#WeAreExclusive

Exclusive Networks

27.02.2023 | 16:00 Uhr

Philipp Wäspy

#WeAreExclusive

Wer ist
Exclusive Networks?

#WeAreExclusive

Einer der weltweit führenden

Value Added Distributoren für Cybersecurity

Our Vision

Eine ‘vollständig vertrauenswürdige’ digitale Welt für alle Menschen und Organisationen.

Our Mission

Der weltweit führende ‘Spezialist für Cybersicherheit’.

#WeAreExclusive

Der Weg zu einer vertrauenswürdigen digitalen Welt

Ihre Vorteile mit

Exclusive Networks

Vertrieb

Erfahrene Mitarbeiter, partnerschaftliche Zusamenarbeit

Marketing

360⁰ Marketing Ansatz Basierend auf Business Strategien

Technical Customer Success

Pre-Sales, Consulting, Training, Support

Managed Service Provider

Unterstützung, Erfahrung, Technologien, Abrechnungsmodelle

Das Exclusive Networks Exabeam-Team

PHILIPP WÄSPY

Business Development Manager
philipp.waespy@exclusive-networks.de
+49 151 62782114

MARKETING

DACHMarketing@exclusive-networks.de

BENNO SITZMANN

Business Development Manager
benno.sitzmann@exclusive-networks.de
+49 170 2266131

TECHNICAL CUSTOMER SUCCESS

Presales_DACH@exclusive-networks.com


Vielen Dank
Stellen Sie sich eine „vollständig vertrauenswürdige“ digitale Welt vor.
Sicherheit schafft Vertrauen.

exabeam

Diagnose: Alert Fatigue

Peter Häufel | Channel Account Director

Modern Security Operations at Scale

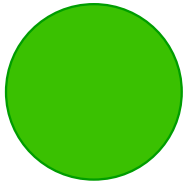
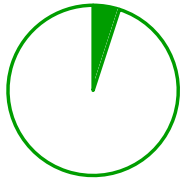
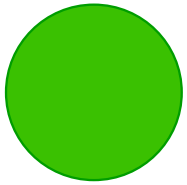
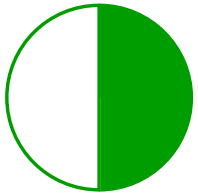
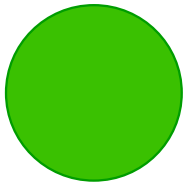
Die Herausforderung traditioneller SIEM Lösungen

- 500 – 1.000.000 Events pro Sekunde!
- Das Regelwerk ist nie aktuell und nicht vollumfänglich
- *Insider Threat* Erkennung ist „wirtschaftlich sinnvoll nicht umsetzbar“
- Managed Service Provider generalisieren das Regelwerk zu großen Teilen
- 80%+ Fehlalarme
- Vollständige Analyse aus Zeitmangel nicht möglich

SIEM Effectiveness Gap

exabeam

Automation des SOC Prozesses

	Ihr SOC		Exabeam
Angriffs-erkennung		12%	
Triage und Untersuchung		62%	
Gegen-maßnahme		26%	

Compromised Insider:
Wie würden Sie die Fragen beantworten?

