



CHECK POINT™

Cyberint
A Check Point Company

Transforming Security Operations With External Risk Management

Bernd Knippers

Solutions Architect ERM

Check Point Software

Organizations face critical security challenges every day

External threats are responsible for 83% of breaches

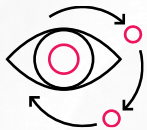


Stolen credentials

are used as an attack entry point to organizations



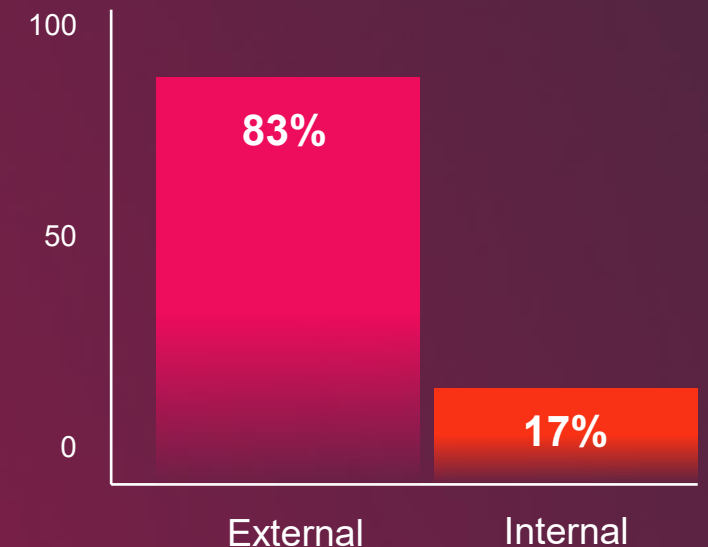
Brand abusing websites and Social Impersonation
causes financial and reputational damage



Limited visibility into external digital footprint
makes it challenging to detect and mitigate vulnerabilities

**External Threats
are the # 1 Risk**

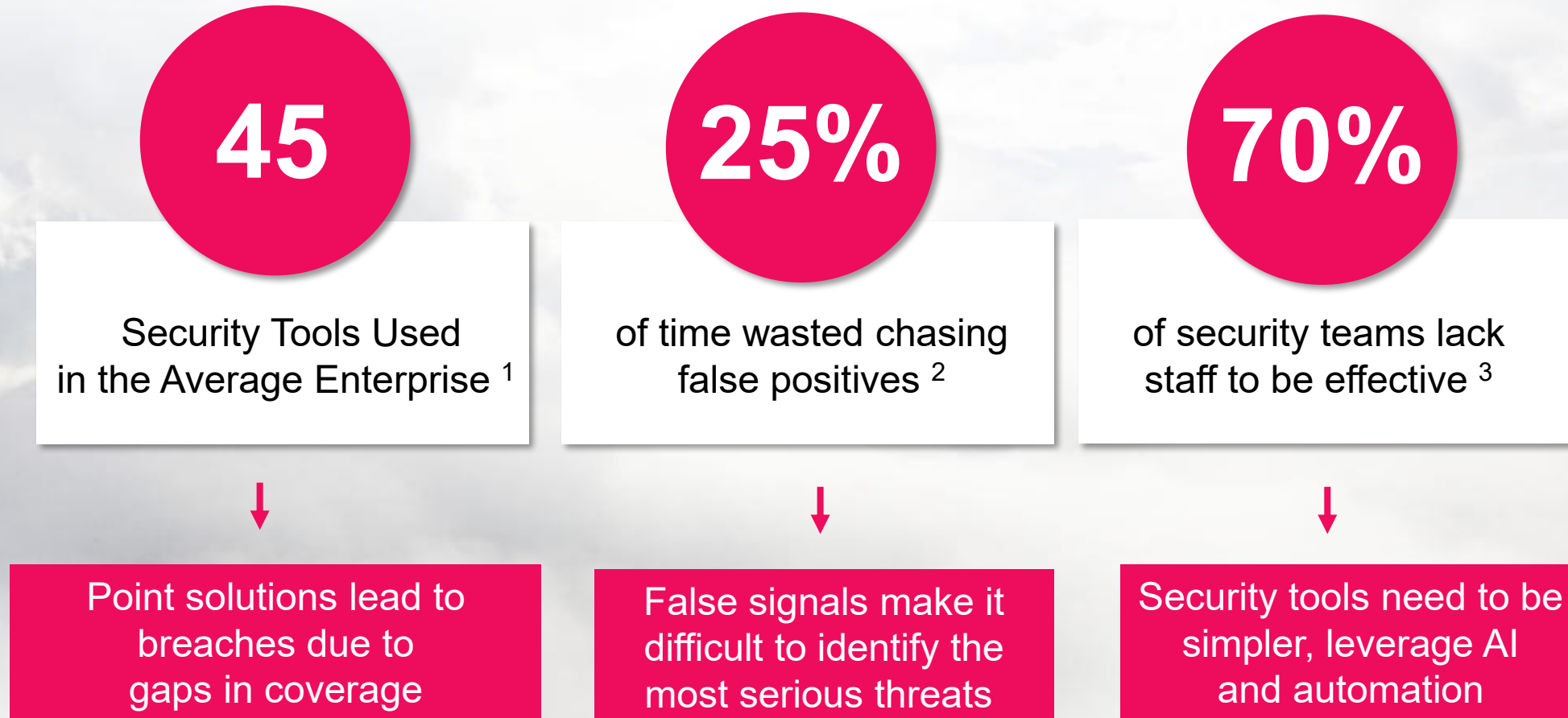
SOURCE OF DATA BREACHES (%)



