empow

You have it in you.

i-SIEM

empowered by Elastic

Donnelley Financial Solutions

„empow ist einzigartig im Sicherheitssektor... sie sorgt dafür, dass alle Tools unseres Arsenals optimal und aufeinander abgestimmt arbeiten und unser Sicherheitsniveau effektiv gesteigert wird.

Dank empow kann ich sicher sein, dass meine Sicherheitsorganisation jedes Mal die richtige Antwort findet."

Dannie Combs, SVP und
Chief Information Security Officer

MIT Media Lab

„Als Universität müssen wir Dinge teilen, offen sein, aber dennoch die Privatsphäre unserer Nutzer schützen – das macht uns zu einem attraktiven Ziel für Cyber-Angreifer.

Mit empow konnten wir unsere Sicherheitsmaßnahmen optimieren und gleichzeitig den Datenschutz und die Transparenz der Vorgänge in unserem Netzwerk erhöhen."

Michail Bletsas, Director of Network
and Computing Systems

Anerkennung und Auszeichnungen

SC 2019 awards Europe **Winner**

„... Ersetzt komplexe und unverständliche Sicherheitssysteme..."

Forbes

Gartner **Cool Vendor** 2017

SC MEDIA

„empows Modelle erzeugen einen kleinen Satz strategischer Regeln, im Gegensatz zu den Hunderten oder Tausenden, die in den meisten Sicherheitsdaten- und Ereignismanagementsystemen (SIEM) verwendet werden.

„...empow hat sich seinen Platz unter den Top-Lösungsanbietern in seiner Kategorie verdient."

„Eine integrative Cybersecurity-Lösung"

NETWORKWORLD FROM IDG

7 erteilte Patente, 9 angemeldete Patente

Die Barrieren für SIEM

Organisationen möchten sich heute kaum noch auf ein SIEM-Projekt einlassen. Die Erfahrung – ihre eigene oder die von anderen – hat sie gelehrt, dass SIEMs komplex sind und eine lange Zeit zur Implementierung benötigen. Darüber hinaus erfordern sie, sobald sie einmal implementiert sind, ein großes Sicherheitsteam, das sie verwalten muss – Korrelationsregeln schreiben, viele Fehlalarme durchsehen und vieles mehr. Tatsache ist, dass Menschen die Cybersicherheitsdaten nicht so schnell durchsuchen und Sicherheitskorrelationsregeln schreiben können, die Angriffsmuster repräsentieren, wie Maschinen neue Angriffe erzeugen können. All dies macht SIEM-Projekte außerdem teuer, so dass die laufenden Kosten und Verwaltungskosten weit über die Kosten der Software hinausgehen.

Aus diesen Gründen verzögern viele Organisationen mit kleinen Sicherheitsteams die Implementierung eines SIEM oder wenden sich alternativen Lösungen wie MSSP-Anbietern zu.