EDR Alarm: Powershell
und Mimikatz auf server

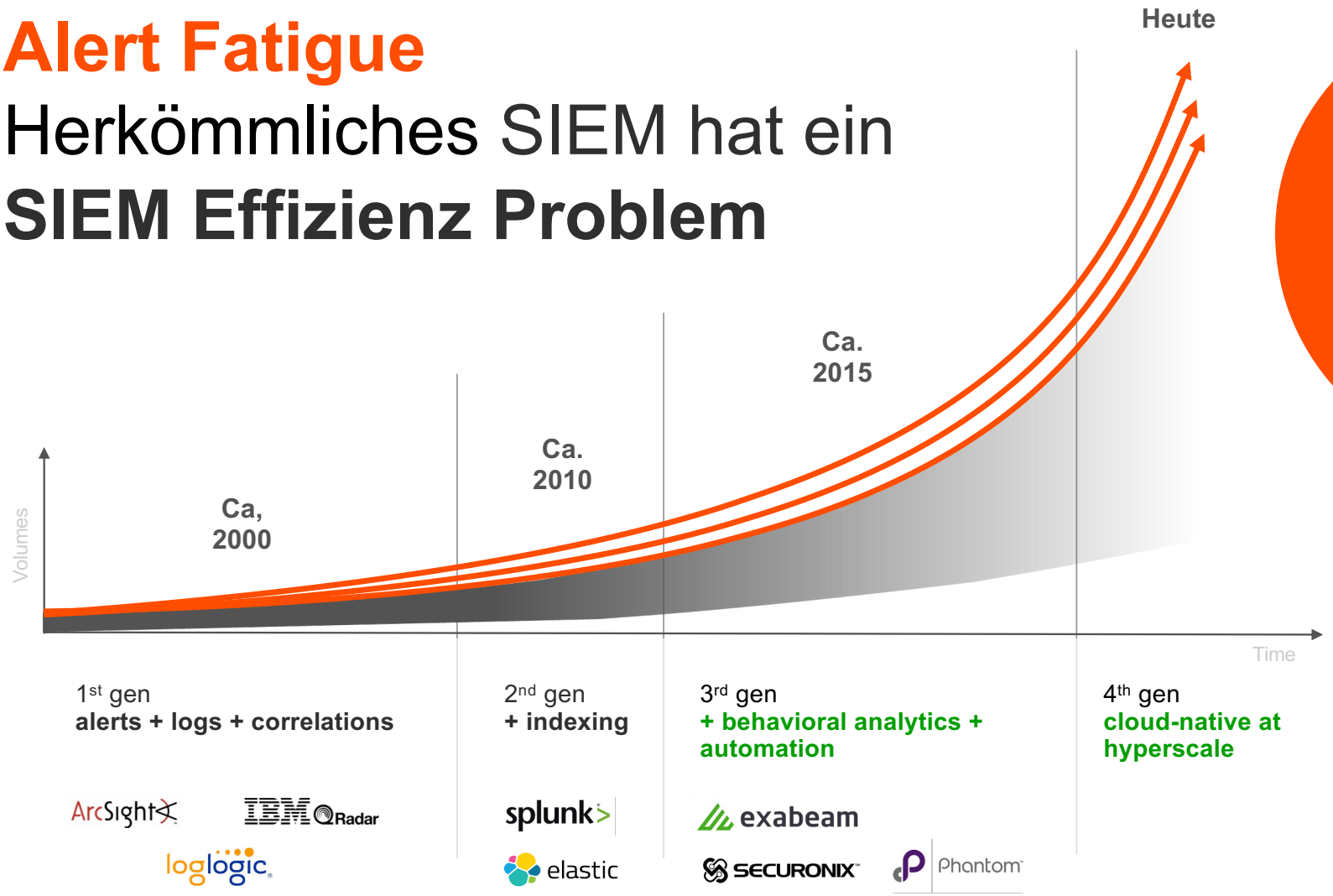
8. Mai, 2:27

- Wie erfolgte der initiale Zugang – Lokation, OS, Browser?
- Wie hat sich der Hacker ausgebreitet?
- Auf welche Geräte hat der Account zugegriffen?
- Hat der Hacker erweiterte Privilegien erlangt oder den Account gewechselt?
- Liefen Prozesse in ungewöhnlichen Verzeichnissen?