Verizon Data Breach Investigations Report 2023 (source)

Security Operations Team Challenges

Enterprises Need a Comprehensive Risk Management Platform



1. IBM Security Cyber Resilient Organization Report 2020 (source)

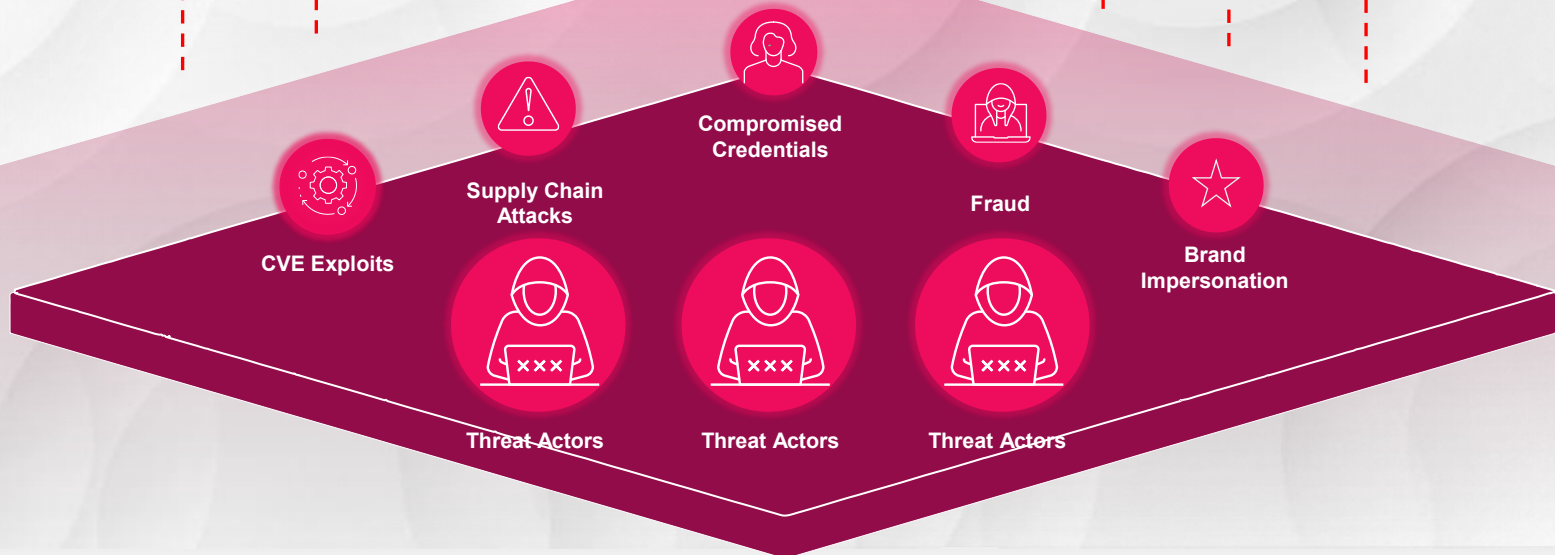
2. Ponemon Institute Reveals Security Teams Spend Approximately 25 Percent of Their Time Chasing False Positives; Response Times (source)

3. (ISC)2 Cybersecurity Workforce Study (source)

WHAT **ASSETS** DO YOU
NEED TO **PROTECT**?



