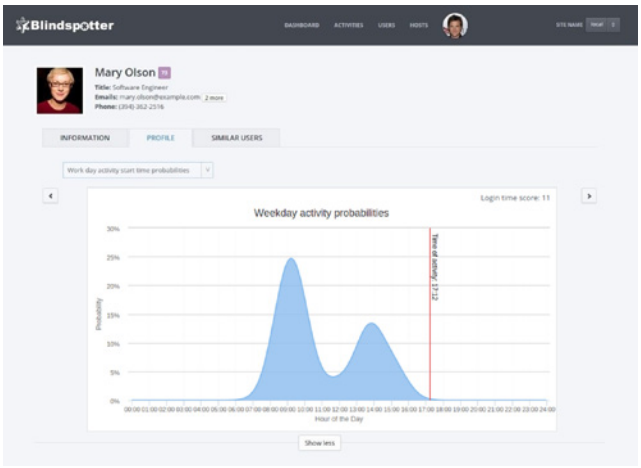
# BLINDSPOTTER

DIE LÖSUNG ZUR ANALYSE DES BENUTZERVERHALTENS IN ECHTZEIT

Blindspotter ist ein Tool zur Analyse des Benutzerverhaltens (User Behavior Analytics, kurz UBA), das Informationen aus unterschiedlichen IT-Systemen erfasst. Ungewöhnliches Verhalten privilegierter Nutzer wird identifiziert und Sicherheitsprobleme werden so erkannt.

Traditionelle IT-Sicherheitsprodukte und -techniken setzen auf eine Art von musterbasierter Technologie für das Verhindern, Erkennen und Stoppen von Angriffen. Diese Tools – ob es sich um präventive Sicherheitsprodukte wie Anti-Virus-Software oder Überwachungslösungen wie IDS oder SIEM handelt – liefern ein integriertes Wissen über Angriffsvektoren, das teilweise mit einfacher Heuristik erweitert wird. Die Erkennungsmuster werden entweder vom Anbieter bereitgestellt oder vom IT-Sicherheitsteam selbst erarbeitet. In beiden Fällen können die Produkte aber nur solche Ereignisse oder Angriffe aufspüren, deren Muster ihnen bekannt sind. Zwar kann Heuristik die Möglichkeiten dieser Sicherheitstools so erweitern, dass polymorphe Viren und bis dahin unbekannte Angriffe mit ähnlichen Mustern aufgespürt werden. Sie kann aber nicht auf bisher unbekannte Angriffstechniken eingehen, denn es ist nicht möglich, heuristische oder „universelle“ Muster für solche Fälle zu erstellen.

Da Blindspotter verschiedene Algorithmen für maschinelles Lernen nutzt, kann er ungewöhnliches Verhalten in Echtzeit erkennen – Anomalien, die bisher unbekannt waren. Algorithmen für maschinelles Lernen arbeiten autonom und erlernen das Benutzerverhalten. Auf diese Weise können sie die blinden Flecken bisheriger Technologien abdecken und nicht nur Anomalien identifizieren, sondern vielmehr auch Informationen darüber liefern, weshalb eine Aktivität als ungewöhnlich betrachtet wird.




Blindspotter erfasst benutzerspezifische Ereignisse und Sitzungsaktivitäten in Echtzeit oder annähernd in Echtzeit. Anschließend vergleicht er jeden Vorgang mit der entsprechenden Baseline der Benutzer und deren Peers, um Anomalien im Verhalten erkennen zu können. Eine schadhafte Benutzeraktivität kann völlig normal erscheinen, wenn sie nur unter einem bestimmten Gesichtspunkt untersucht wird. Da Blindspotter eine Reihe von Algorithmen einsetzt, werden Aktivitäten aus vielen verschiedenen Perspektiven betrachtet. Dadurch werden Anomalien erkannt, die sonst unentdeckt bleiben würden.