exabeam

Alert Fatigue

Herkömmliches SIEM hat ein **SIEM Effizienz Problem**

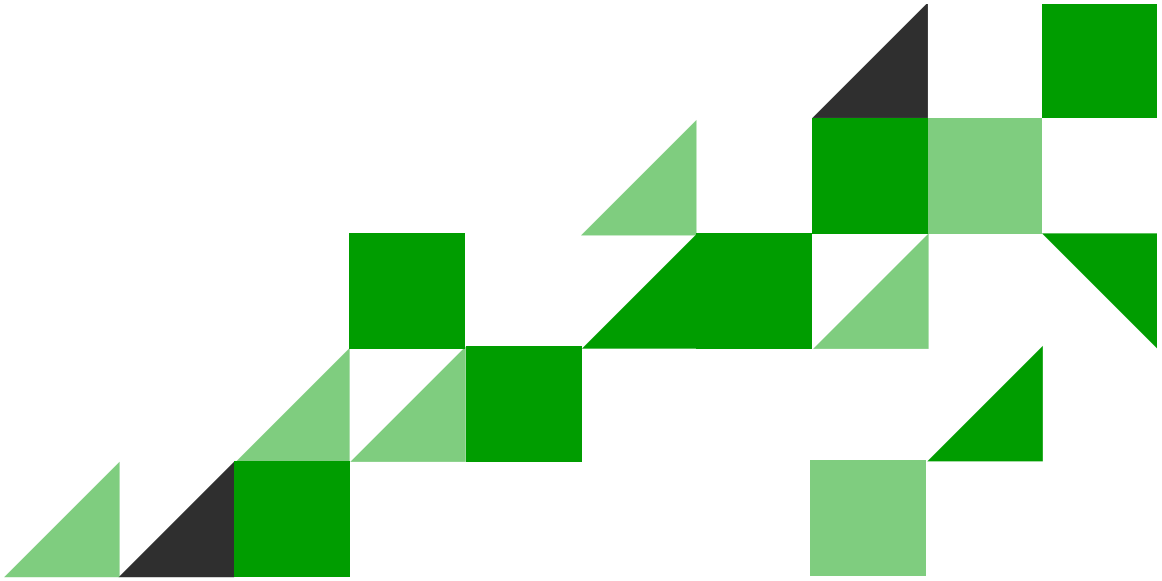


- Datenvolumen und Quellen
- Angriffsvektoren
- Credential basierte Angriffe
- Fehlalarme
- Personalkosten
- Speicherkosten

exabeam

exabeam

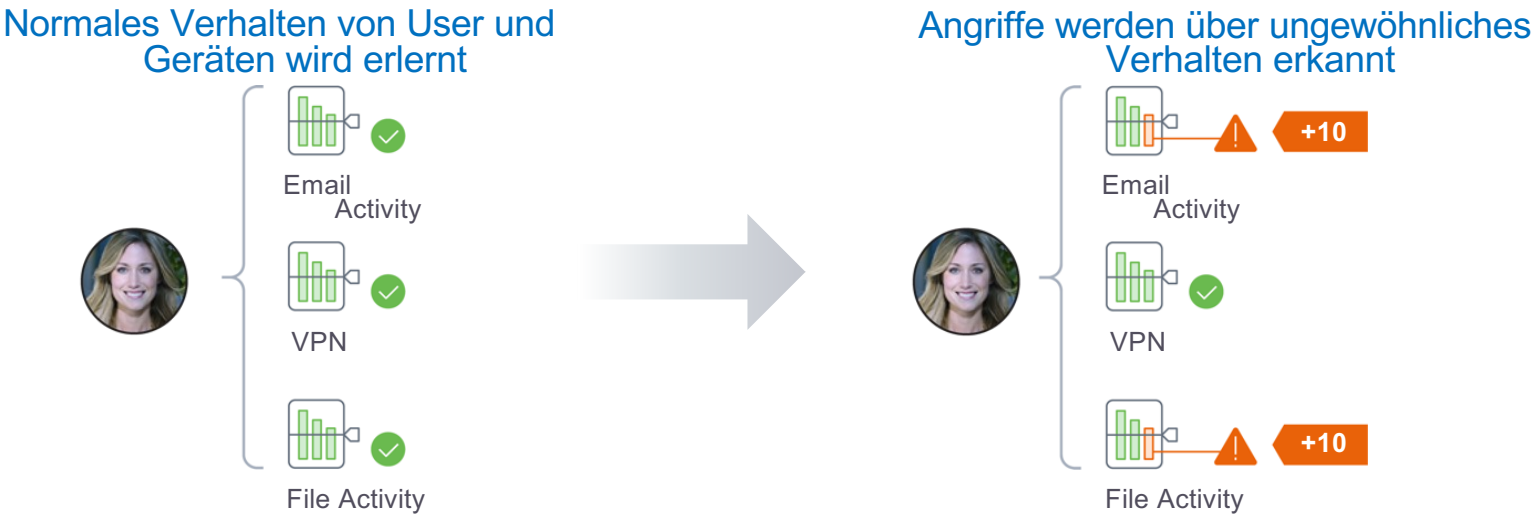
New-Scale SIEM™



Cloud-scale Security Log Management + **Powerful Behavioral Analytics** + **Automated Investigation Experience**

