CYBEREASONS MASSGESCHNEIDERTE ARCHITEKTUR_

NEUER BLICKWINKEL AUF IT-SICHERHEIT

IT-Infrastrukturen reichern sich immer weiter mit Informationen an. Zur effektiven Verteidigung gegen Cyber-Angriffe ist es daher nötig, die Aktivitäten, Beziehungen und Rollen eines komplexen Datenpools zu verstehen: Die maßgeschneiderte Architektur von Cybereason bietet Sicherheitsteams einen völlig neuen technischen Ansatzpunkt. In Echtzeit zeigt sie bösartige Aktivitäten auf Firmenebene an und deckt Anomalien sowie Gefahren auf. Gleichzeitig unterscheidet die Lösung zwischen gutartigen und bösartigen Vorgängen.

SKALIERBARE ERKENNUNG

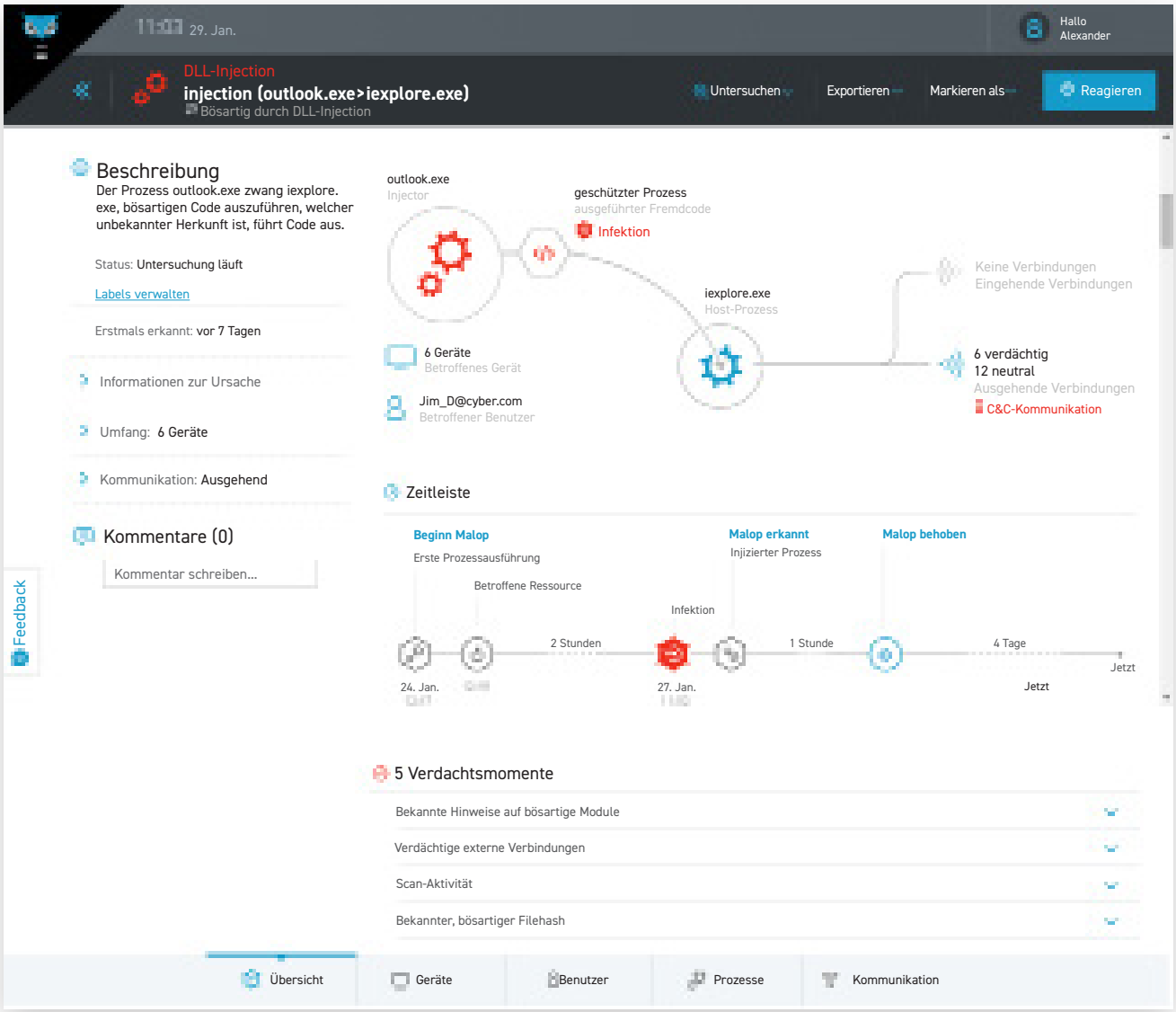
Eine Deep-Graph-Technologie ergänzt die proprietäre Architektur von Cybereason – eine zentralisierte In-Memory-Graphdatenbank. Diese erweitert sich durch gesammelte Informationen zu Datei- und Netzwerkaktivitäten ständig. Darüber hinaus verbindet Deep Graph Datenpunkte und Endpoints eines Unternehmens dauerhaft miteinander und fragt so Millionen von Aktivitäten pro Sekunde ab. Die Dynamik von Deep Graph ermöglicht es, bösartige Aktivitäten präzise von gutartigen zu unterscheiden sowie verbundene Angriffselemente automatisch in einem einzigen Alert zusammenzufassen

