Ransomware

Die wichtigsten Vorteile

- Selbstlernende Cyber-KI macht sich entwickelnde Ransomware unschädlich – ohne Regeln oder Bedrohungssignaturen
- Das Enterprise Immune System identifiziert auch neuartige und sehr gezielte Ransomware-Stämme
- Antigena reagiert eigenständig in Echtzeit – egal wo, wann und wie der Angriff erfolgt
- Der Cyber AI Analyst untersucht Vorfälle automatisch Ransomware-Vorfälle und stellt alle wichtigen Informationen bereit, die Sie für die Behebung benötigen

Abbildung 1: Cyber-KI erkennt Ransomware-Angriff

Verluste in Höhe von 381 Mio. US-Dollar durch Ransomware-Angriffe entstanden im vergangenen Jahr aus 350 Unternehmen

Quelle: Hiscox, 2020

Die heutigen Arbeitsplatzvorschriften und technischen Innovationen entwickeln sich rasant weiter und Ransomware-Angriffe werden immer raffinierter und weitreichender.

Es bilden sich neue Ransomware-Stämme heraus, die dateilose Malware und Taktiken zur Datenausschleusung nutzen, und gewiefte Angreifer nutzen jede Veränderung der Rahmenbedingungen, um noch effektivere Kampagnen zu starten. Herkömmliche Sicherheitstools, die Cyberbedrohungen nur anhand von Regeln und Signaturen erkennen, sind blind für sich entwickelnde Ransomware-Stämme, für die es keine Signaturen gibt.

Sicherheitsteams können mit traditionellen Tools allein nichts ausrichten, vor allem nicht, wenn sie unterbesetzt oder nicht im Büro sind. Stattdessen brauchen Unternehmen eine Sicherheitstechnologie, die Ransomware stoppen kann, sobald sich diese entwickelt und bevor sie Schaden anrichten kann.

Darktrace Cyber-KI-Plattform: die Erkennung und Unterbindung von neu auftretende Ransomware

Die Darktrace Cyber-KI-Plattform besitzt die einzigartige Fähigkeit, komplexe Ransomware in Echtzeit unschädlich zu machen – ohne Daten zu bekannten Bedrohungen oder Signaturen. Die Cyber-KI basiert auf nichtüberwachtem maschinellem Lernen und Deep-Learning-Methoden und lernt die normalen Verhaltensmuster, die sogenannten „Patterns of Life", jedes Benutzers und jeder Technologie im Unternehmen. So ist sie in der Lage, subtile Abweichungen zu erkennen, die auf eine sich entwickelnde Bedrohung hindeuten.

Das Enterprise Immune System nutzt das sukzessive angereicherte Wissen der Cyber-KI über die normalen Verhaltensweisen, um Cyberbedrohungen jeder Art aufzuspüren, auch völlig neuartige Ransomware, die von allen anderen Verteidigungsstrategien übersehen wird. Der Cyber AI Analyst als wichtige Komponente des Immunsystem-Ansatzes untersucht automatisch jede Bedrohung und hilft Ihnen, jedes betroffene Gerät zu finden und das volle Ausmaß eines Ransomware-Vorfalls zu verstehen und zu.

Sobald ein schwerwiegender Angriff erkannt wurde, stoppt Darktrace Antigena – die plattformeigene Technologie für eigenständige Reaktion – die schädliche Aktivität binnen Sekunden. Angriffe werden gezielt und minimalinvasiv unschädlich gemacht, während der Geschäftsbetrieb ganz normal weiterlaufen kann. Die Technologie passt sich auf intelligente Weise den Bedrohungen an, während sie sich entwickeln, und schützt Ihre gesamte Belegschaft rund um die Uhr. Das ist vor allem dann entscheidend, wenn Sicherheitsteams überlastet oder nicht im Büro sind.