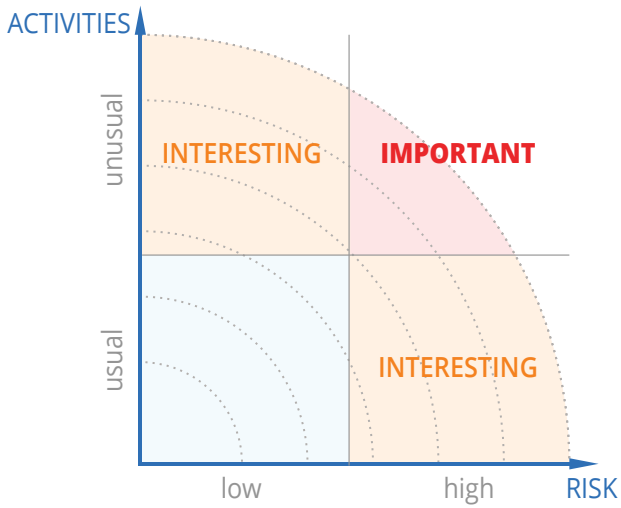
## BIOMETRISCHE ANALYSE

Von diesen verschiedenen Perspektiven ist die Biometrie vermutlich die bemerkenswerteste. Blindspotter ist die einzige Lösung zur Analyse des Benutzerverhaltens, die nicht nur Logdaten analysiert, sondern auch biometrische Informationen über jeden einzelnen Benutzer berücksichtigt, etwa das Tippverhalten oder typische Mausbewegungen. Zu den Aspekten der Tastaturanalyse zählen Tippgeschwindigkeit, zeitlicher Abstand zwischen einzelnen Tastenanschlägen und häufige Tippfehler. Auch wenn mehrere Benutzer für die gleiche Aufgabe zuständig sind, zeigt doch jeder sein ganz eigenes Verhaltensmuster – beispielsweise die Geschwindigkeit, mit der der Mauszeiger bewegt wird, oder einfach die Anzahl einzelner Bewegungen.

Dank der außerordentlich präzisen und mit Zeitstempel versehenen Audit Trails, die von Balabits Privileged-User-Monitoring-Lösung „Shell Control Box" bereitgestellt werden, können die in Blindspotter integrierten Algorithmen diese Merkmale untersuchen. Die Shell Control Box eröffnet Unternehmen eine Möglichkeit, Benutzer biometrisch zu analysieren, ohne dass hierfür zusätzliche Systeme, Tools oder Agenten erforderlich wären. Die Untersuchung basiert auf den normalen Aktivitäten der Mitarbeiter – diese müssen nichts Besonderes tun, sondern einfach nur wie gewohnt arbeiten. Die biometrischen Analysefunktionen von Blindspotter erkennen nicht nur Identitätsdiebstähle, sondern fungieren zudem als zusätzliche biometrische Authentifizierung. So können Sicherheitsanalysten jederzeit feststellen, ob der Benutzer auch tatsächlich derjenige ist, der er zu sein vorgibt.

Sobald eine ungewöhnliche Aktivität oder Anomalie erkannt wird, greift Blindspotter automatisch ein, um sowohl eine Reaktion in Echtzeit durchzuführen als auch den Untersuchungsprozess zu automatisieren und zu unterstützen. Automatisierte Reaktionen können erheblich die Zeit reduzieren, die einem böswilligen Angreifer bleibt, bis Gegenmaßnahmen ergriffen werden. In den meisten Angriffsszenarien geht einem schadhaften Ereignis eine Phase des Ausspähens voraus. Erkennen und Reagieren in dieser Phase sind entscheidend für das Verhindern künftiger Aktivität mit großem Schaden. Bei ungewöhnlicher Aktivität kann vom Benutzer eine Bestätigung angefordert werden: Der Kontoinhaber wird über die verdächtige Aktivität benachrichtigt und aufgefordert, diese zu bestätigen. Mit dieser Methode kann ein Identitätsdiebstahl schneller und genauer erkannt werden.

