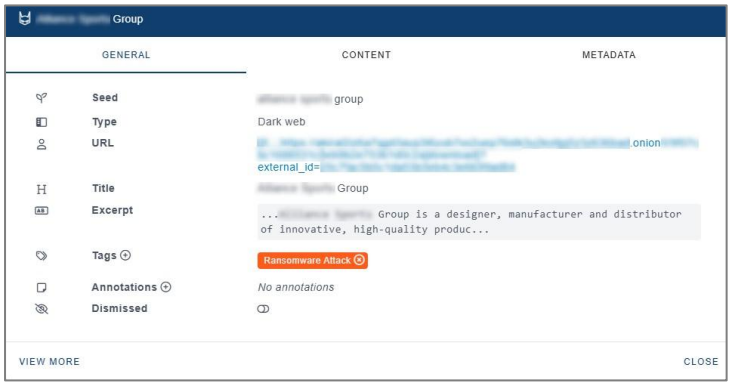
Digital Risk Protection

Mit einem intelligenten Schutz vor Cyberbedrohungen für Ihr Betriebsvermögen können Sie schadhaften Angriffen vorbeugen.

Die heutige Bedrohungslandschaft gestaltet sich immer schnelllebiger. Akteure mit böswilliger Absicht nutzen immer ausgefeiltere Techniken für Angriffe auf Organisationen. **Alle online agierenden Organisationen verfügen über Daten, die für Cyberkriminelle überaus wertvoll sind, seien es Aufzeichnungen über Finanzgeschäfte oder personenbezogene Kundendaten oder über vertrauliches Unternehmensvermögen oder industrielles geistiges Eigentum**. Eine Datenschutzverletzung kann verheerende geschäftliche Auswirkungen, Reputationsschäden und Compliance-Strafen nach sich ziehen.

Mit der Lösung **Outpost24 Digital Risk Protection (DRP)** können Sie externe Bedrohungen für Ihr Geschäft erkennen und abwehren. DRP deckt die gängigsten marktüblichen Bedrohungen ab und liefert umsetzbare Einblicke zur **Maximierung des Reaktionsvermögens auf Datenschutzvorfälle**. Dank der **einfachen Einrichtung** der Cloud-Plattform verschaffen Sie sich umgehend und fortwährend ein **wertvolles Situationsbewusstsein**. Mit einer **zentralen Schaltstelle** befähigen Sie Ihre Sicherheitsteams zu einer automatisierten, operativen, taktischen und strategischen Bedrohungsintelligenz.

Geleakte Anmeldedaten



Aufspüren von Ransomware im Dark Web

Wichtige Produktmerkmale

- **+13 Jahre** historische Daten zu Cyberbedrohungen
- Datengewinnung aus **offenen, geschlossenen und privaten Quellen**
- Unternehmenseigenes **„Threat Intelligence"-Forschungsteam** für die Bereitstellung von Terabyte an verifizierten Daten
- „Big Data"-Analyse mit **Kontext** und den zugrunde liegenden **Details**
- Verfügbare Plug-ins für **SIEMs, SOAR und TIPs**
- Flexibles Geschäftsmodell für verschiedene **Partnerschaften**, einschließlich MSSP-Programme
- Anhaltende Partnerschaft mit **Cyber Threat Alliance (CTA)**

Individuelle Begleitung durch die Bedrohungslandschaft

- Wer hat es auf Ihre Organisation abgesehen und von **welchem Standort** aus erfolgt der Angriff?
- Wissen Sie über Ihre Präsenz im **Dark Web** Bescheid?
- Wie konnte Ihr Unternehmensnetzwerk **kompromittiert** werden?
- Wer gibt sich für Ihre **Marke** oder Ihre **VIP**s aus?
- Wurden sensible Informationen **geleak**t?
- Wurden **Anmeldedaten** kompromittiert, werden diese für Betrugsversuche verwendet?
- Kennen Sie Ihre **Compliance-Pflichten** im Falle einer Datenschutzverletzung

Über Digital Risk Protection

Dark Web

Verschaffen Sie sich einen besseren Überblick über die Geschehnisse im Untergrund, überwachen Sie bösartige Aktivitäten, die auf Ihre Organisation abzielen, und verhindern Sie proaktiv zukünftige Angriffe. Verschaffen Sie sich durch Insider-Einblicke den entscheidenden Vorteil: erlangen Sie eingehendere Informationen über Kriminelle, die auf Ihre Organisation abzielen; bereiten Sie proaktiv Gegenmaßnahmen vor.