Blitzschnelle Resilienz ist unumgänglich, um die Auswirkungen von Ransomware zu minimieren, die häufig in wenigen Minuten die Infrastruktur eines Unternehmens verschlüsseln kann. Die Cyber-KI-Plattform ist auch in einzigartiger Weise in der Lage, Muster im Unternehmen in Beziehung zu setzen und damit zentrale Einblicke und Steuerungsmöglichkeiten bereitzustellen, wenn Ransomware-Angriffe unterschiedliche Teile des digitalen Ökosystems attackieren – von E-Mail-Systemen über SaaS-Plattformen bis hin zu Unternehmensnetzwerken oder Industriesystemen.

Antigena Network: Neutralisiert Angriffe in Echtzeit

Wenn sich Ransomware entwickelt, ist Antigena Network die einzige Lösung, die den Angriff in Echtzeit und mit chirurgischer Präzision abwehren kann, selbst wenn die Bedrohung sehr gezielt oder völlig unbekannt ist. Die Technologie reagiert eigenständig mit intelligenten, verhältnismäßigen Maßnahmen – von der Trennung einer Verbindung bis hin zur Durchsetzung des normalen „Pattern of Life" eines bestimmten Geräts. Wenn Ihr Sicherheitsteam überlastet oder nicht im Büro ist, können Sie sich darauf verlassen, dass Ihr gesamtes Unternehmen mit Antigena Network rund um die Uhr geschützt ist.

Darktrace hat die Antigena Autonomous Response Technologie entwickelt, die das sukzessive angereicherte Wissen der Cyber-KI über das Unternehmen nutzt, um sich in Echtzeit an Bedrohungen anzupassen und basierend auf Ihrem spezifischen Kontext die am besten geeigneten Maßnahmen zu ergreifen. Anstatt einen Binärblock zu verwenden (z. B. das Gerät vollständig zu isolieren), wie es herkömmliche Tools tun würden, agiert Antigena chirurgisch präzise, um den Angriff zu stoppen. So kann der Geschäftsbetrieb ganz normal weiterlaufen. Sie können die Technologie auch in Ihre bestehende Sicherheitsinfrastruktur integrieren, um Ihren Sicherheits-Stack zu erweitern – indem Firewalls, SIEMs und andere Tools mit KI-basierten Einblicken und Handlungsmöglichkeiten angereichert werden.

Darktrace stoppt Ryuk-Ransomware während einer Teststellung

Als die Ryuk-Ransomware in einem Unternehmen zuschlug, in dem Darktrace gerade testweise installiert war, erkannte das Enterprise Immune System diese sofort – und demonstrierte, wie Antigena Network die Bedrohung komplett hätte stoppen können.

Zunächst bemerkte die Cyber-KI eine sehr ungewöhnliche Admin-Aktivität, die vorher noch nie im Netzwerk beobachtet worden war. Nach dem Vorfall verfolgte das Unternehmen die Kompromittierung, mit der alles begonnen hatte, zurück und fand den Ursprung in einem Bereich seines Netzwerks, in den Darktrace während der Testphase keinen Einblick hatte.

Die Cyber-KI stellte dann fest, dass der berühmt-berüchtigte TrickBot Banking-Trojaner heruntergeladen wurde. Anschließend wurde Command & Control-Traffic beobachtet. Wenngleich viele Geräte anormales Verhalten aufwiesen, konnte die Cyber-KI ein bestimmtes Gerät an der Quelle ausmachen.

Als die Ryuk-Ransomware schließlich zuschlug, wurden über 200.000 Dateien in nur 12 Stunden verschlüsselt. Aufgrund der unübersichtlich vielen verdächtigen SMB-Aktivitäten konnte sich die Cyber-KI ein klares Bild vom Ausmaß des Angriffs machen und das Unternehmen entsprechend warnen.

Hätte das Team nicht erst nach der Verschlüsselung auf die Warnmeldungen von Darktrace reagiert, hätte dieser Ransomware-Angriff gestoppt werden können, gleich nachdem das Enterprise Immune System die erste Hinweise auf eine Kompromittierung erkannt hatte.