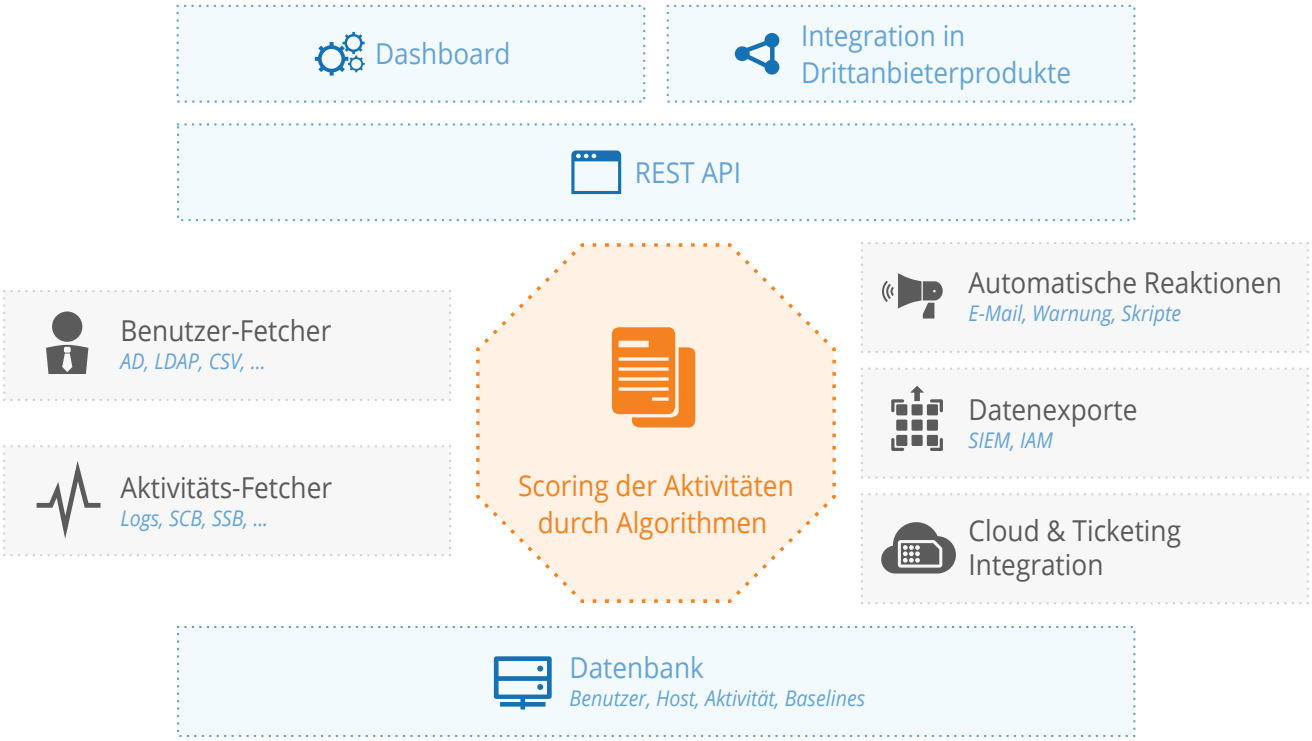
Um ein besseres Verständnis darüber zu erlangen, was im IT-System vor sich geht, und um die Aufmerksamkeit des Sicherheitsteams auf die wichtigsten Informationen zu lenken, stellt Blindspotter eine priorisierten Liste von Aktivitäten bereit. Dabei werden die potenziell risikoreichsten Aktivitäten ganz oben aufgeführt. Auf diese Weise kann das Sicherheitspersonal seine Zeit auf die wirklich wichtigen Ereignisse konzentrieren und wird nicht durch Benachrichtigungen und Alarme überlastet.




