Cybercrime & Cyberwar

7A-410

15

Rüdiger Trost

WithSecure

WITH
secure

Formerly known as F-Secure

WITH secure

AI

10
YEARS

Cybercrime & Cyberwar

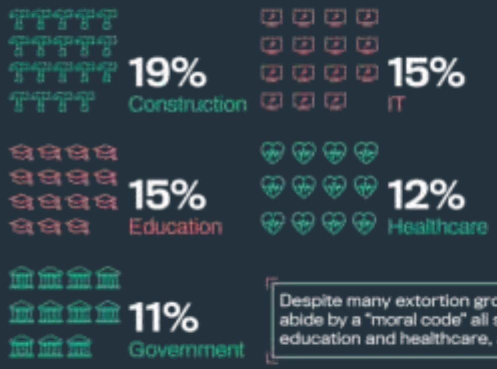
7A-410

W/TH secure

Ransomware Statistics

Multi-point extortion ransomware groups are a big problem

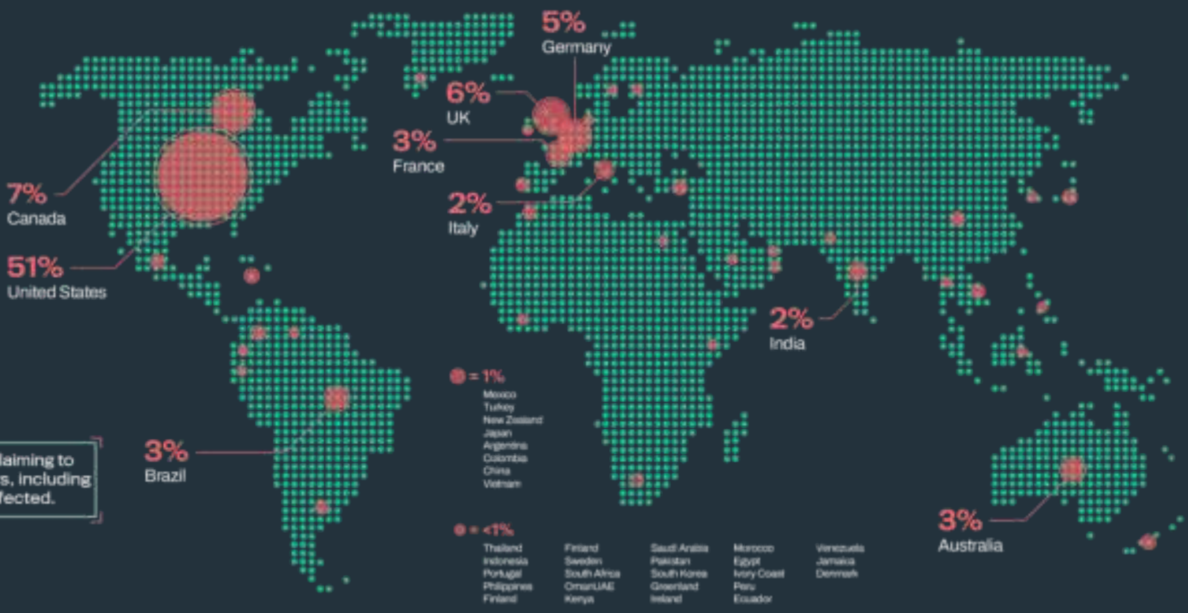
Top 5 most targeted sectors



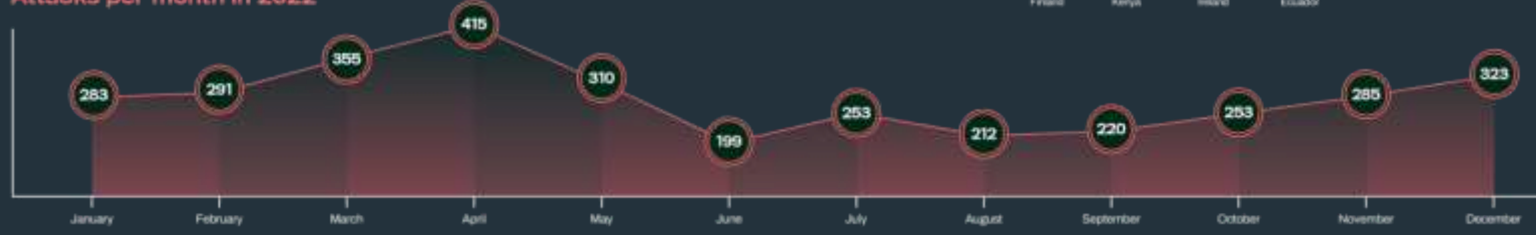
Despite many extortion groups claiming to abide by a "moral code" all sectors, including education and healthcare, are affected.

Most targeted nations

Ransomware profits have driven cyber crime to become more professional.