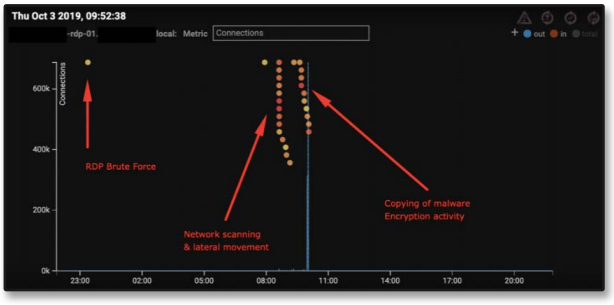

Abbildung 2: UI-Diagramm zeigt beispielhaften Ransomware-Angriff: Jeder Punkt stellte eine Warnmeldung von Darktrace dar.

Eigenständige Reaktion binnen Sekunden

Wäre in dem Unternehmen die Antigena Network Autonomous Response Technologie installiert gewesen, wäre es nicht schlimm gewesen, dass niemand auf die Warnmeldungen von Darktrace reagiert hat: Während vier Stunden zwischen dem ausführbaren Download und der ersten verschlüsselten Datei vergingen, hätte Antigena die Bedrohung binnen Sekunden unschädlich gemacht. Antigena hätte als Reaktion auf einige der Warnmeldungen bei diesem Vorfall folgende Maßnahmen ergriffen:

- **Ungewöhnliche Admin-SMB-Sitzung:** Verwendung kompromittierter Zugangsdaten für die Serveranmeldung
  - **Maßnahme von Antigena:** Diese einzelne Anomalie löst keine Maßnahme aus, erhöht aber die Warnstufe.
- **Neue Admin-Zugangsdaten auf Client:** Der Angreifer verwendete verschiedene neue Admin-Zugangsdaten auf dem Gerät
  - **Maßnahme von Antigena:** Da jetzt zuverlässig auf eine Bedrohung geschlossen werden kann, würde Antigena die typischen „Patterns of Life" für die Anmeldung durchsetzen; alle Administratoren, die sich normalerweise bei diesem Gerät anmelden, können dies auch weiterhin tun, es werden nur neue Logins für eine Stunde blockiert.
- **Netzwerk-Scan:**Der Angreifer scannte das Netzwerk, um weitere Angriffsopfer zu identifizieren
  - **Maßnahme von Antigena:** Dieser Server hatte das Netzwerk noch nie zuvor gescannt – nur Admin-Geräte tun dies. Antigena hätte daher dafür gesorgt, dass das Gerät das Netzwerk zwei Stunden lang nicht scannen kann.
- **EXE von ungewöhnlichem externem Ort:** Payload-Downloads für weitere Infektion in einer späteren Phase
  - **Maßnahme von Antigena:** Antigena würde dem Gerät weiterhin normale Downloads erlauben, nicht aber Downloads von ungewöhnlichen Orten.

Antigena Email:
Stoppt Ransomware an der Quelle

Viele Ransomware-Angriffe erfolgen über E-Mail-Plattformen. Das zeigt, dass traditionelle E-Mail-Gateways und herkömmliche Erkennungsansätze, die auf Regeln und Signaturen basieren, nicht stark genug sind, um komplexe Ransomware abzuwehren. Hinzu kommt, dass diese traditionellen Lösungen nicht weitreichend genug und nicht in der Lage sind, E-Mail-Aktivitäten mit schädlichen Handlungen in der gesamten digitalen Infrastruktur in Beziehung zu setzen.

Mithilfe der leistungsstarken Cyber-KI macht sich Antigena Email ein umfassendes Bild von dem Individuum hinter der E-Mail-Adresse. Die Technologie passt sich an Ihre dynamische Belegschaft an, um kaum merkliche Veränderungen im Verhalten zu erkennen, die auf eine Ransomware-Kampagne hindeuten.

Sie reagiert dann eigenständig und verhältnismäßig, um die Bedrohung blitzschnell zu stoppen und Ihr Unternehmen vor Schaden zu bewahren – beispielsweise kann die E-Mail zurückgehalten, ein Link blockiert oder ein Anhang in einen harmlosen Dateityp konvertiert werden.