Ungewöhnliche Aktivitäten von Benutzern mit hohem Risiko haben für die Untersuchung höchste Priorität. Natürlich kann es sich auch lohnen, ungewöhnliche Aktivitäten von risikoärmeren Benutzern zu untersuchen; Vorrang haben aber solche mit höherem Risiko. In gleicher Weise ist es auch hilfreich, über weniger ungewöhnliche Aktivitäten von Benutzern mit hohem Risiko informiert zu sein. Diese „risikoorientierte" Skala versieht jede Aktivität mit einemScorewert, wodurch alle Aktivitäten global vergleichbar gemacht werden.

## WAS MUSS ICH WISSEN?

Wenn Sie eine erfolgreiche Sicherheitsarchitektur erstellen möchten, müssen sowohl bekannte Angriffe als auch unbekannte Angriffsvektoren berücksichtigt werden. In vielen Fällen besteht die echte Herausforderung darin, festzustellen, was wir überwachen möchten, welche Warnungen einzurichten sind und wie wir das System die Angriffe „lehren" können, die wir erkennen möchten. Das Problem besteht nun darin, „die richtigen Fragen" zu stellen und „Antworten zu geben", ohne dabei das Sicherheitsteam mit irrelevanten Antworten oder Alarmen zu überfluten. Blindspotter hilft und „beantwortet" Fragen auf einer höheren Ebene: „Zeige mir, was ich über die Benutzer meines IT-Systems wissen sollte." Das versetzt das IT-Sicherheitsteam in die Lage, sich auf bisher übersehene Ereignisse zu konzentrieren. Die Informationen, die aus der Untersuchung dieser Ereignisse gewonnen wurden, lassen sich auch in die bestehende Sicherheitsarchitektur integrieren und so dafür nutzen, „bessere Fragen" zu stellen.



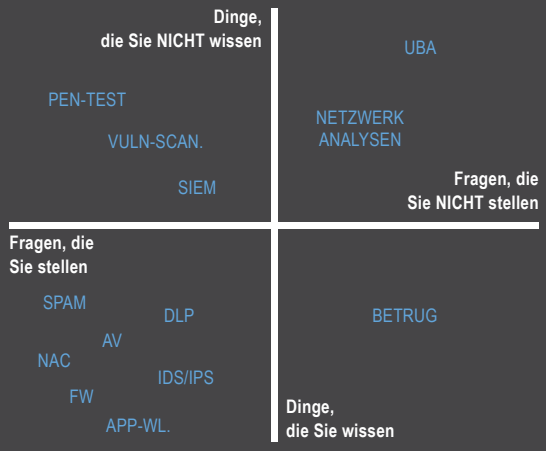

*Blindspotter-Architektur*

Blindspotter besteht aus verschiedenen, lose miteinander verbundenen Komponenten, die bei der Implementierung für hohe Flexibilität sorgen. Datenkonnektoren, Algorithmen, Datenbanken und das Frontend lassen sich trennen und so in großen Umgebungen, bei denen es um hohe Datenvolumina und viele Benutzer geht, optimal skalieren. Das System kann auf einem einzigen Server installiert oder bei zunehmender Last horizontal skaliert werden.

Zur Integration benutzerdefinierter Anwendungen werden modifizierte oder neue Add-Ons einfach in Blindspotter geladen, mittels derer die Daten der Anwendung gesammelt und integriert werden. Blindspotter bietet ein umfassendes API, um die Entwicklung neuer Add-Ons zu erleichtern.

Menschen haben aufgrund ihrer Natur eindeutige Verhaltenseigenschaften, die durch Algorithmen und Analysen identifiziert werden können. Benutzerprofile oder Baselines werden allesamt mithilfe von historischen Daten erstellt. Blindspotter lernt das Benutzerverhalten durch die Analyse von Verhalten in der Vergangenheit.