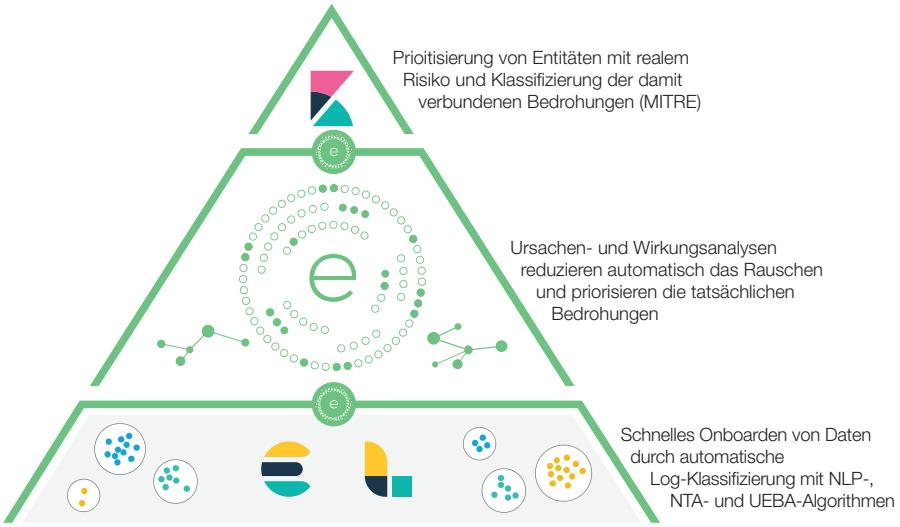
i-SIEM empowered by Elastic

empows patentierte intentbasierte SIEM-Technologie (bzw. i-SIEM) basiert auf KI- und Natural-Language-Processing-(NLP)-Algorithmen, kombiniert mit UEBA- und NTA-Engines, die zusammen einen automatisierten Klassifizierungs- und Priorisierungsprozess ermöglichen. Durch diese Automatisierung kann i-SIEM den gesamten Prozess des Schreibens von Korrelationsregeln umgehen. Der Prozess von i-SIEM führt zu einer sehr geringen Anzahl wirklich risikoreicher Entitäten (abzüglich der Berge von falsch-positiven Ergebnissen, die von anderen SIEMs erzeugt werden), die von weniger als einem Sicherheitsanalysten effektiv verwaltet werden können.

SIEM-Plattformen müssen alle IT-Daten in der Organisation sammeln und einen sehr schnellen Zugriff darauf ermöglichen. Um diesen Prozess zu rationalisieren, hat empow sich mit Elastic, dem führenden Unternehmen im Bereich der Datensuche mit über 300 Millionen Nutzern, in einer strategischen OEM-Partnerschaft zusammengeschlossen. empows einzigartige „regelfreie" SIEM-Technologie, die in die Datenbank- und Suchfunktionen von Elastic integriert ist, liefert das effizienteste und effektivste SIEM auf dem Markt.
Die integrierte Lösung bietet mittleren bis großen Unternehmen und Dienstanbietern eine skalierbare, sicherheitsoptimierte „Data Lake"-Lösung.

empow bietet Kunden zudem die vollständigen Elastic-Funktionen der Platinum-Lizenz (einschließlich Alarmierung, Überwachung, Berichterstattung, maschinelles Lernen, Canvas, Elastic Search SQL, Graphen-Algorithmen und andere) sowie den Elastic-Anbieter-Support.

In der Abbildung unten zeigen wir, wie sich das i-SIEM von empow nahtlos in die Tools Logstash, Beats und Kibana von Elastic integriert und so ein effektiveres SIEM-Konzept schafft. Beginnend am unteren Ende der Pyramide, ergänzt empow jedes Sicherheitsereignis mit der Absicht des Angreifers auf der Verarbeitungsebene. All diese angereicherten Logs werden in Elasticsearch gespeichert, wodurch die Analysten viel effizientere Untersuchungen und forensische Operationen durchführen können. In der Mitte der Pyramide wendet i-SIEM Cause & Effect Intelligence an, die automatisch alle klassifizierten Ereignisse korreliert und die tatsächlichen Angriffe und Entitäten mit realen Risiken priorisiert. An der Spitze der Pyramide nutzt empowow das Kibana-Framework, um diese hochriskanten Angriffe und Entitäten klar zu visualisieren und eine einfache Drill-Down-Analyse der wichtigsten Daten zu ermöglichen. Die Gesamtlösung bietet eine Top-Down-Analyse zur Identifizierung von Angriffen, und das alles ohne von Menschen erzeugte Regeln.



Vorteile von i-SIEM

Heutige SIEM-Lösungen	empows i-SIEM
Lange Dauer bis zur Ausgereiftheit – langwieriger und teurer Implementierungsprozess	Kürzester Weg zu einer ausgereiften Sicherheitslösung
⊗ Out-of-the-Box auf grundlegende Anwendungsfälle beschränkt	✓ Breite Abdeckung – automatische Korrelation von Sicherheitslogs (keine von Menschen erstellten Regeln erforderlich)
⊗ Reaktiv, beschränkt auf bekannte Angriffsmuster	✓ Proaktiv – leistungsstarke KI ermöglicht das permanente Erkennen neuer Angriffsmuster
⊗ Keine adaptiven Untersuchungs- und Incident-Response-Funktionen	✓ Automatisierte Untersuchungs- und Response-Prozesse
⊗ Überflutung des Systems mit Fehlalarmen	✓ Reduziert Fehlalarme um durchschnittlich mindestens 90 %
⊗ Aufwendige Integration mit Datenquellen	✓ Nahtlose Datenverarbeitung basierend auf empows Datenklassifizierungstechnologie
⊗ Mangel an allgemeinen Daten- und Loganalysetechniken Out-of-the-Box	✓ Best-in-Class-Data-Lake mit vollem Elastic-Funktionsumfang zur Loganalyse und größter Community
⊗ Hohe TCO – massiver Experteneinsatz, teuer und langsam in der Umsetzung	✓ Hoher ROI dank nahtloser Integration und nahezu keiner Wartungskosten