Sollte die Ransomware über den Posteingang in das Netzwerk gelangen, ist Antigena Email in einzigartiger Weise in der Lage, zusammen mit dem Enterprise Immune System den Angriff zum Ursprung rückzuverfolgen und eine laterale Ausbreitung zu verhindern.

Die Cyber-KI setzt Aktivitätsmuster aus den übrigen Bereichen des Unternehmens mit der E-Mail-Umgebung in Beziehung und kann auf dieser Grundlage eine Ursachenanalyse vornehmen. Dabei können die E-Mail-Quelle und sonstige E-Mail-Aktivität, die mit dem Vorfall zusammenhängt, identifiziert werden. Antigena Email holt dann weitere gefährliche E-Mails aus den Posteingängen anderer Mitarbeiter und minimiert dadurch das Ausmaß eines Ransomware-Angriffs.

Bis 2021 wird es alle 11 Sekunden einen Ransomware-Angriff geben.

Quelle: Cybersecurity Ventures

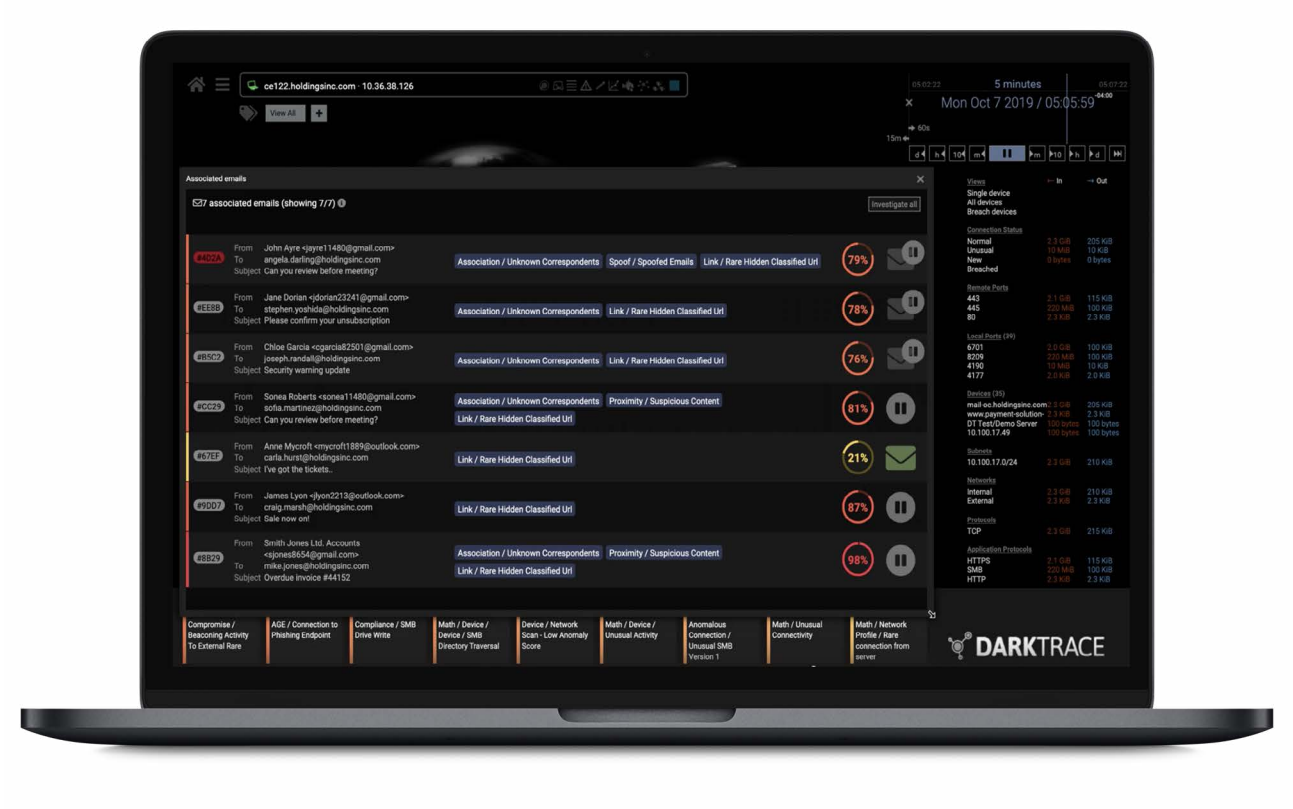

Abbildung 3: Antigena Email erkennt eine Reihe von E-Mails, die mit einer Ransomware-Kampagne in Zusammenhang stehen