exabeam

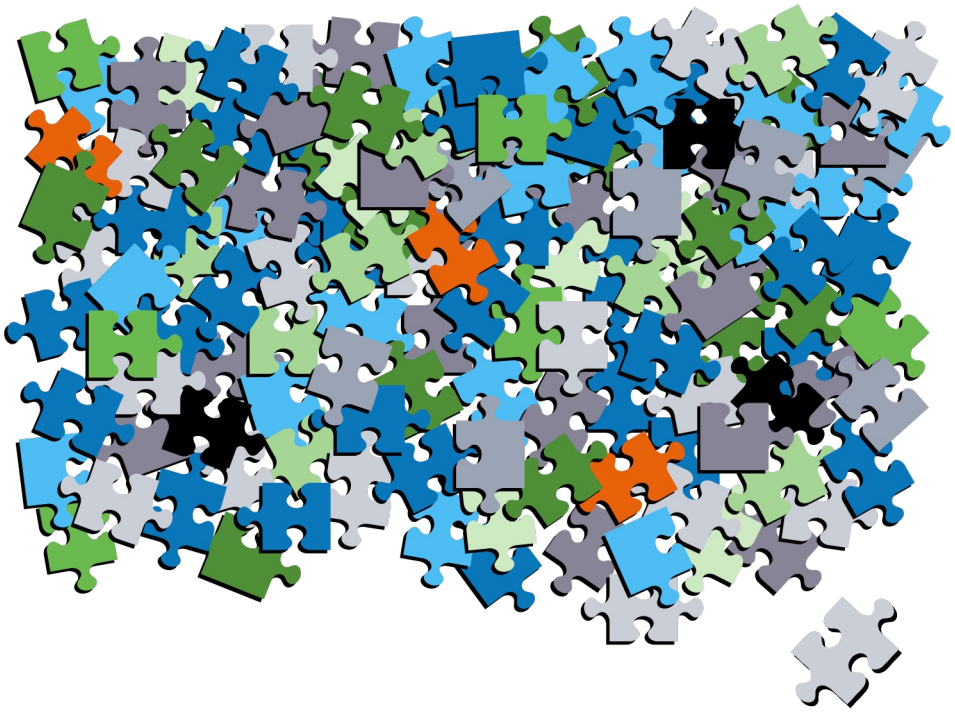
Exabeam erkennt unbekannte Angriffe mittels User und Device Verhaltensanalyse



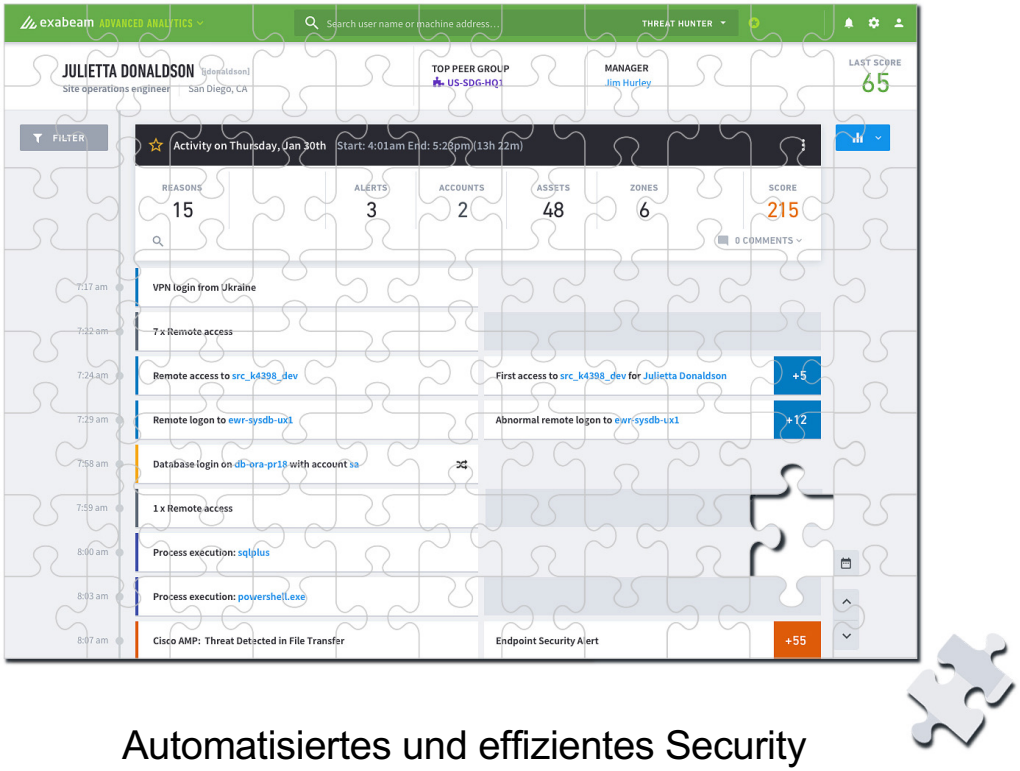
Advanced Analytics

- Einfache Erkennung von bekannten und unbekannten Angriffen
- Korrelationsregeln müssen weder erstellt noch gewartet werden
- Reduzierung der Fehlalarme durch Verständnis der Rollen, Gruppen and des normalen Verhaltens