Abwehrmodelle

empows i-SIEM bietet vorgefertigte, anpassbare Abwehrmodelle (als Security Apps bezeichnet), mit denen Unternehmen bestimmen können, auf welche Risiken und Compliance-Anforderungen sie sich konzentrieren möchten. Auf diese Weise kann das i-SIEM von empow Angriffe mit den entsprechenden böswilligen Absichten optimal erkennen und angemessene Untersuchungen und Reaktionen einleiten. i-SIEM ermöglicht es den Benutzern, Modelle mit Hilfe der Sprache MITRE ATT&CK zu definieren, wodurch die Klassifizierung vereinheitlicht und übersetzbar wird.

Security Apps können ganz leicht aus dem Security App Store von empow heruntergeladen und binnen Minuten implementiert werden. Vorgefertigte Sicherheitsmodelle decken sowohl allgemeine als auch komplexere Anwendungsfälle ab, darunter: Bedrohungen durch Insider, Datenexfiltration, Rechteeskalation, Suche nach kompromittierten Hosts und Benutzern, Identitätsdiebstahl, verschiedene Untersuchungsabläufe und mehr. Mit jedem Modell können komplexe Bedrohungen erkannt und bekämpft werden, darunter:

- **Ransomware**
- **Identitätsdiebstahl und Account-Übernahme (ATO)**
- **Informationssammlung**
- **Phishing und Social-Media-Angriffskampagnen**
- **Bedrohung durch Insider**
- **Diebstahl von Daten**

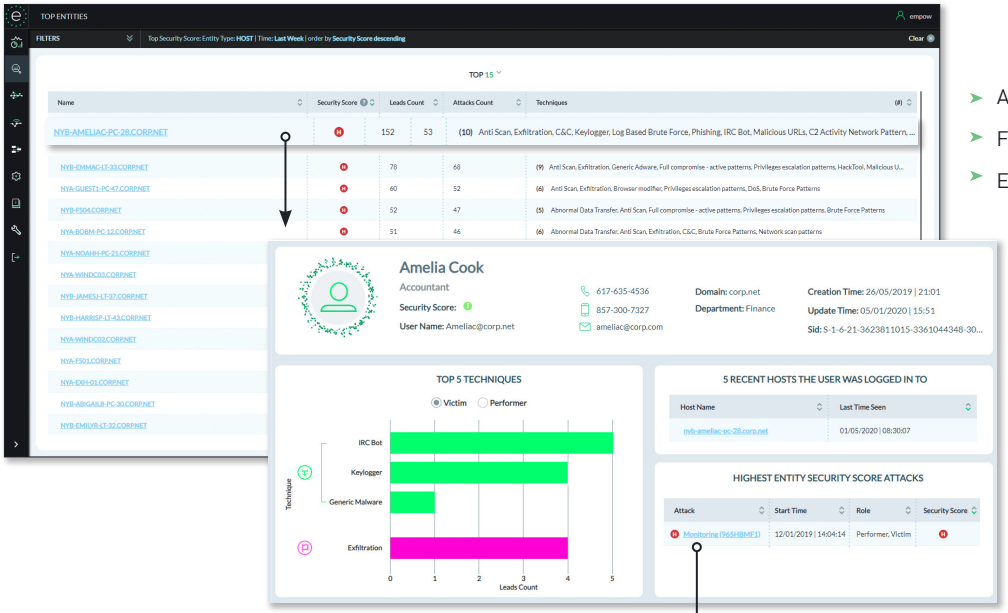
Benutzererfahrung - von oben nach unten arbeiten

i-SIEM stellt den Arbeitsablauf des Analysten auf den Kopf. Statt einer Armee von Analysten, die sich von unten nach oben durch die Logs arbeiten, können sie nun von oben nach unten arbeiten. Der Sicherheitsanalyst erhält eine kleine Anzahl von Hochrisikoeinheiten, nimmt jede verdächtige Einheit genau unter die Lupe, sieht alle Stufen und Informationen zu dieser Einheit, kann das Risiko für die Organisation nachvollziehen und ist nun in der Lage, darauf zu reagieren.