Schädliche Links bei einer Kommunalbehörde neutralisiert

Eine bekannte Kommunalbehörde in den USA wurde vor kurzem Opfer eines gezielten E-Mail-Angriffs, mit dem Ransomware eingeschleust werden sollte. Antigena Email erkannte aber die Bedrohung, als sie sich entwickelte, und stellte sicher, dass keine schädlichen Payloads, Ransomware oder sonstiges heruntergeladen werden konnten.

Der Bedrohungsakteur schien Zugriff auf das Adressbuch der Behörde gehabt zu haben, da jede E-Mail sorgfältig auf den jeweiligen Empfänger zugeschnitten war und der Angriff in alphabetischer Reihenfolge von A bis Z erfolgte. Jede E-Mail erschien harmlos, aber alle Nachrichten enthielten eine schädliche Payload, die sich hinter einer als Link zu Netflix, Amazon oder anderen vertrauenswürdigen Diensten getarnten Schaltfläche verbarg.

Antigena Email war in der Lage, die verborgenen Links in Verbindung mit den normalen „Patterns of Life" der Empfänger zu analysieren. Als die erste E-Mail eintraf, erkannte Antigena sofort, dass weder der Empfänger noch eine andere Person in seiner Peer-Group noch irgendein anderer Mitarbeiter der Stadtverwaltung die Domain des Absenders jemals zuvor besucht hatte.

Die Technologie gab sofort eine Warnmeldung über die zuverlässig erkannte Bedrohung heraus und schlug eine eigenständige Sperrung jedes Links vor, der in das Netzwerk gelangte.

Da Antigena im „passiven Modus" genutzt wurde, konnte es nicht eigenständig reagieren, um die Bedrohung blitzschnell zu stoppen – der Vorfall machte aber deutlich, wie effizient die Cyber-KI und Autonomous Response sind. Während Antigena die Kampagne beim Buchstaben „A" erkannte und versuchte zu neutralisieren, wurden die Legacy-Tools des Sicherheitsteams erst bei „R" auf die Bedrohung aufmerksam.

Im „aktiven Modus" hätte Antigena den Angriff neutralisiert, noch bevor er überhaupt einen Benutzer erreicht hätte, und diese kritische Behörde vor einem weitreichenden potenziellen Ransomware-Angriff geschützt.

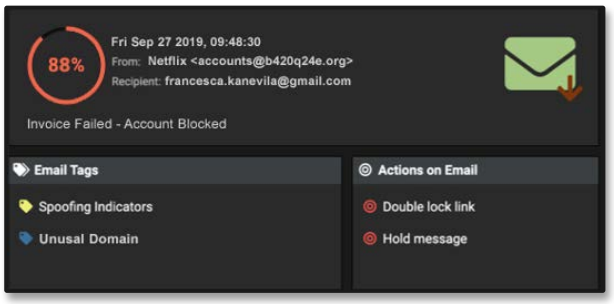

Abbildung 4: Antigena Email kennzeichnete jede E-Mail als höchst anomal

Ransomware zu persönlichem E-Mail-Konto rückverfolgt

Als Ransomware in den Posteingang eines großen Telekommunikationsunternehmens gelangte, erkannte die Cyber-KI-Plattform von Darktrace den Angriff und konnte ihn unschädlich machen, bevor auch nur eine einzige Datei verschlüsselt werden konnte.

Die Kompromittierung, mit der alles angefangen hatte, fand statt, als ein Mitarbeiter seine privaten E-Mails mit einem Firmen-Smartphone abrief. Dabei ließ er sich dazu verleiten, eine schädliche Datei herunterzuladen – die Ransomware enthielt. Sekunden später verband sich das Gerät mit einem externen Server in Tor, einem Netzwerk zur Anonymisierung von Verbindungsdaten, und die SMB-Verschlüsselungsaktivität begannen.