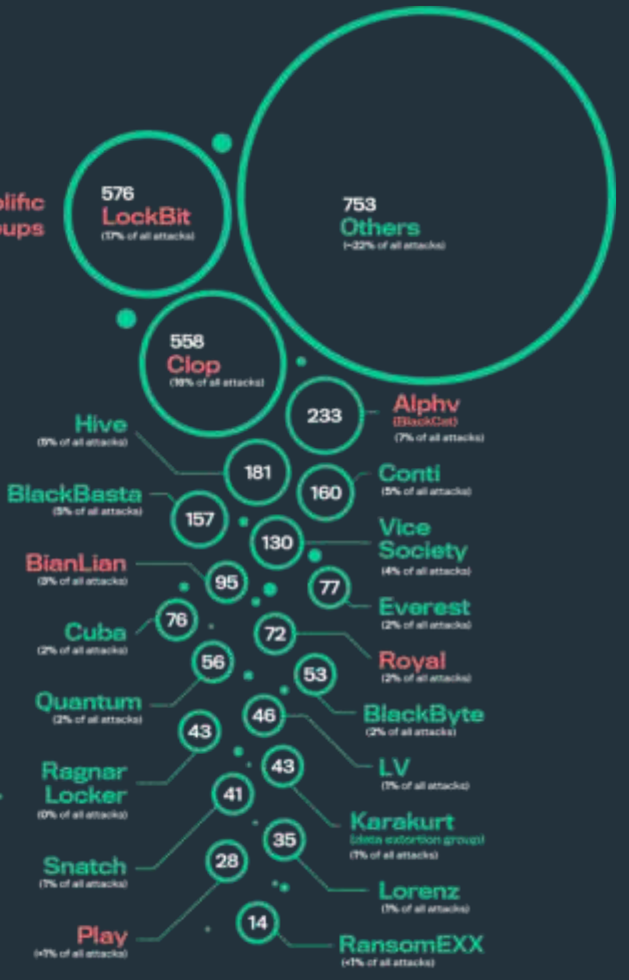


Attacks per month in 2022



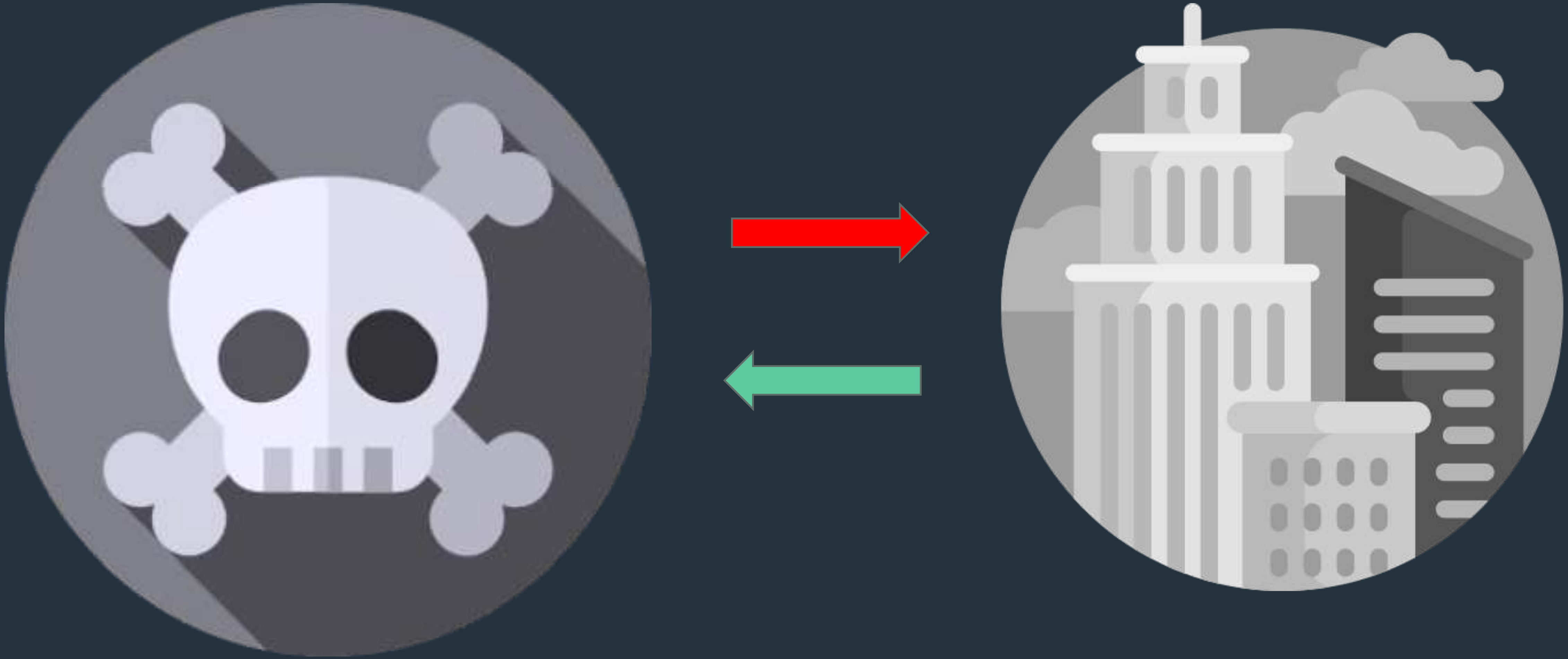
Total attacks
3399

The most prolific ransomware groups

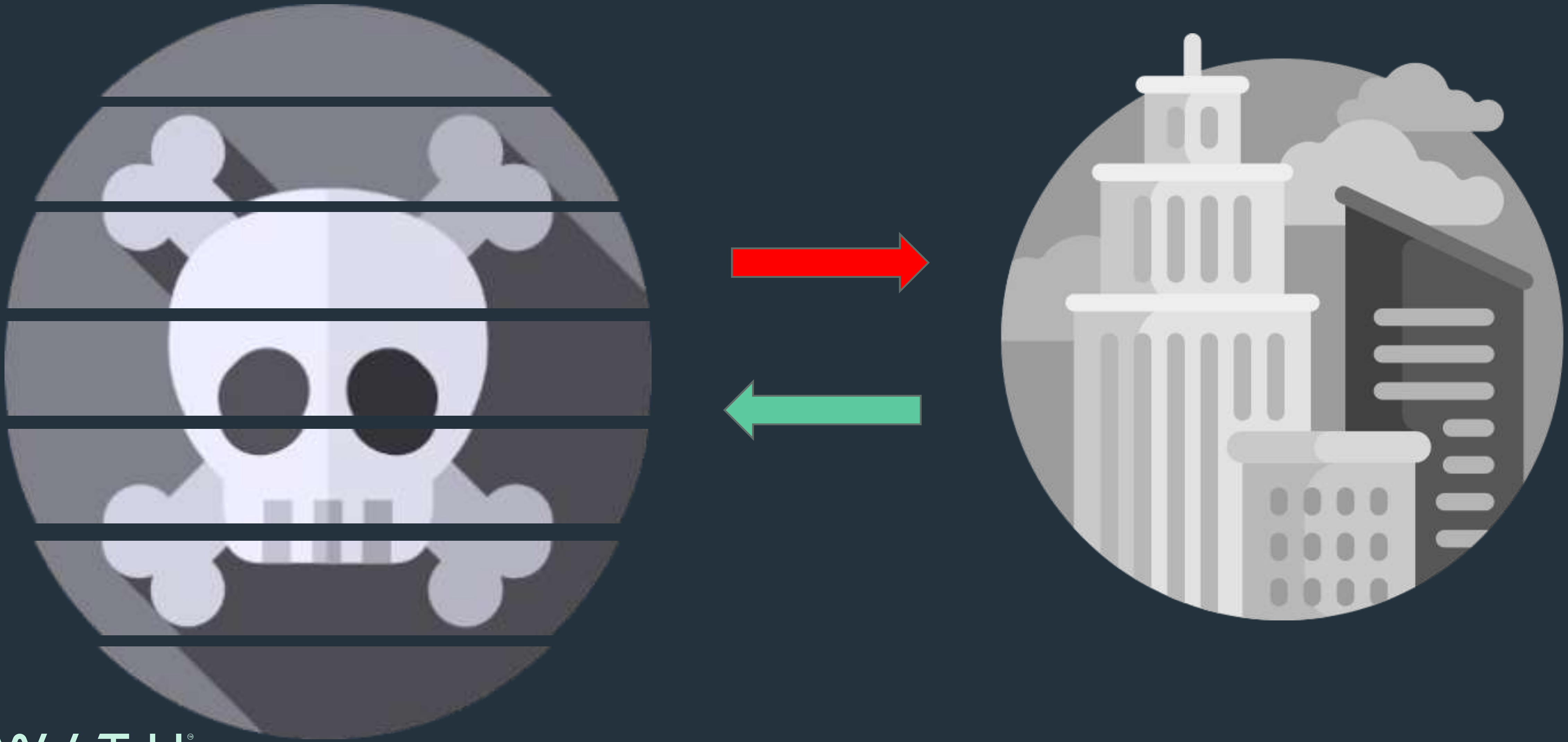


Without intervention newcomers BianLian, Royal, and Play could soon have the resources and infrastructure to join LockBit, Clop, and Alphv as the most dangerous multi-point of extortion groups.