## Zero-Knowledge-Bedrohungen




In den Datenwissenschaften gibt es eine sehr wichtige Unterscheidung zwischen den Dingen, die wir nicht wissen („Unknowns“) und denjenigen, über die wir noch nicht einmal Fragen stellen können („Unknown Unknowns“), denn wir wissen gar nicht, wonach wir suchen sollen. In der IT-Sicherheit gibt es immer Bedrohungen aus beiden Kategorien. Die meisten Produkte befassen sich mit der ersten Gruppe und suchen nach bekannten Angriffen im System. Das wirkliche Problem sind aber Angriffe, die bisher unbekannt waren.

Sie werden allgemein als Zero-Day- oder Zero-Hour-Angriffe bezeichnet. Wir müssen mit den „Unknown Unknowns“ der IT-Sicherheit umgehen, die die hauptsächlichen Herausforderungen heute und morgen darstellen.

*Anatomy of an APT attack*

**1**

## Anmeldeinformationen des DB-Operators werden gestohlen

Die meisten APT-Angriffe beginnen damit, den Computer einer Person im Unternehmen durch Phishing, „Watering-Hole-Angriffe“ oder andere Mittel zu kompromittieren. Die Kontrolle über ein Endgerät zu erlangen, heißt auch den Zugriff auf die meisten Anmeldeinformationen seiner Benutzer zu erlangen: Gespeicherte Kennwörter oder Tastatureingaben abrufen sind lediglich zwei von endlosen Möglichkeiten. Von diesem Punkt an kann der Angreifer im Namen des Insiders agieren und das System erkunden, um die Daten zu finden, nach denen er sucht.

**2**

## Mehrfacher Zugriff auf Datenbankserver

Der Angreifer verschafft sich mit den gestohlenen Anmeldeinformationen Zugang zu verschiedenen Datenbankservern, um das IT-System und dessen Komponenten zu analysieren. Die erfolgreichen Anmeldungen werden aufgezeichnet und die Logdaten werden von der syslog-ng Store Box eingesammelt und zudem zum SIEM-System weitergeleitet. Da die Anmeldungen jedoch erfolgreich sind, werden vom SIEM-System keine Alarme ausgelöst.

Algorithmus *Anmeldezeit* → Zu viele Verbindungen

Algorithmus *Host-Anmeldung* → Usual servers

Algorithmus *Aktivitätszähler*

Algorithmus *Auswahl stochastische Ausreißer*

Algorithmus *Frequent Itemset*

Algorithmus *biometric identifier*

**3**

### Zu viele Verbindungen

Blindspotter holt sich die Logdaten in Echtzeit von der syslog-ng Store Box und analysiert die Verbindungen. Es werden mehrere Algorithmen verwendet. Jedoch erkennen weder der „logintime“- noch der „hostlogin“-Algorithmus irgendeine ungewöhnliche Aktivität, da sowohl die Zeit der Anmeldung als auch die Datenbankserver, auf die zugegriffen wurde, im Rahmen des Profils des Opfers als normal gelten. Die Analyse von Häufigkeit und Anzahl paralleler Verbindungen löst jedoch nichtsdestotrotz einen Hinweis auf eine verdächtige Aktivität aus.

**4**

### Ungewöhnliche biometrische Muster

Auch wenn sich der Angreifer erfolgreich anmelden kann, erkennt Blindspotter Mausbewegungen und Tastatureingaben, die für den Benutzer ungewöhnlich sind. Dies bedeutet, dass die Geschwindigkeit der Mausbewegungen wie auch der zeitliche Abstand zwischen den Tastenkombinationen vom üblichen Muster abweichen. Diese Aktivität erhöht die Risikobewertung des Benutzers erheblich.

**5**

### Benutzerrisiko dynamisch erhöhen

Blindspotter erhöht das mit diesem Benutzer verknüpfte Risiko dynamisch.

**6**

## Zugriff auf Datenbank, Datendiebstahl wird versucht

Jetzt taucht der Angreifer tiefer in die Datenbankserver ein und beginnt, Daten zu stehlen. Zu diesem Zeitpunkt werden jedoch alle ausgeführten Befehle aufgezeichnet und in der Shell Control Box protokolliert. Blindspotter ruft die Ereignisse über ausgeführte Befehle ab und analysiert diese in Echtzeit.

