Outpost24

Threat Compass

Vorrauschauendes Cyber Risiko Management

Die Cyber Bedrohungslage nimmt kontinuierlich zu. Angreifer nutzen immer ausgefeiltere Techniken, um Unternehmen zu infiltrieren. Alle Organisationen, die online tätig sind, verfügen über Daten, die für Cyberkriminelle wertvoll sind - von Finanztransaktionen über personenbezogene Daten von Kunden bis hin zu vertraulichen Unternehmensdaten und geistigem Eigentum. Ein Angriff auf diese Daten kann katastrophale Auswirkungen auf das operative Geschäft haben, den Ruf schädigen und Strafen für die Nichteinhaltung von Vorschriften nach sich ziehen.

Ihre Organisation ist gefährdet, und statische oder reaktive Cyberabwehr ist nicht länger ausreichend. Outpost24 verfolgen einen proaktiven Ansatz bei der Cyberabwehr, indem sie gezielte, umsetzbare Informationen über Cyberbedrohungen bereitstellen, um Cyberrisiken zu minimieren: Threat Compass. Zielgerichtete Bedrohungsinformationen sparen Zeit und ermöglichen eine optimale Nutzung der vorhandenen Ressourcen, indem die Erkennung von Bedrohungen, die Reaktion auf Vorfälle und die Analyse beschleunigt werden.

Threat Compass verwendet hochentwickelte Algorithmen, um automatisch aussagekräftige Informationen über Cyberbedrohungen aus offenen, geschlossenen und privaten Quellen, einschließlich Malware-Botnets, zu liefern. Dies erleichtert die Identifizierung und Verwaltung von realen Bedrohungen, die auf Ihr Unternehmen abzielen - und sorgt für eine schnellere Entscheidungsfindung sowie eine verbesserte Effizienz.

Threat Compass deckt das gesamte Spektrum an möglichen Bedrohungen auf dem Markt ab, und die modulare Pay-as-you-need-Architektur bedeutet, dass Sie nur die Informationen erwerben müssen, die für Ihr Unternehmen relevant sind.

Jedes einzelne Modul wird von unserem erstklassigen internen Analysten-Team bereitgestellt. Setzen Sie Bedrohungen in den richtigen Kontext, um mögliche Angriffe aufzudecken, Ihre Assets zu verteidigen und die Strategien der Angreifer zu verstehen, noch bevor diese aktiv werden - dank der Pay-as-you-need-Architektur sind unsere Informationen schlank, kostengünstig und skalierbar.

Die automatisierte Bereitstellung der Informationen ermöglicht es uns, den Zeit- und Kostenaufwand für Analysten zu minimieren und Informationen zu liefern, die für alle Ebenen von Nutzen und Bedeutung sind: Analysten wollen wissen, wie es zu einem Sicherheitsvorfall gekommen ist, während die Unternehmensleitung sicherstellen möchte, dass sich ein solcher Vorfall nicht wiederholt. Threat Compass bietet Antworten auf beide Fragestellungen!

Die nahtlose Integration erfolgt über eine umfassende API und flexible Plugins, so dass die zielgerichteten Informationen von Threat Compass sofort für Ihre Sicherheitssysteme und -teams verfügbar sind. Die einfache Einrichtung der Cloud-Plattform bedeutet, dass Sie sofort einen wertvollen Überblick über die Situation gewinnen.

Threat Compass ist innerhalb von Minuten und nicht erst nach Monaten einsatzbereit, hat extrem niedrige Betriebskosten sowie einen geringen Personalbedarf für die Administration. Noch besser: Sie brauchen keinen Experten, um die bereitgestellten Informationen zu verstehen. Threat Compass unterstützt Ihre Jagd auf Bedrohungen außerhalb Ihres Unternehmensnetzwerks und liefert die nötigen Informationen, um bösartige Aktivitäten, Vorfälle und Akteure zu erkennen und zu überwachen, bevor sie innerhalb Ihrer Infrastruktur Schaden anrichten können.

Threat Compass sammelt, analysiert, korreliert und liefert automatisch aufbereitete Bedrohungsinformationen aus einer Vielzahl von Kategorien, die Ihr Unternehmen beeinträchtigen könnten. Ob es um die Identifizierung von Botnetzen und Command & Control-Servern geht oder um Varianten von Malware, um das Aufspüren gestohlener Kreditkarten und kompromittierter Zugangsdaten, bis hin zum Aufspüren bösartiger mobiler Apps, hacktivistischer Aktivitäten und Phishing-Kampagnen, die auf Ihr Unternehmen abzielen.