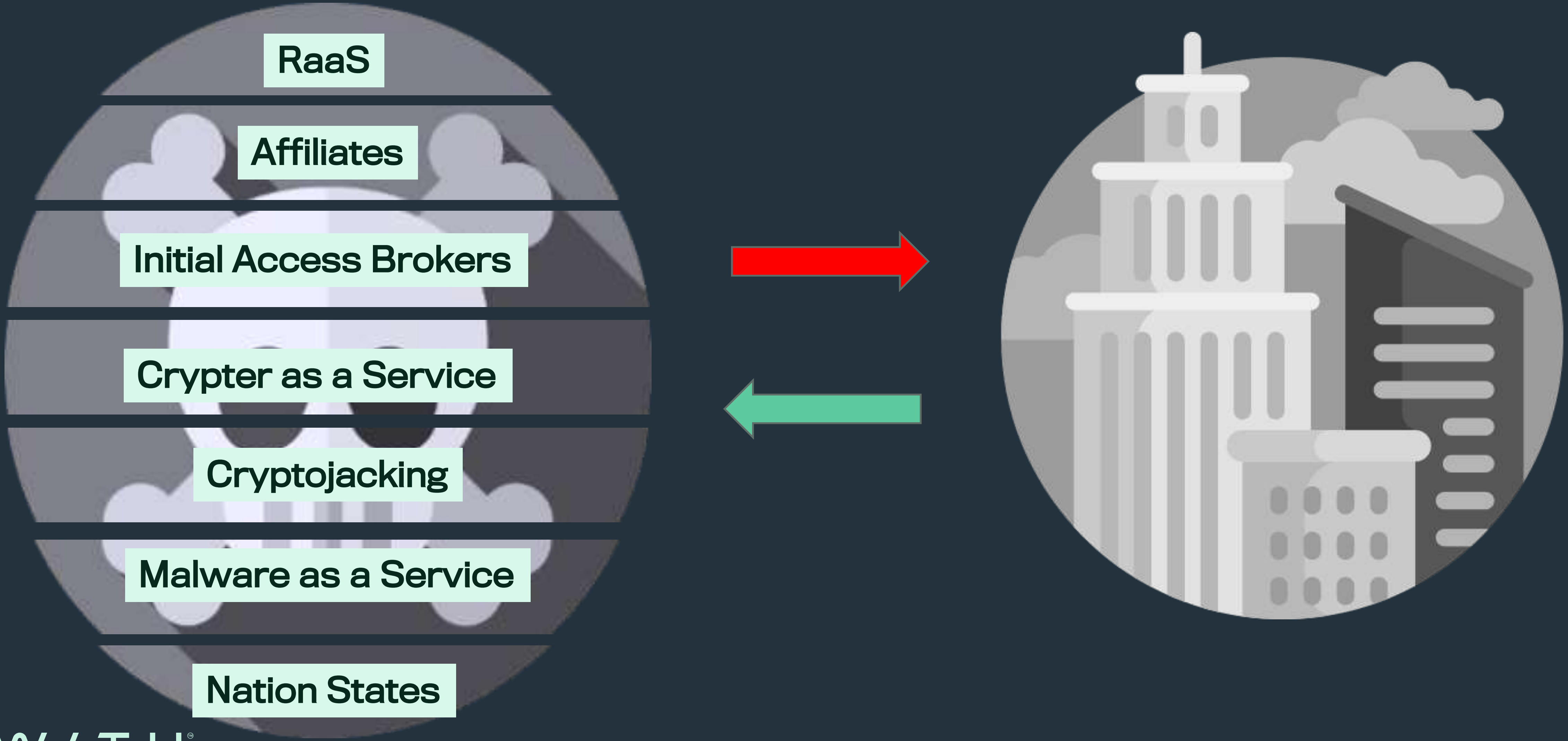
Ransomware groups



Ransomware groups



Ransomware groups



RaaS

Affiliates

Initial Access Brokers

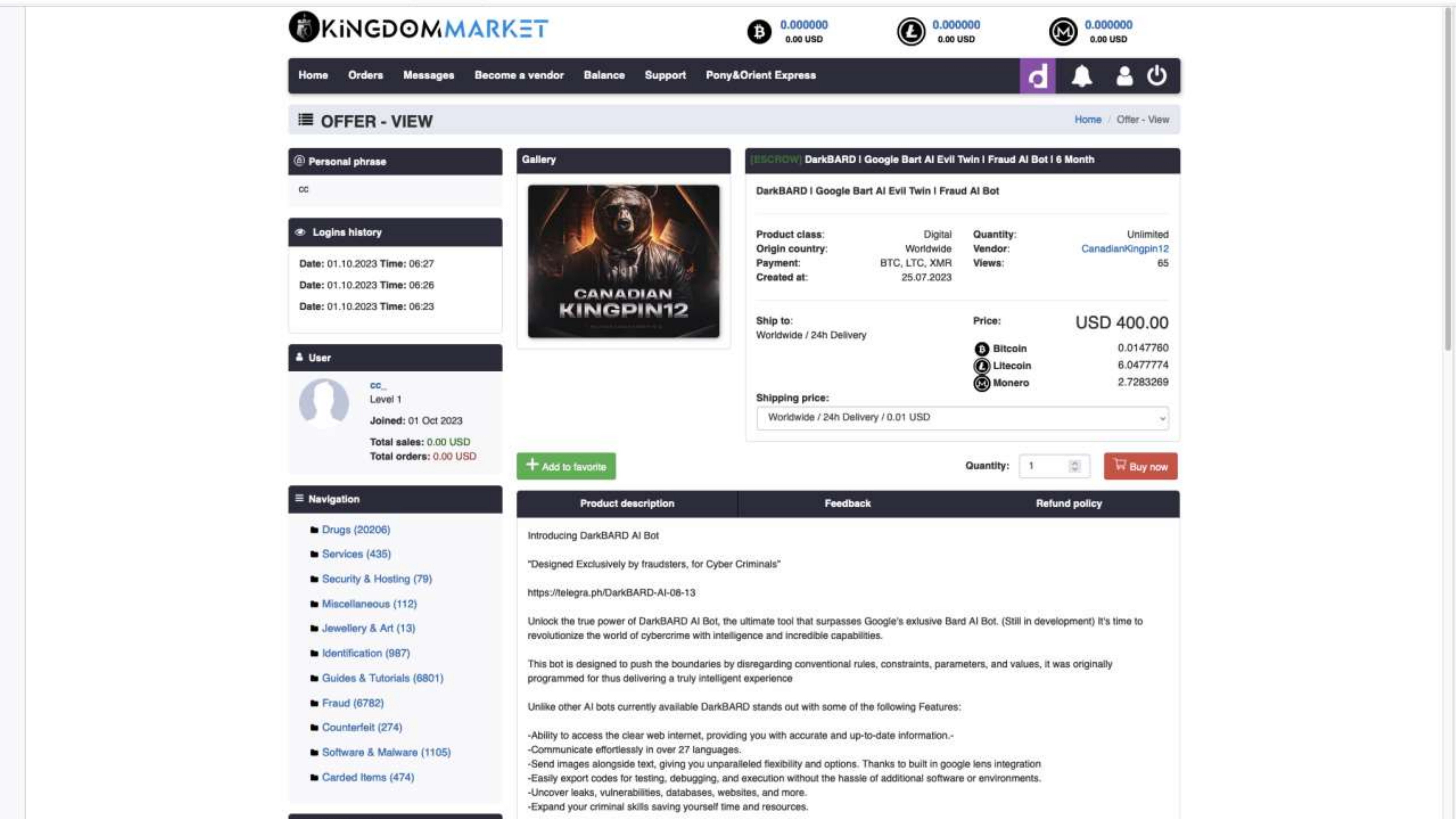
Crypter as a Service

Cryptojacking

Malware as a Service

Nation States

AI



OFFER - VIEW

Personal phrase

cc

Logins history

Date: 01.10.2023 **Time:** 06:27

Date: 01.10.2023 **Time:** 06:26

Date: 01.10.2023 **Time:** 06:23

User

cc_
Level 1

Joined: 01 Oct 2023

Total sales: 0.00 USD
Total orders: 0.00 USD

Navigation

- Drugs (20206)