Algorithmus *Analyse des Bildschirminhalts* → >_

**7**

### Ungewöhnlicher Befehl für die Datenbank-Administration

Die Analyse zeigt, dass die ausgeführten Befehle für Datenbankoperatoren und -administratoren ungewöhnlich sind. Dadurch wird automatisch eine weitere Erhöhung des dynamischen Risikos ausgelöst.

**8**

### Benachrichtigung des Benutzers und/oder des Sicherheitsteams über die verdächtigen

Das Opfer bestätigt nicht, dass die verdächtigen Aktivitäten von ihm durchgeführt wurden, was darauf hindeutet, dass ein Identitätsdiebstahl aufgetreten ist.

Konto deaktivieren

Weitere Untersuchung durchführen

**9**

Das Sicherheitsteam hat alle relevanten Informationen (Logdaten der syslog-ng Store Box und Audit Trails der Shell Control Box) in Blindspotter parat und kann schnell den Angriff untersuchen und weitere Gegenmaßnahmen ergreifen. Die frühzeitige Erkennung von Blindspotter konnte verhindern, dass der Angreifer die Daten des Unternehmens stiehlt.

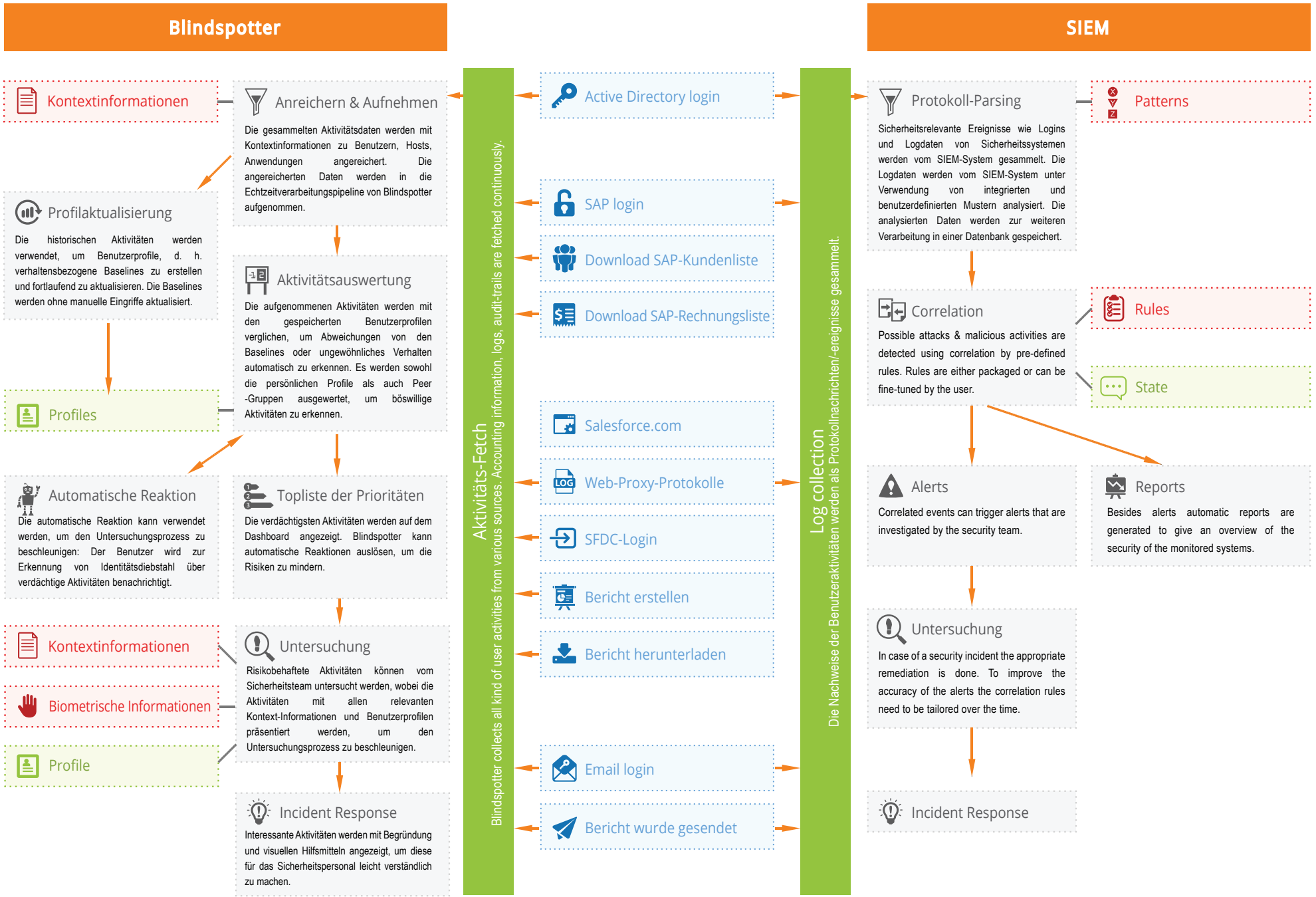
Blindspotter erleichtert den Untersuchungsprozess durch Zeigen des Kontexts: Anhand des üblichen Verhaltensprofils des Benutzers wird herausgestellt, weshalb und wie sich die aktuelle Situation von dem unterscheidet, was normal ist. Die Ermittlern können sich schnell einen Überblick über die Aktivitäten des Benutzers verschaffen und diese mit den Aktivitäten von Peers vergleichen.