WHAT **RISKS** DOES YOUR
ORGANIZATION **FACE**?



The External Risk Management Stack: Core Capabilities

Active Exposure Validation



Use advanced automation to actively test your organization's exposures for exploitability.

Attack Surface Management

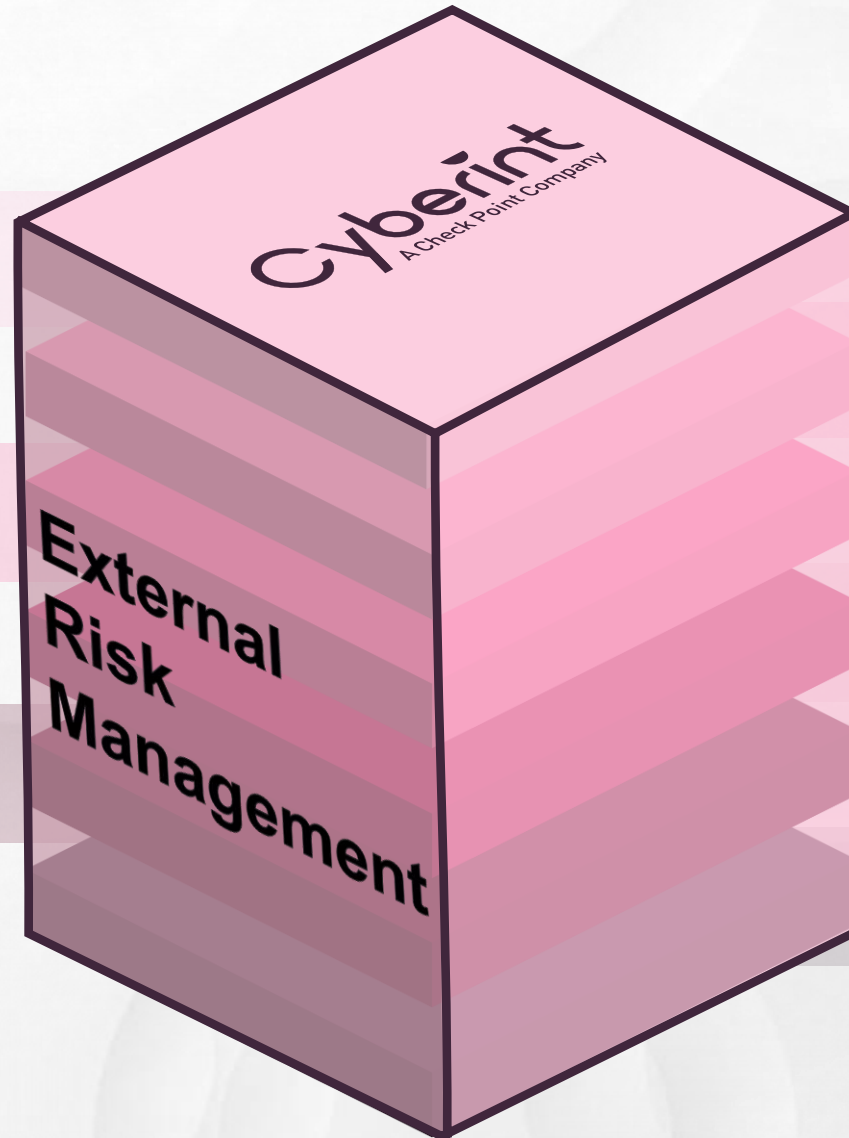


Continuously discover your Internet-facing assets to understand relevant exposures and risks.

Deep & Dark Web Monitoring



Gain visibility into cybercrime activity on the deep and dark web to uncover hidden threats.



A complete solution for mitigating external risks



Optimal visibility on assets and relevant cyber threats



Supported by expert threat intelligence services

Access strategic threat intelligence, track ransomware activity, and understand your unique threat landscape.

