

# External Risk Management

## Infinity ERM von Check Point

Externe Cyberrisiken entstehen ausserhalb der direkten Kontrolle eines Unternehmens – auf öffentlich zugänglichen Systemen, in der Lieferkette oder im Open, Deep und Dark Web. External Risk Management setzt genau hier an.

### HERAUSFORDERUNGEN

#### Fehlende Sichtbarkeit

Viele Unternehmen wissen nicht genau, welche Assets, Services oder Daten tatsächlich öffentlich erreichbar sind. Neue Systeme entstehen oft unbemerkt – etwa durch Schatten-IT, Fusionen, Übernahmen oder Aktivitäten von Drittanbietern – und entziehen sich so der Sicherheitskontrolle.

#### Fragmentierte Bedrohungsinformationen

Bedrohungsinformationen aus Open, Deep und Dark Web liegen meist unvollständig vor. Ohne zentralen Kontext und Priorisierung verlieren Security-Teams wertvolle Zeit damit, aus einer Flut von Daten die relevanten Risiken zu filtern. Gerade bei Angriffen zählt jedoch jede Stunde: Phishing-Domains, geleakte Zugangsdaten oder Zero-Day-Exposures können innerhalb kürzester Zeit ausgenutzt werden.

#### Abhängigkeiten & Supply-Chain-Risiken

Kompromittierte Partner-Systeme, Datenlecks oder Fehlkonfigurationen können sich unmittelbar auf das eigene Unternehmen auswirken. Viele Organisationen haben bislang keine systematische Möglichkeit, solche Supply-Chain-Risiken zu überwachen.

#### Hohe Kosten und Aufwand

Nicht zuletzt verursachen der Einsatz mehrerer Einzellösungen für Angriffsflächenmanagement, Threat Intelligence, Markenschutz und Third-Party-Monitoring hohe Kosten, komplexe Integrationsprojekte und potenzielle Sicherheitslücken.

### WIE HILFT ERM

ERM begegnet diesen Herausforderungen, indem es alle relevanten externen Risiken auf einer zentralen Plattform sichtbar macht, die tatsächliche Ausnutzbarkeit von Schwachstellen überprüft, Bedrohungen frühzeitig erkennt und Gegenmassnahmen wie Takedowns automatisiert einleitet. Dabei werden auch Drittparteien kontinuierlich überwacht.

#### Vorteile

- Kontinuierliche Überwachung, Erkennung, Priorisierung und Abwehr eines breiten Spektrums externer Cyberrisiken.
- Volle Sichtbarkeit auf Schwachstellen in Ihrer Angriffsfläche sowie auf relevante Bedrohungen im Deep und Dark Web.
- Schutz für Unternehmen, Marken, Domains und Führungskräfte vor böswilligen Identitäts- und Markenmissbrauchsangriffen.
- Maximale Effizienz des Security-Budgets durch eine benutzerfreundliche Low-Touch-Plattform, optimiert für Einfachheit und Effektivität.
- Nahtlose Integration von Alerts in der Plattform oder in Ihre bestehende Sicherheitsumgebung über Integrationen und REST-APIs.

## Infinity External Risk Management



Die Lösung für External Risk Management von Check Point kombiniert die kontinuierliche Erfassung der externen Angriffsfläche mit der automatisierten Auswertung grosser Datenmengen aus Open, Deep und Dark Web. Dadurch entsteht ein umfassendes Bild über potenzielle Gefahrenquellen ausserhalb der Unternehmensgrenzen.

Ein internationales Expertenteam mit langjähriger operativer Erfahrung unterstützt Unternehmen bei der schnellen Identifikation, Analyse und Eindämmung relevanter Bedrohungen, bevor diese Auswirkungen auf den Geschäftsbetrieb haben.

Zu den adressierten Risiken zählen unter anderem Schwachstellen in exponierten Systemen, Fehlkonfigurationen, Phishing und Identitätsmissbrauch, Schadsoftware, gestohlene Zugangsdaten, Datenlecks, Betrug sowie Risiken aus der Lieferkette. Weltweit setzen zahlreiche Organisationen, darunter auch Fortune-500-Unternehmen aus verschiedenen Branchen, auf diesen Ansatz, um externe Gefahren frühzeitig zu erkennen und kontrollierbar zu machen.



**ensec** unterstützt Sie und ist Ihr Partner für sämtliche Information Security Fragen - natürlich auch im Bereich (External) Risk Management.

Als einziger deutschschweizer ELITE Check Point Partner verfügen wir über maximale Expertise.