**10**

## Der Angreifer wurde neutralisiert

Da das Opfer die Aktivitäten des Angreifers nicht bestätigt hat, hat das Sicherheitsteam das Konto mit den gestohlenen Anmeldeinformationen deaktiviert, sodass der Angreifer gestoppt wurde, bevor er auf Daten zugreifen oder Daten ausgeschleusen konnte.

*Comparison of Blindspotter and SIEM solutions*



BALABIT

CONTEXTUAL SECURITY INTELLIGENCE

# ÜBER BALABIT

Das Unternehmen Balabit wurde in Budapest (Ungarn) gegründet und ist ein führender Anbieter von Contextual-Security-Technologien. Damit verfolgt das Unternehmen das Ziel, den Verlust von Unternehmensdaten zu unterbinden, ohne die Geschäftstätigkeit zu beeinträchtigen. Balabit ist weltweit über ein Netz von Niederlassungen in den USA und Europa tätig und arbeitet mit einem Netzwerk von Fachhandekspartnern zusammen. Balabits Plattform für Contextual Security IntelligenceTM schützt Unternehmen in Echtzeit vor Gefahren, die durch den Missbrauch von IT-User-Accounts mit hohem Risikopotenzial und privilegierten Zugriffsrechten entstehen können. Das Portfolio von Balabit umfasst ein System- und Applikations-Log-Management, das kontextbezogene Daten liefert, sowie Lösungen in den Bereichen Privileged User Monitoring und User Behavior Analytics. In Kombination identifizieren diese Technologien ungewöhnliche Aktivitäten von Nutzern und stellen detaillierte Informationen über potenzielle Bedrohungen zur Verfügung. Zusammen mit herkömmlichen kontrollorientierten Strategien stellt Balabit einen flexiblen, auf den Nutzer zugeschnittenen Ansatz bereit, der ein höheres Maß an Sicherheit bietet, ohne dadurch Geschäftsabläufe zu beeinträchtigen.

Balabit wurde im Jahr 2000 gegründet. Zu den Kunden zählen 23 Prozent der Fortune-100-Unternehmen. Zudem setzen mehr als eine Million Nutzer in Unternehmen die Lösungen von Balabit ein.

Weitere Informationen erhalten Sie unter www.balabit.com.