Comprehensive External Risk Management Solution

Attack Surface Monitoring

-  Shadow IT & Asset Discovery
-  Vulnerabilities & Exposure Detection
-  Active Exposure Validation

Global Threat Intelligence

-  Ransomware watch & Threat landscape
-  Enriched IoC Feeds
-  Intelligence Knowledgebase

Targeted Threat Intelligence

-  Dark web Monitoring & Actor Chatter
-  Credentials and Account Takeover
-  Fraud & Data leakage

Brand Protection & Impersonation

-  Brand & Phishing Protection
-  Social Media Impersonation
-  Mobile App Impersonation

Supply Chain Intelligence

-  Vendors & Technology Detection
-  3rd party Risk Management
-  Alerting on Critical Risks and Breaches

Remediation & Managed Takedown Services

Expert Threat Intelligence Services

Cyberint (ERM) Solution Packages

MODULE	CAPABILITY	ESSENTIAL	ADVANCED	COMPLETE	ELITE
Argos Application Fundamentals	Asset Discovery Engine	✓	✓	✓	✓
	Number of Users	1	3	5	8
Attack Surface Management	Vulnerabilities, Exposure detection, Technologies	Weekly	Daily	Daily	Daily
	Risk Posture Monitoring	✓	✓	✓	✓
	Active Exposure Validation	Fees Apply	Fees Apply	Fees Apply	Fees Apply
Digital Risk Protection	Typosquatting & Phishing Protection	✓	✓	✓	✓
	Social Media & Mobile App impersonation module		✓	✓	✓
	Impersonation manual Threat Hunting (Cyberint Analyst)			✓	✓
Targeted Threat Intelligence	Leaked credential detection from malware logs, marketplaces, and other sources	✓	✓	✓	✓
	Open, deep and darkweb sources collection & search engine		✓	✓	✓
	Targeted intelligence manual threat hunting for data leakage & fraud			✓	✓
Global Threat Intelligence	Global Cyber news and ransomware watch & IOC searches	✓	✓	✓	✓
	Global Intelligence Knowledgebase (Threat actors, Malware, CVE)		✓	✓	✓
Supply Chain Intelligence	Automatic Detection of used vendors		✓	✓	✓
	Vendor risk monitoring		3	5	10
	Proactive alerts on high identified risks		✓	✓	✓
Managed Services	Remediation: Cyberint coins for fully-managed Takedowns & Investigations	20	100	250	400
	Dedicated CTI Expert for on-going support, triage, review, analysis, and threat hunting			✓	✓
	Proactive threat hunting by CTI Expert				✓
	SLA for intelligence threat hunting for Cyber Incidents			24 Hours	4 Hours
Add-On Modules & Capabilities	Threat Hunting Users				1
	IOC Feed (Daily distribution)				
	IOC Enrichment API				

How Do We Sell

Enterprise (VAR)

- Customer owns the license
- SaaS platform covering ASM, Darkweb, Brand, 3rd party
- Can be managed or non-managed

Check Point provides CSM, onboarding, QBRs, support.

MSSP

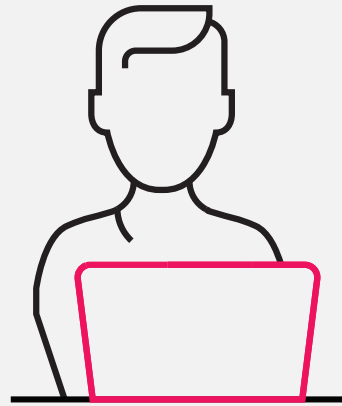
- MSSP owns the license
- SaaS platform covering ASM, Darkweb, Brand, 3rd party (Standalone or as a bundle)
- Fully managed

MSSP provides analyst services, Customer management, etc.

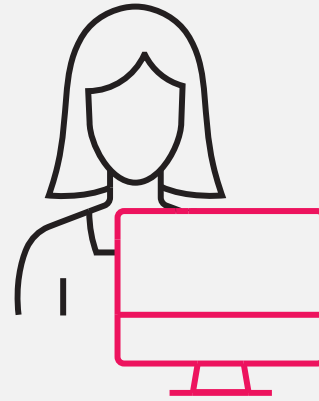
Customer Target Persona



CISO



SOC Manager











Threat Intelligence (TI)
Manager



Cybersecurity /
SOC Analyst

Target ICP

		Size	Team Size	CTI Maturity	Business Pain	Timing	ERM Package	Potential Deal Size
	Tier-1 	10,000 +	+5-7 Security Analysts	High	Silos (Fraud, ASM, CTI)	Reap & Replace	Elite	\$150k-400k
	Tier-2 	< 10,000	3-5	Medium	DRPS	Reap & Replace	Complete	\$80K-\$150K
	Tier-3 	< 3,000	3-5	Low-Medium	CTEM (BAS, ASM, DRP)	Upgrade	Advanced	\$50K-\$80K
	Tier-4 	< 1,000	Less than 3	Low	CTEM (BAS, ASM, DRP)	Create/Upgrade	Essential	\$25K-\$50K



Thank You