Dieser Arbeitsablauf bietet drei wesentliche Vorteile:

- Schnellere Ursachenanalyse, d.h. Nachvollziehen der Quelle des Angriffs (wie alles begann).
- Potenzielle Auswirkungen des Angriffs vollständig erfassen. Zum Beispiel, wie viele andere Einheiten von derselben Angriffskampagne infiziert sind, oder das Ausmaß des Angriffs, der sich innerhalb der Organisation ausbreitet.
- Schnelle und effektive Abhilfemaßnahmen dank der Sprache MITRE ATT&CK™.

Echtzeit-Überwachung von priorisierten Einheiten

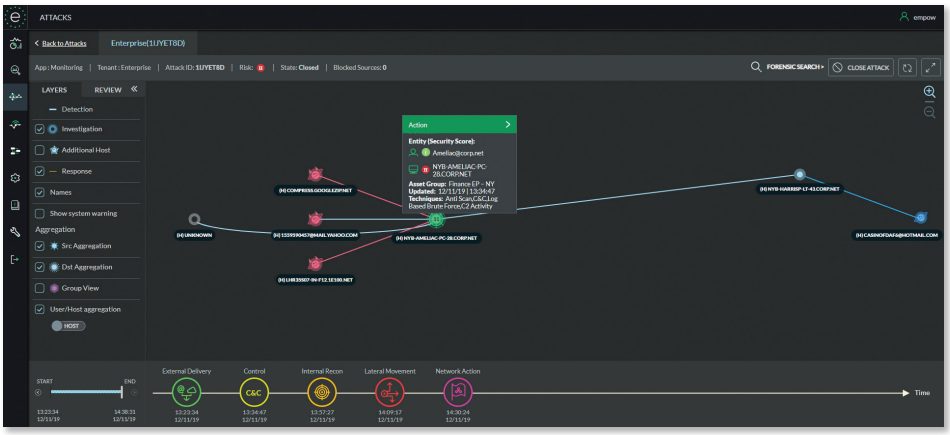


- Automatische Priorisierung
- Fokus auf hochsensible Einheiten
- Eine gemeinsame Sprache

Einheitenkarte

- Organisatorischer Kontext der Einheit
- Auswirkungsanalysewert

Angriffsgeschichte



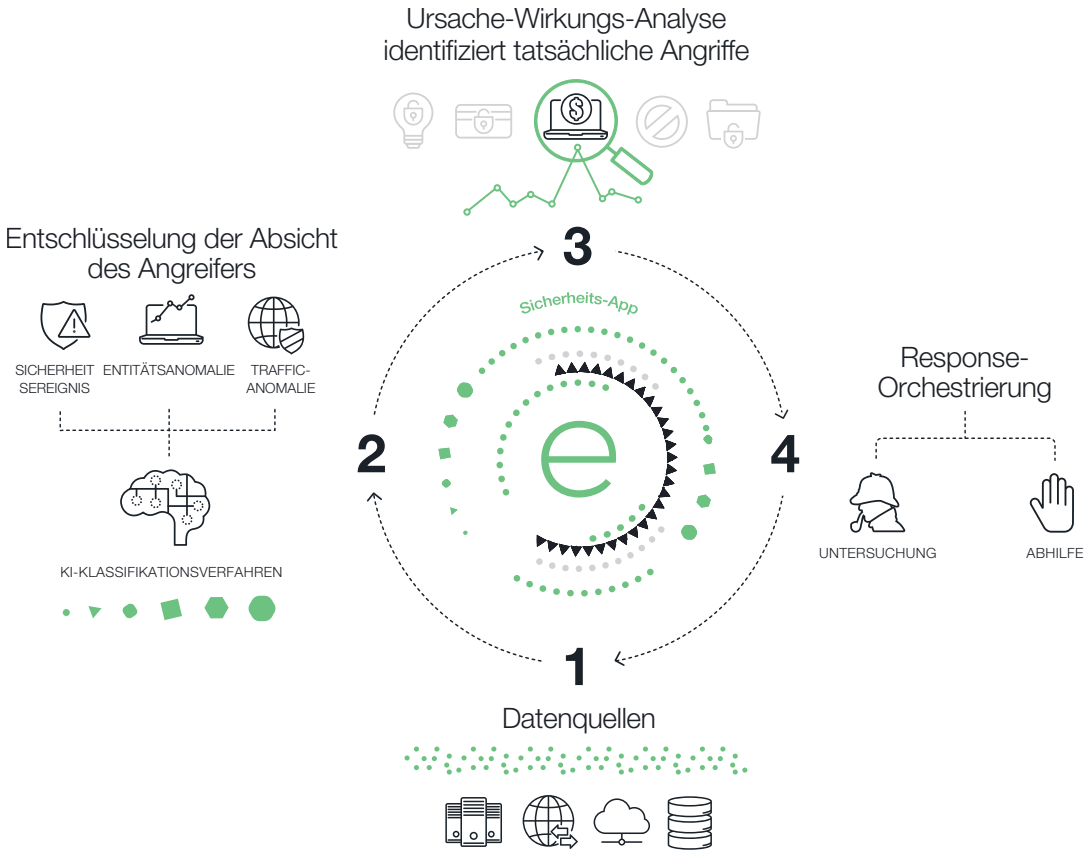
- Zeitbasierte Visualisierung der Angriffsgeschichte
- Schnelle Ursachenanalyse
- Response-Arten vorschlagen
- Ermöglicht forensische Suche und Jagd