Wir begleiten Sie durch die moderne Bedrohungslandschaft

- Wer hat es auf Ihr Unternehmen abgesehen, und von wo?
- Wissen Sie, wie es um die Präsenz Ihrer Organisation im Dark Web bestellt ist?
- Wie wurde Ihr Unternehmensnetzwerk kompromittiert?
- Wer gibt sich als Ihre Marke, Geschäftsführung oder VIPs aus?
- Wurden sensible Informationen veröffentlicht?
- Wurden Anmeldedaten kompromittiert, werden sie für Betrugszwecke verwendet?
- Wissen Sie, welche Konsequenzen Sie im Falle einer Kompromittierung zu erwarten haben?

Umfassende, modulare IT-Sicherheit

Jedes Threat Compass-Modul kann einzeln erworben und verwendet werden. Sie brauchen nur die Module zu lizenzieren, die die für Ihr Unternehmen relevanten Bedrohungsinformationen liefern.

Bedrohungszusammenhang

Threat Context versorgt Sicherheitsteams mit ständig aktualisierten und intuitiven Informationen über Threat-Actors, Kampagnen, IOCs, Malware, Angriffsmuster, Tools, Signaturen und CVEs. Eine Datenbank mit mehr als 200 Millionen Einträgen bietet anschauliche Zusammenhänge, sodass Analysten vor, während und nach einem Angriff schnell angereicherte, kontextualisierte Informationen sammeln können. Wir haben mehr als zehn Jahre historischer Bedrohungsdaten gesammelt und zur Verfügung gestellt, die ständig aktualisiert werden und unseren Kunden die umfangreichste Bedrohungssammlung bieten.

Dark Web

Schärfen Sie Ihr Bewusstsein für die Vorgänge im Verborgenen, beobachten Sie böswillige Vorgänge, die auf Ihr Unternehmen abzielen, und verhindern Sie proaktiv zukünftige Angriffe. Verschaffen Sie sich einen Vorteil, indem Sie Angreifern in die Karten schauen: Seien Sie besser informiert, wenn Kriminelle Ihr Unternehmen ins Visier nehmen; bereiten Sie proaktiv Gegenmaßnahmen vor und spüren Sie gestohlene Anmeldedaten sowie Assets in Echtzeit auf.

Zugangsinformationen

Finden Sie brauchbare Informationen über geleakte, gestohlene und verkaufte Zugangsdaten. Wir spüren sie zusammen mit Informationen über relevante Malware, die zum Diebstahl der Daten verwendet wurde, im Open, Deep und Dark Web in Echtzeit auf. Die Sinkholes, Honeypots, Crawler und Sensoren von Outpost24 suchen kontinuierlich nach Ihren gestohlenen Zugangsdaten. So eliminieren Sie ernstzunehmende Angriffsvektoren und illegale Aktivitäten innerhalb von Minuten und nicht erst nach Monaten.

Datenlecks

Entdecken Sie, ob sensible Dokumente und Quellcode Ihres Unternehmens im Internet, Deep Web oder in P2P-Netzwerken absichtlich oder unabsichtlich an die Öffentlichkeit gelangt sind, z. B. durch die gemeinsame Nutzung interner Dokumente mit schlecht gesicherten Filesharing-Anbietern.

Kreditkarteninformationen

Wenn man tief genug gräbt, kann man online alle möglichen Kreditkartendaten finden. Dieses Modul kann den Schaden durch Diebstahl und Betrug mit Kreditkarten drastisch reduzieren.

Wir rufen gestohlene Kreditkarteninformationen ab und stellen relevante Information zur Verfügung, um Unternehmen bei der Schadensbegrenzung zu unterstützen.

Hacktivism

Überwachen Sie globale Hacktivism-Aktivitäten in sozialen Netzwerken und im Open und Dark Web, die Ihre Infrastruktur bedrohen können. Mithilfe eines fortschrittlichen Frühwarnsystems und eines aktiven Geolokators generiert das Modul gezielte Bedrohungsinformationen, um sich gegen potenzielle Angriffsvektoren zu schützen.

Mobile Apps

Bösartige und illegale Anwendungen verstecken sich auf nicht-offiziellen Marktplätzen, ködern Ihre Kunden und stehlen sogar deren Daten.

Unser Modul ist darauf spezialisiert, Anwendungen aufzuspüren, die eine angebliche Verbindung zu Ihrem Unternehmen vorgeben oder Unternehmensressourcen unbefugt nutzen. So schützen Sie Ihre Marke und Ihren Ruf.