ERKENNUNG KOMPLEXER BEDROHUNGEN IN ECHTZEIT

Neben Feeds, Signaturen oder statischen IOCs, um Bedrohungen sichtbar zu machen, nutzt Cybereason Verhaltensanalysen und korreliert sie. Damit haben Verteidiger gegenüber Angreifern einen klaren Vorteil: Die Cyber Defense Plattform von Cybereason wurde speziell zur Prüfung von Dateiaktivitäten und nicht nur von Dateieigenschaften entwickelt. Sie erkennt automatisch anhand vorkonfigurierter Modelle, ob feindliche Tools, Techniken und Prozesse (TTPs) aktiv sind – und das mit einer Geschwindigkeit von acht Millionen Rechenvorgängen pro Sekunde.

VISUALISIERUNG BÖSARTIGER VORGÄNGE

Unternehmen erhalten durch die maßgeschneiderte Architektur von Cybereason eine umfassende Übersicht über jeden unbefugten Zugriff. Dafür werden Informationen zu Benutzern, Geräten, Prozessen, Netzwerkverbindungen oder Autostarts nach und nach in eine einzigartige Kunden-Deep-Graph-Instanz eingepflegt und analysiert. Nutzer erhalten so eine Cybereason Warnung über eine Malop (oder Malicious Operation), welche die komplette Historie der Ereignisse auflistet. Das ermöglicht Analysten anhand einer einzigen Warnung alle mit dem Angriff in Verbindung stehenden Elemente einzusehen: den Beginn des Angriffs, alle betroffenen Geräte und Nutzer, eingehende und ausgehende Kommunikation sowie eine Angriffszeitleiste. So können sie das Ausmaß eines Angriffs zeitnah einschätzen.



Da die Lösung automatisch alle Schlüsselelemente für eine Untersuchung vereint, können Analysten schnell alle Details einsehen und genau feststellen, was passiert ist, bevor und nachdem der Malop ausgelöst wurde und so das Ausmaß und die Schwere des Angriffs zeitnah einschätzen.

VEREINFACHUNG DER JAGD NACH ANGREIFERN

Die Cybereason Investigation Console spiegelt Analysten den kompletten firmenweiten Kontext wider. Die ständig aktualisierten Daten durch Deep Graph ermöglichen eine einfache Untersuchung, wie Nutzer, Prozesse, Netzwerkverbindungen, Dateien oder Maschinen miteinander agieren: Das erlaubt Analysten einfach Zusammenhänge zwischen Benutzern, Geräten, oder Netzwerkverbindungen zu untersuchen und jeweiliges Verhalten zu verknüpfen. Darüber hinaus sammelt die Cybereason Lösung Daten und Informationen im Arbeitsspeicher. Analysten können so innerhalb von Sekunden komplexe Untersuchungen durchführen und erhalten die benötigten Informationen, um einen Angriff effektiv abzuwehren, bevor Schäden entstehen.

DER VORSPRUNG DURCH DIE CYBEREASON ARCHITEKTUR

DIE CYBEREASON ARCHITEKTUR IST SO AUSGERICHTET, DASS SIE FIRMEN FOLGENDES ERMÖGLICHT:

- **Anpassung auch an größte Unternehmen**
  Deep Graph verarbeitet riesige Datenmengen in Höchstgeschwindigkeit: Alle Aktivitäten werden im Arbeitsspeicher ausgeführt, wodurch die Engine Informationen viel schneller miteinander abfragen und verbinden kann als herkömmliche Lösungen. Das ermöglicht selbst größten Unternehmen bösartige Aktivitäten nahezu in Echtzeit erkennen zu können.

- **Schnellere Entwicklung als der Feind**
  Die Cybereason Lösung erkennt automatisch komplexe bösartige Aktivitäten auf Basis von Verhaltensanalysen. Die Lösung ist so konfiguriert, dass sie automatisch nach komplexen Bedrohungen sucht. Dies gilt einschließlich für DGA, Pass the Ticket/Hash, Ransomware und dateilose Malware-Angriffe.

- **Verbesserung der Effizienz Ihrer Analysten**
  Die Cybereason Lösung zeigt automatisch Ereignisse mit hoher Priorität an und stellt alle Angriffselemente grafisch in einer Übersicht dar. Das vermeidet zu häufige Warnungen und ermöglicht es Analysten aus allen Bereichen, die dringendsten Vorfälle zu erkennen und darauf umgehend zu reagieren.

- **Reduktion von Risiken durch erhöhte Transparenz**
  Die Cybereason Lösung bietet Firmen eine beispiellose Transparenz, damit Analysten Risiken verstehen und schnell auf Bedrohungen reagieren können. Sie erhalten ein vollständiges Bild über Geräte, angemeldete Benutzer sowie von ausgeführten Prozessen und Modulen in Ihrem Unternehmen.

Komplexität und Dynamik von Daten in einer Firma erfordern eine flexible Lösung - keine statische.