Exabeam spart Zeit UND liefert bessere Erkennung



Manuelles und ineffizientes
Sicherheitsmanagement mit herkömmlichem SIEM



Automatisiertes und effizientes Security
Management mit New-Scale SIEM

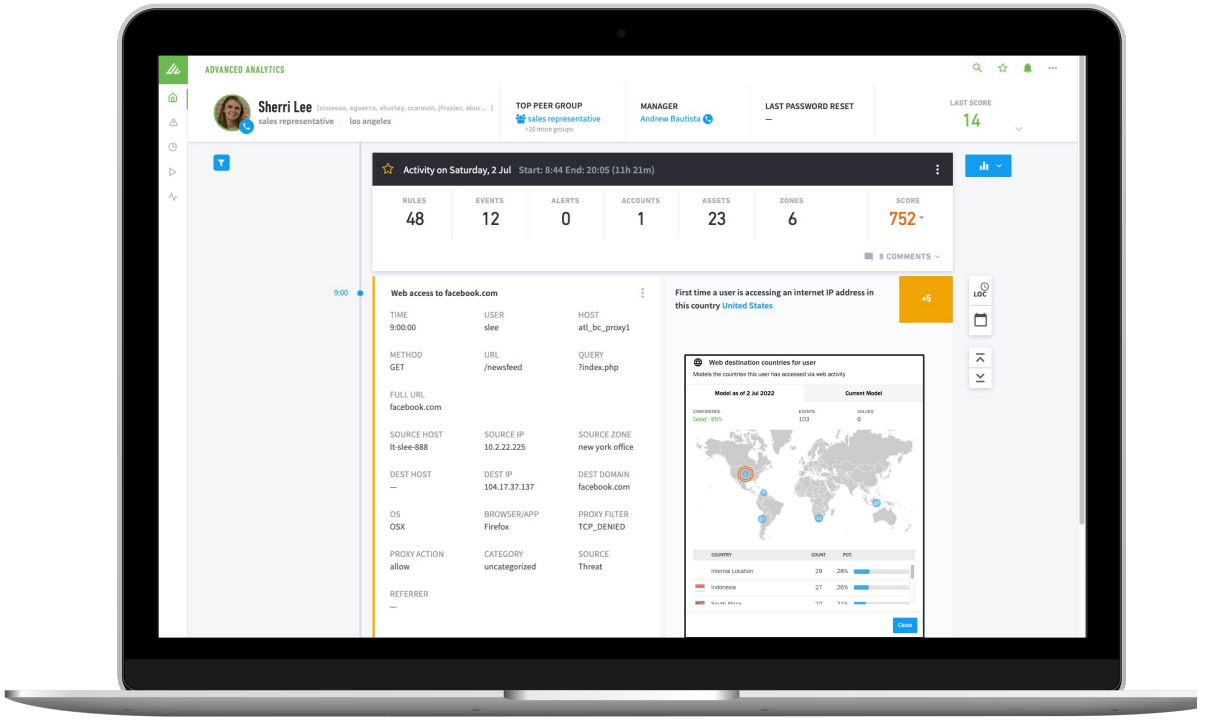
exabeam

Wie sieht effiziente Verhaltensanalyse aus?