Social Media

Überwachen Sie den digitalen Fußabdruck Ihrer Organisation in sozialen Netzwerken und Suchmaschinen. Finden Sie Websites, die nicht berechtigt sind, Ihre Marken, Logos, Assets und vieles mehr zu verwenden, oder gar Partnerschaften mit Ihrer Organisation anzugeben, so dass Sie proaktiv Maßnahmen ergreifen können, um diese zu unterbinden.

Schutz Ihrer Domains

Betrügerische Domains stellen ein Risiko für Ihr Unternehmen und Ihre Endkunden dar. Solche Domains haben oft die Absicht, Informationen zu stehlen oder Ihre Marke zu schädigen. Bekämpfen Sie Phishing und Cybersquatting, indem Sie Angriffe proaktiv erkennen und Gegenmaßnahmen ergreifen.

Jetzt Beratungstermin vereinbaren

Werden Sie Partner

Individuell anpassbar

Threat Compass bietet einen zentralen Kontrollpunkt für automatisierte, operative, taktische und strategische Bedrohungsinformationen.

Sammlung

Outpost24 automatisiert die Sammlung von Bedrohungsinformationen aus verschiedenen Quellen und in verschiedenen Formaten.

Korrelation & Anreichern

Threat Compass bietet eine leistungsstarke Kategorisierung von Informationen, Honey-Client-Direct-Side-Validierung sowie Sandbox-Analysen und -Bewertungen.

Wir untersuchen auch Daten, die von Drittanbietern gesammelt werden, um gemeinsame Angriffsvektoren und Akteure zu identifizieren.

Umsetzbare Ergebnisse

Die leistungsstarken Visualisierungsfunktionen von Outpost24 stellen zielgerichtete, verwertbare Bedrohungsinformationen intuitiv dar. Nutzen Sie die Informationen, um Ihre eigenen YARA-Regeln zu erstellen, sich einen taktischen Vorteil zu verschaffen und strategische Reaktionsmöglichkeiten auf Cyberbedrohungen zu schaffen.

Integration von Bedrohungsinformationen

Plugins sind für die gängigsten SIEMs, SOAR-Plattformen und TIPs verfügbar. Outpost24 unterstützt STIX/TAXII für den einfachen Informationsaustausch zwischen verschiedenen Datenformaten.

Gemeinsam stark

Teilen Sie relevante Informationen mit internen Gruppen und vertrauenswürdigen Partnern.

Ermöglichen Sie es einem einzelnen Benutzer, Bedrohungsdaten von spezifischem Interesse zu sammeln und relevante, zeitnahe und genaue Indikatoren für die Gefährdung durch neue oder laufende Cyberangriffe weiterzugeben, um Verletzungen zu vermeiden oder den Schaden eines schweren Angriffs zu minimieren.