Innerhalb von nur neun Sekunden gab die Cyber-KI eine priorisierte Warnmeldung heraus und empfahl, das ungewöhnliche Verhalten sofort zu untersuchen.

Da sich an dem Verhalten in den darauffolgenden Sekunden nichts änderte, korrigierte die Cyber-KI ihre Einschätzung und Antigena reagierte eigenständig.

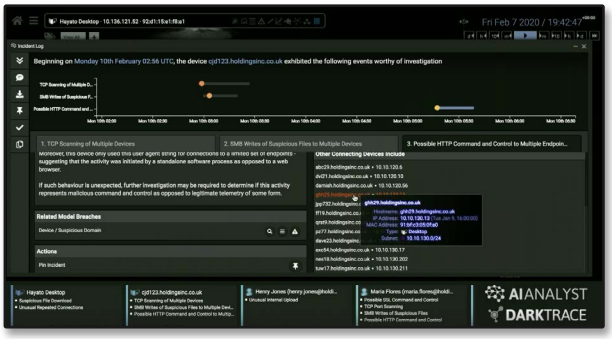

Abbildung 5: Abbildung 5: UI-Beispiel-Screenshot, der zeigt, dass die Cyber-KI ähnliche anormale SMB-Aktivitäten meldet.

Das Sicherheitsteam war bereits im Wochenende, sodass Antigena Network eingriff und den Angriff eigenständig stoppte. Dabei wurden alle Versuche unterbunden, verschlüsselte Dateien in Netzwerkfreigaben zu schreiben.

Wäre in dem Unternehmen Antigena Email installiert gewesen, wäre die Ransomware vermutlich nie heruntergeladen worden. Kein Tool ist eine Wunderwaffe – aber selbst wenn die Ransomware es über den Posteingang in das Netzwerk schaffen würde, würde Antigena Email die im Netzwerk erkannte schädliche Aktivität mit der ursprünglichen kompromittierten E-Mail in Verbindung bringen. Die Technologie würde dann ähnlich gefährliche E-Mails aus den Posteingängen weiterer Mitarbeiter holen.

Nur mit dem vertieften, sukzessive angereicherten Wissen über die DNA Ihres Unternehmens können Antigena Email und die Darktrace Cyber-KI-Plattform Bedrohungen in Echtzeit erkennen und auf komplexe Ransomware-Angriffe reagieren.

Das Enterprise Immune System im Zusammenspiel mit dem Cyber AI Analyst: voller Einblick eines Ransomware-Vorfalls

Die selbstlernende Cyber-KI ermöglicht es dem Enterprise Immune System, kaum merkliche Veränderungen der Aktivität zu erkennen, die auf sich entwickelnde Ransomware hindeuten – ohne dass Daten zu bekannten Bedrohungen vorliegen müssen. Mit seinem individuellen und sich sukzessive weiterentwickelnden Verständnis der normalen „Patterns of Life" in Ihrer Infrastruktur spürt das Enterprise Immune System selbst subtile Abweichungen auf und sorgt dafür, dass Ihr Sicherheitsteam sofort über einen sich ultraschnell ausbreitenden Angriff informiert wird.

Der Cyber AI Analyst, eine Kernkomponente des Immunsystem-Ansatzes, untersucht automatisch jedes erkannte anormale Ereignis. Bei Ransomware-Kampagnen spürt er jedes betroffene Gerät und die Quelle der Infektion auf und stellt alle kontextbezogenen Informationen bereit, damit Sie sofort reagieren können.

Der Cyber AI Analyst reduziert die Auswertungszeit erwiesenermaßen um 92 % und kann sich entwickelnde Ransomware zuverlässig als kritische Bedrohung einstufen, die einen menschlichen Eingriff erforderlich macht. Ein KI-generierter „Incident Report" stellt einen interaktiven Zeitstrahl, eine präzise Zusammenfassung der Kampagne sowie detaillierte Daten zu dem betroffenen Gerät oder Benutzerverhalten bereit.