Versteht das Normalverhalten aller Mitarbeiter und Geräte

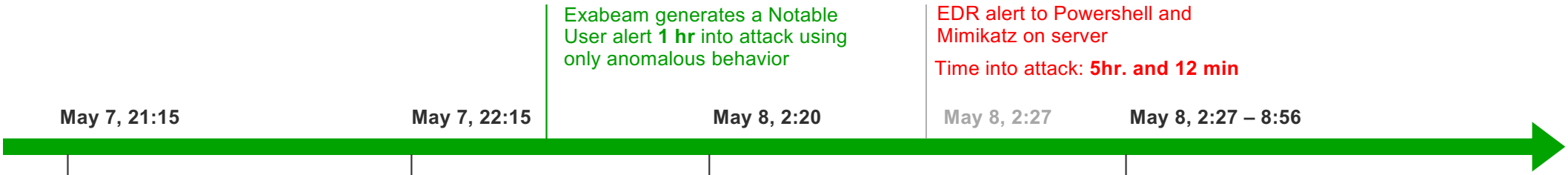
Intuitive Darstellung komplexer Verbindungen

Fokussiert auf die Anomalien mit hohem Risiko zuerst



exabeam

Exabeam zeigt das vollständige Bild bei einem *Compromised Insider*



Initial access: First login from Singapore for user and org

- First activity from ISP for user
- First OS/browser combination in user agent string

Risk score: +10

Lateral movement:

# of first access to asset for user: **272**

Risk score: +30

Lateral movement:

- Attacker pivots off initial host to ServerX
- First RDP activity for user
- First access to ServerX

Risk score: +30

Lateral movement & privilege escalation:

# of first access to assets by user: 487

# of first communication between assets : 487

# of first credential switches from host: **233**

Risk score: +60

Automation spart Zeit

- Detaillierte Darstellung des gesamten Vorfalls
- Liste der betroffenen Accounts automatisch erstellt
- Liste der betroffenen Devices automatisch erstellt
- Hohe Analysequalität – vollständiges Bild
- Gegenmaßnahmen können ganzheitlich eingeleitet werden

Nutzen für den Kunden

- Zeit- und Personaleinsparung
- Geringeres unternehmerisches Risiko
- SOC Analysten werden von Routineaufgaben entlastet
- Höhere Zufriedenheit des Personals

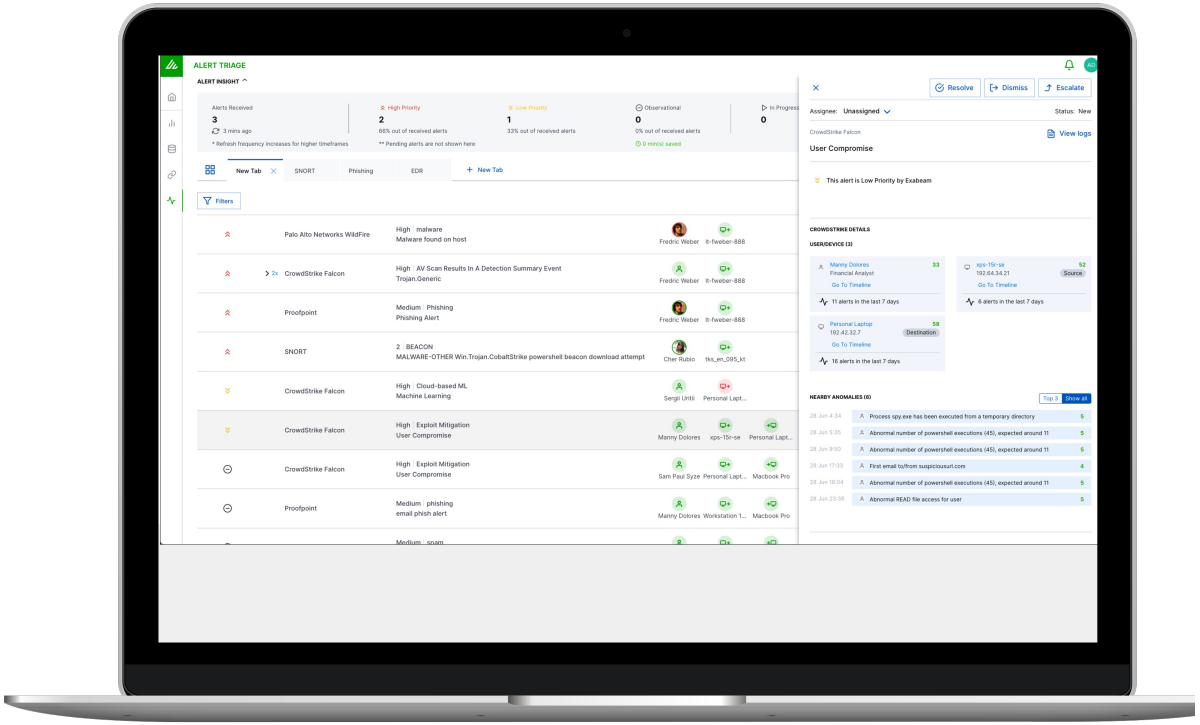
exabeam

Wie sieht eine gute Analyse eines Vorfalls aus?