i-SIEM ist durch vordefinierte und angepasste Warnmeldungen, welche die Benachrichtigung von Sicherheitsbetriebssystemen von Drittanbietern, einschließlich Ticketing- und Fallmanagementlösungen, ermöglichen, nahtlos in die bestehenden Arbeitsabläufe und Systeme der Organisation integriert.

So funktioniert es

empows i-SIEM erfasst und analysiert die IT-Daten und bringt dann die ausgewählten und auf Kundenbedürfnisse ausgerichteten Abwehrmodelle zum Einsatz. Die i-SIEM-Technologie bietet eine ständig aktualisierte Schleife von Erkennung, Untersuchung und Reaktion.

Die Lösung wird durch proprietäre, patentierte KI-Technologien ermöglicht, die strategisch in folgenden Prozess eingebunden sind:



1/ Datenquellen

Das integrierte i-SIEM empowered by Elastic erfasst sämtliche IT-Datentypen, einschließlich Sicherheitslogs, aufbereitete Sicherheitsdaten, OS-Logs, Server- und Anwendungslogs, Daten zum Netzwerkfluss und mehr, durch Nutzung einer Reihe von verfügbaren Datenquellen-Plug-ins.

2/ Entschlüsselung böswilliger Absichten

Die KI-, NLP- und Adaptive Expert-Engines von empow klassifizieren Verhaltensauffälligkeiten und Absichten potenzieller Angreifer in der gemeinsamen Sprache MITRE ATT&CK. Böswillige Absichten werden dabei in drei Kategorien unterteilt: Auffälligkeiten im Benutzerverhalten, Auffälligkeiten im Netzwerkverkehr und Sicherheitsevents. Dieser Prozess läuft kontinuierlich und automatisch ab, nahezu ohne menschliche Eingriffe. Logs und Events werden dabei mit Intent-Metadaten versehen und in die Elastic-DB eingespeist. Beispiele einer Intent-Klassifizierung: Interne Aufklärung, externe Zustellungsarten, Eskalation von lokalen und Remote-Rechten, Extraktion personenbezogener Daten und Finanzdaten und Ransomware sowie weitere MITRE-Klassen.

3/ Analyse von Ursache und Wirkung

empows Sicherheitsanalyse-Engine identifiziert Kausalzusammenhänge zwischen den erfassten entzifferten Absichten, fasst sie zusammen und stellt dabei die echten Angriffe und kompromittierten Entitäten im Unternehmen in den Vordergrund.

Diese Engine emuliert Prozesse von menschlichen Sicherheitsexperten, filtert dabei echte Angriffe aus den Datenmassen heraus und entscheidet in Echtzeit anhand der Angriffsabsicht, welche Untersuchungsmethoden erforderlich und welche proaktiven Reaktionsmaßnahmen einzusetzen sind.

4/ Reaktionsorchestrierung

empows Contextual Orchestration Engine identifiziert und selektiert dynamisch die besten verfügbaren Lösungen und Netzwerktools zur Durchführung der Untersuchungs- und Reaktionsmaßnahmen. Dies führt zu einer schnellen und optimalen Ereignisreaktion bei gleichzeitiger Vereinfachung des Sicherheitsbetriebs und Vermeidung von Wartungskosten.

UEBA- und NTA-Engines

empows i-SIEM umfasst sofort einsetzbare UEBA-(User Entity Behavioral Analytics)- und NTA-(Network Traffic Anomaly)-Engines, die normale Verhaltensmuster von Benutzern, Anwendungen und Datenverkehr lernen und analysieren, um dann bei Abweichungen von diesen Mustern Auffälligkeiten zu erkennen.