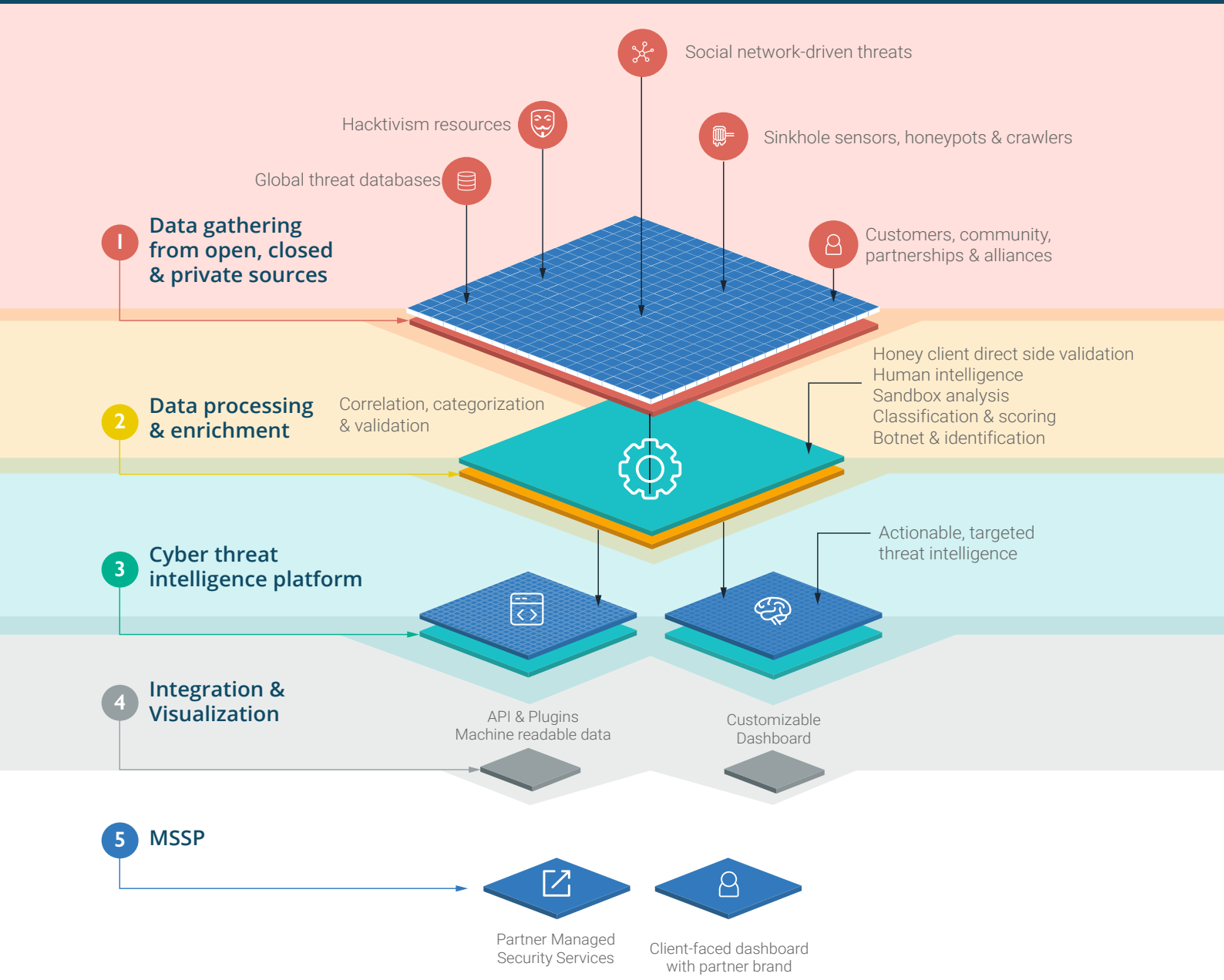
Schnell & flexibel reagieren

Durch die Automatisierung der Sammlung und Präsentation gezielter Bedrohungsinformationen erhalten Sie einen besseren Einblick in die Bedrohungslage und verkürzen die Reaktionszeit auf Zwischenfälle.

Big Data-Analysefunktionen liefern schnell verwertbare Informationen mit minimalen Falschmeldungen in einer einzigen Dashboard-Ansicht - mit Hintergrundinformationen und zugrunde liegenden Details - für eine schnellere Entscheidungsfindung.

Effiziente Nutzung von Ressourcen

Eliminieren Sie die lästige Auswertung von Tausenden von Warnmeldungen und ermöglichen Sie es Ihrem Team, sich mit ausgefeilten Analysefunktionen auf spezifische Bedrohungen zu konzentrieren.



Strategische Antworten erarbeiten

Threat Compass ermöglicht es Ihnen, eine Liste bösartiger IP-Adressen zu erstellen, die in interne und periphere Sicherheitskontrollen integriert werden können. Es identifiziert kompromittierte Konten, die für den Zugriff auf Unternehmensressourcen verwendet werden, und gewährleistet eine genauere Prüfung und Kontrolle von mobilen Anwendungen und vermeintlichen Zusammenhängen. Mit Threat Compass können Benutzer die Kill Chain verstehen und die Effizienz der internen Sicherheit maximieren.

Schnell bereitgestellt

Die modulare Architektur von Threat Compass ist einfach zu implementieren und liefert sofort aussagekräftige Ergebnisse. Die Cloud-basierte Lösung macht die Installation von Hardware oder Software überflüssig. Flexible Lizenzierungsoptionen erleichtern die Bereitstellung eines maßgeschneiderten Schutzes für das gesamte Unternehmen und für Abläufe an unterschiedlichen Standorten. Setzen Sie richtlinienkonforme Kontrollen genau dort ein, wo sie benötigt werden, und sehen Sie die Resultate innerhalb von Minuten, nicht Monaten.

Über Outpost24

Als einer der größten europäischen Anbieter für Lösungen im Bereich Cyber-Risikomanagement mit Team in Deutschland und starken Wurzeln in der Ethical Hacking Community leisten wir Pionierarbeit

im Cyber-Risikomanagement.

Über 2.500 Kunden in mehr als 65 Ländern vertrauen auf Lösungen der Unternehmen der Outpost24 Gruppe, um Schwachstellen zu identifizieren, Zugangsdaten sicher zu gestalten, externe und interne

Bedrohungen zu überwachen sowie die Angriffsflächen schnell und zuverlässig zu reduzieren.

outpost24.com/de

info@outpost24.com

twitter.com/outpost24

linkedin.com/outpost24