Automation für den gesamten SOC Prozess

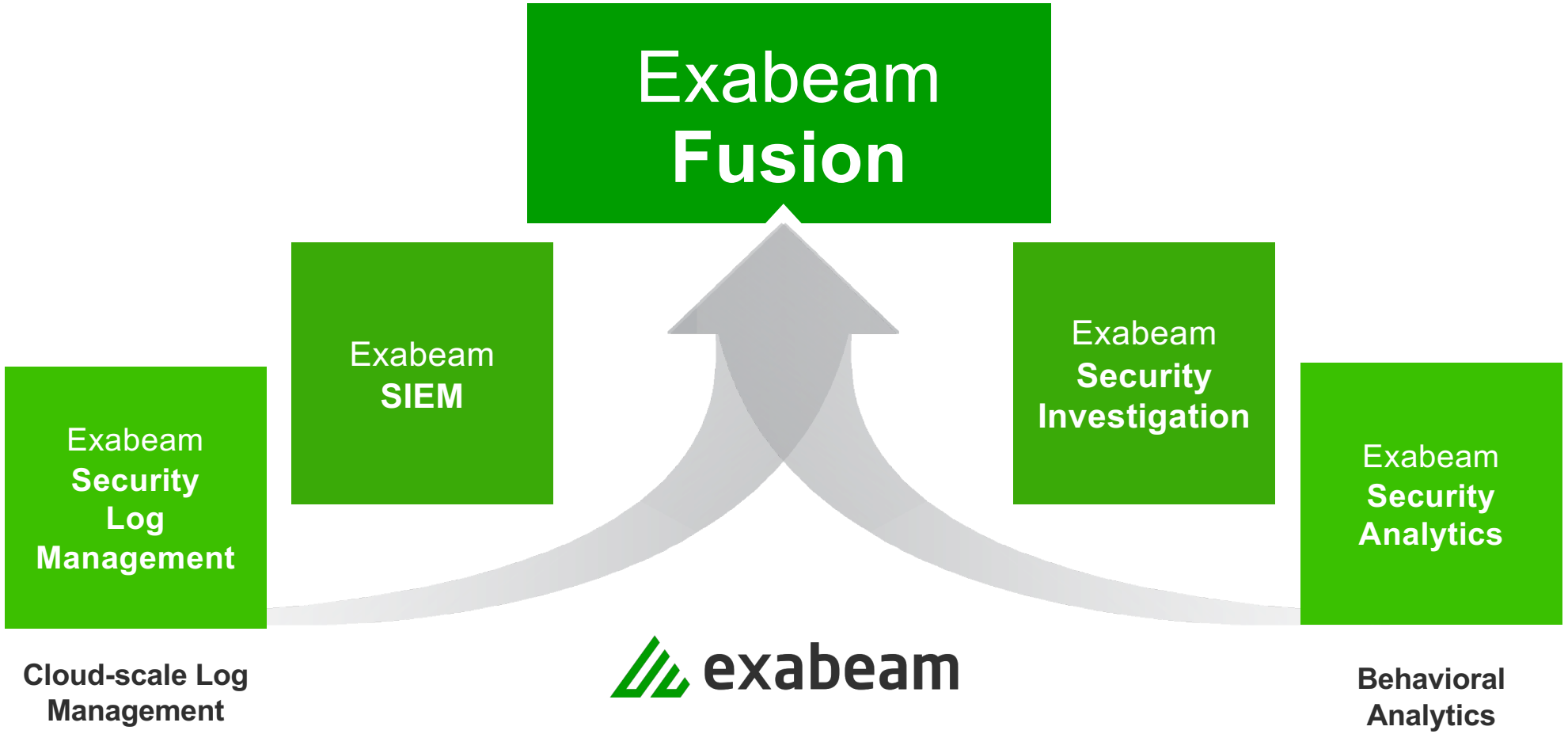
Alarme werden mit Kontext und dazugehörigen Events angereichert

Gegenmaßnahmen werden in Playbooks zusammengefasst und ausgeführt



exabeam

Mehrere Wege um mit Exabeam zu starten



exabeam

Detect the Undetectable™

exabeam

Thank you

Demo