Diese Engines verleihen einem Detektionssystem eine wichtige, zusätzliche Ebene:

- Sie erkennen verdächtige und auffällige Verhaltensweisen, die darauf hinweisen, dass ein Angreifer bereits in das System eingedrungen oder ein böswilliger Insider aktiv ist – Signale, die von signaturbasierten oder heuristischen Tools und von statischen, auf Schwellenwerten basierenden SIEM-Regeln übersehen werden.
- Sie identifizieren kritische Wahrnehmungslücken, wo die meisten Unternehmen lediglich perimeter- und hostbasierte Tools einsetzen und ihre internen Netzwerke, ihre Cloud und ihre Benutzeraktivitäten unbeaufsichtigt lassen.
- Durch Erkennung zusätzlicher Angriffsschritte entlang der Cyber Kill Chain können sie zur Bestätigung und Vervollständigung von Angriffswegen beitragen und entsprechende Gegenmaßnahmen einleiten.
- Ihre Bereitstellung als integrierte Out-of-the-Box-Features von empows i-SIEM ermöglicht die Zustellung von Alarmmeldungen, die automatisch nach Angriffsabsichten klassifiziert werden – ohne Korrelationsregeln.

Klassifikation auf der Grundlage von Bedrohungsinformationen

i-SIEM integriert Bedrohungsinformationen in Echtzeit aus verschiedenen Quellen von Drittanbietern, einschließlich kommerzieller und offener Quellen, um das System mit Informationen zu ergänzen, die eine Automatisierung der Klassifizierung von Logs und der Untersuchungsprozesse ermöglichen. Das TI-basierte Klassifizierungsverfahren ermöglicht es:

- Alle Logs in eine Sprache (MITRE ATT&CK) zu übersetzen, auch wenn die ursprüngliche Beschreibung der Logs vage ist oder nicht existiert
- Gutartige Logs zu klassifizieren, d.h. Rauschen und Fehlalarme zu entfernen
- Websites mit schlechtem Ruf zu identifizieren und zu klassifizieren

Integration von Datenquellen

Im Angebot von empow sind eine Reihe von Plug-ins für Netzwerke, Server und Sicherheitsdatenquellen von Drittanbietern enthalten, wie z. B. Intrusion-Detection-Systeme (IDS), Netzwerk-Malware-Schutz, Reputationsdienste, Endpoint-Schutz, Firewalls, OS-Logs und viele weitere. Neue Plug-ins können bei Bedarf von empows Professional Services Team oder speziellen Sicherheitsteams des Kunden entwickelt werden. Alternativ können auch über die Community bereitgestellte Elastic Logstash-Plug-ins verwendet werden.

Das i-SIEM-Ökosystem unterstützt Produkte von Dutzenden von Anbietern, darunter:

paloalto NETWORKS, lastline, McAfee, Symantec, CISCO, FORCEPOINT

cybereason, TREND MICRO, SOURCEfire, Carbon Black., Check Point SOFTWARE TECHNOLOGIES LTD, WAZUH

CYLANCE, FIREEYE, SOPHOS, WEBROOT, ANOMALI, f5

JUNIPER NETWORKS, Microsoft, CROWDSTRIKE, eset, SNORT, FORTINET

i-SIEM empowered by Elastic

Bietet eine Abkürzung zur ausgereiften Sicherheitslösung und ein SIEM, das von weniger als einem Sicherheitsanalysten verwaltet werden kann.

Identifiziert und entschärft automatisch hochentwickelte Bedrohungen, die von einzelnen (isolierten) Tools übersehen werden – keine Regeln erforderlich.

Proaktiv – leistungsstarke KI ermöglicht das permanente Erkennen neuer Angriffsmuster

Reduziert Rauschen um mindestens 90 % und erhöht die Wirksamkeit der Sicherheitssysteme um das 10-Fache.

Bietet EINE EINZIGE Quelle für durchsuchbaren Best-in-Class-Data-Lake (von Elastic) kombiniert mit intentbasiertem SIEM.

Verwandeln Sie das, was Sie haben, in das, was Sie brauchen

empow
You have it in you.

Tel: +1-877-647-4361
129 Newbury Street, 2nd Floor
Boston, MA 02116, USA

Tel: +972-3-519-5517
Hayetzira 29, Ramat Gan,
Israel 5252171

www.empow.co
info@empow.co