Diese Berichte werden im Zuge der sich entwickelnden Bedrohung eigenständig aktualisiert und sind sehr wichtig für die Sicherheitsexperten, um die Situation richtig einschätzen zu können, und auch für nicht-technische Beteiligte.

Expertenanalyse eines Dharma-Angriffs

Als ein britisches Unternehmen mit einer gezielten Dharma Ransomware-Kampagne angegriffen wurde, spielte das Enterprise Immune System eine entscheidende Rolle bei der Erkennung der Bedrohung – und demonstrierte, wie leistungsstark der Cyber AI Analyst in der Erkennung und Meldung eines sich entwickelnden Angriffs ist.

Die Cyber-KI erkannte sofort das Risiko, als ein RDP-Server eine Vielzahl von Verbindungsanfragen von ungewöhnlichen IP-Adressen erhielt. Bei der späteren Untersuchung stellte sich heraus, dass die RDP-Zugangsdaten vermutlich irgendwann vor dem Angriff kompromittiert worden waren.

Am darauffolgenden Tag beobachtete die Cyber-KI, dass der Bedrohungsakteur das SMB-Protokoll Version 1 missbrauchte. Dann wurde eine ungewöhnliche externe Verbindung zu einer ungewöhnlichen marokkanischen IP-Adresse und eine fehlgeschlagene SMB-Sitzung über die IP-Adresse über einen sehr ungewöhnlichen Port beobachtet. Zwei Stunden später richtete der Bedrohungsakteur stärkere Command & Control-Kanäle ein, die sich mit ungewöhnlichen Zielen in Indien, China und Italien verbanden.

Die Cyber-KI stellte des Weiteren interne Auskundschaftung fest, als eingehende RDP-Verbindungen anfingen, das Netzwerk zu scannen, und ein großes Datenvolumen zu einer ungewöhnlichen IP-Adresse in Panama übertragen wurde.

Zum Schluss wurde die Dharma-Payload ausgeführt. Parallel zu der Verschlüsselungsaktivität versuchte die Ransomware, weitere Rechner zu infizieren, und nutzte dafür die Zugangsdaten eines Administrators, die bei der internen Auskundschaftung abgegriffen wurden. Als die Verschlüsselung begann, zogen die IT-Mitarbeiter den Stecker am RDP-Server.

Auch wenn das Team es zunächst versäumt hatte, auf die Warnmeldungen von Darktrace zu reagieren, war die Cyber-KI dennoch in der Lage, jeden einzelnen Schritt dieses komplexen Angriffs zu identifizieren, sodass das Team effizient reagieren und weiteren Schaden verhindern konnte.

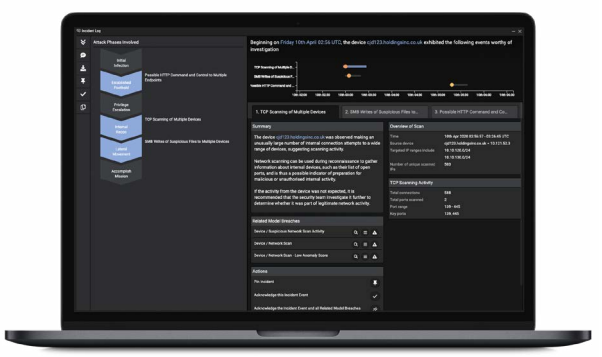

Abbildung 6: UI-Beispiel-Screenshot, der zeigt, dass der Cyber AI Analyst einen Ransomware-Angriff meldet.

Das Enterprise Immune System erkannte jeden Schritt dieser Kampagne basierend auf dem anormalen Verhalten im Kontext des Unternehmens – und war nicht auf Abgleiche mit Bedrohungssignaturen angewiesen.

Bei einem Angriff wie diesem, der über einen längeren Zeitraum ausgeführt wird und bei dem es nur isolierte Hinweise auf die schädliche Aktivität gibt, spielt der Cyber AI Analyst eine entscheidende Rolle für die Einschätzung und Kommunikation der Art und des Ausmaßes der Bedrohung.