Anmeldedaten

Entdecken Sie umsetzbare Einblicke zu geleakten, gestohlenen und verkauften Anmeldedaten von Benutzern. Wir machen diese Details in Echtzeit im offenen, Deep und Dark Web ausfindig, einschließlich von Informationen über die betreffende Malware, die für den Datendiebstahl verwendet wurde. Die Sinkholes, Honeypots, Crawler und Sensoren von Outpost24 sind kontinuierlich auf der Suche nach Ihren gestohlenen Anmeldedaten – aufgrund von Datenleaks, in Foren und in Echtzeit aufgrund von zielgerichteten Malware-Angriffen. Hierdurch können ernstzunehmende Angriffsvektoren und betrügerische Handlungen in Minutenschnelle anstelle von Monaten beseitigt werden.

Datenleak

Finden Sie heraus, ob sensible Dokumente und Quellcode Ihrer Organisation versehentlich oder bewusst im Internet, Deep Web oder in P2P-Netzwerken geleakt wurde (z. B. bei internen Dokumenten, die über Filesharing-Anbieter mit unzureichendem Schutz verbreitet wurden).

Soziale Medien

Überwachen und überprüfen Sie den digitalen Fußabdruck Ihrer Organisation in Web 2.0-Repositorys wie Blogs, Foren, Websites und sozialen Netzwerken. Machen Sie Websites ausfindig, die Ihre Marken, Ihre Logos und Ihr Firmeneigentum usw. in unbefugter Weise verwenden oder die sich als Partner Ihrer Organisation ausgeben, um proaktive Maßnahmen für deren Stilllegung zu ergreifen.

KrakenLabs Threat Intelligence Team

Wir sind auf die Bereitstellung kundenspezifischer, profunder Bedrohungsanalysen und Berichte spezialisiert, die speziell auf Ihre Organisation zugeschnitten sind. Dank unserer Services erlangen Sie umsetzbare Einblicke in einem benutzerfreundlichen Format über die neuesten Cyberbedrohungsaktivitäten für Ihre Organisation, einschließlich von IOCs, Schwachstellen und TTPs. Wir unterstützen Sie zudem durch einen fachkompetenten und persönlichen Service bei der Ergreifung proaktiver Maßnahmen zum Schutz Ihrer Organisation – einschließlich von Bedrohungen aus dem Dark Web, der Analyse von Datenschutzverletzungen und Abschätzungen mittels OSINT, damit Ihre Organisation Cyberkriminellen stets einen Schritt voraus bleibt. Threat Intelligence ist Teil der Risikomanagement-Anforderungen für die DORA-Compliance, so dass KrakenLabs auch diesen Bedarf erfüllt.

MSSP WERDEN

DEMO ANFORDERN

Über Outpost24

Die Outpost24-Gruppe ist ein Pionier im Bereich des Cyberrisikomanagements mittels Schwachstellenmanagement, Testung der Anwendungssicherheit, Bedrohungsintelligenz und Zugriffsverwaltung – in einem einzigen Lösungspaket. Über 2.500 Kunden in mehr als 65 Ländern vertrauen bei der Identifizierung von Schwachstellen, Überwachung externer Bedrohungen sowie Reduzierung der Angriffsfläche auf die schnelle und sichere ganzheitliche Lösung von Outpost24. Outpost24 wird über unsere Cloud-Plattform mit leistungsstarker Automatisierung und Unterstützung durch unsere Experten für Cybersicherheit bereitgestellt, um Organisationen durch die Fokussierung auf die wesentlichen Cyberrisiken noch erfolgreicher zu machen.