Der Cyber AI Analyst stellte dem Team einen Incident Report bereit, mit einem Überblick des Ransomware-Angriffs und detaillierten Informationen zu jeder Phase des Vorfalls.

Das Industrial Immune System: Schutz operativer Systeme vor Ransomware

Wenn es um den Schutz vor Ransomware geht, ist das Industrial Immune System die leistungsstärkste Lösung für Sicherheit in modernen operativen Umgebungen. Vor allem vor dem Hintergrund von Bedrohungen wie der EKANS Ransomware – die erste bekannte Ransomware, die gezielt ICS-spezifische Maschinen angreift – ist es entscheidend, Sicherheitstools einzusetzen, die sich kontinuierlich an OT-Umgebungen anpassen und diese Systeme auch vor Zero-Day-Angriffen schützen.

Viele Ransomware-Kampagnen richten sich auch gegen Industrieumgebungen und nutzen Sicherheitslücken in der IT-Infrastruktur. Indirekte Kompromittierung ist eine zusätzliche Bedrohung, da OT-Systeme bei einem IT-fokussierten Angriff Kollateralschaden nehmen können. Angesichts des potenziellen Schadens für kritische Infrastruktur ist es immer dringender erforderlich, Sicherheitstechnologie einzusetzen, die Muster in verteilter Infrastruktur in Beziehung setzen kann.

Selbstlernende KI ermöglicht es dem Industrial Immune System, selbst so komplexe Bedrohungen wie neuartige Ransomware eindeutig zu identifizieren. Die Technologie ist in der Lage, die normalen Verhaltensmuster – die „Patterns of Life" – völlig unterschiedlicher Technologien und Bereitstellungsformen zu lernen, von jahrzehntealten PLCs bis hin zu verteilten Sensoren und IIoT.

Darüber hinaus erkennt die Cyber-KI dank ihrer zentralen Einblicke den Zusammenhang zwischen schädlicher Aktivität in IT-Systemen und Verhalten in OT-Systemen – sie ist so in einzigartiger Weise in der Lage, Bedrohungen zu stoppen, die sich zwischen den traditionellen Sicherheitssilos bewegen.

Ransomware in einer Ölraffinerie gefunden

Bei einer integrierten Ölraffinerie, die gleichzeitig Lieferant ist, spielte das Industrial Immune System von Darktrace eine entscheidende Rolle bei der Abwehr eines Ransomware-Angriffs, der im Unternehmensnetzwerk seinen Ursprung hatte.

Die Cyber-KI erkannte die ersten Hinweise auf eine Ransomware-Infektion auf einem Desktop-Gerät im Netzwerk. Das Gerät schrieb nicht nur seine eigenen Dateien mit Lösegeldforderungen, sondern baute zudem über einen internen Proxyserver Verbindungen zu ungewöhnlichen externen Zielen auf und lud dann potenziell schädliche Dateien herunter – Aktivitäten, die Darktrace aufgrund seines granularen Wissens über die normalen Verhaltensmuster im Unternehmen erkennen und in Beziehung setzen konnte.

Das Gerät nahm im weiteren Verlauf eine Reihe von SMB-Verzeichnisabfragen vor – eine weitere Aktivität, die die Cyber-KI als Abweichung von ihrem Verständnis des Verhaltens des betreffenden Geräts erkannte.

Das Industrial Immune System identifizierte diese Aktivität als wahrscheinliche Ransomware und warnte das Sicherheitsteam des Kunden, bevor sich die Infektion in den OT-Umgebungen ausbreiten konnte.

Dank der Fähigkeit der Cyber-KI, Muster aus der gesamten vielfältigen Infrastruktur in Beziehung zu setzen, konnte das industrielle System vor diesem sich ultraschnell ausbreitenden Angriff geschützt werden.

Abbildung 7: UI-Beispiel-Screenshot zeigt ein Gerät, das mit von der Cyber-KI erkannter Ransomware infiziert ist.