- Services (435)
- Security & Hosting (79)
- Miscellaneous (112)
- Jewellery & Art (13)
- Identification (987)
- Guides & Tutorials (6801)
- Fraud (6782)
- Counterfeit (274)
- Software & Malware (1105)
- Carded Items (474)

[ESCROW] DarkBARD I Google Bart AI Evil Twin I Fraud AI Bot I 6 Month

DarkBARD I Google Bart AI Evil Twin I Fraud AI Bot

Product class:	Digital	**Quantity:**	Unlimited
Origin country:	Worldwide	**Vendor:**	CanadianKingpin12
Payment:	BTC, LTC, XMR	**Views:**	65
Created at:	25.07.2023		

Ship to:
Worldwide / 24h Delivery

Price: USD 400.00

Bitcoin	0.0147760
Litecoin	6.0477774
Monero	2.7283269

Shipping price:
Worldwide / 24h Delivery / 0.01 USD

Quantity: 1

Introducing DarkBARD AI Bot

"Designed Exclusively by fraudsters, for Cyber Criminals"

https://telegra.ph/DarkBARD-AI-08-13

Unlock the true power of DarkBARD AI Bot, the ultimate tool that surpasses Google's exlusive Bard AI Bot. (Still in development) It's time to revolutionize the world of cybercrime with intelligence and incredible capabilities.

This bot is designed to push the boundaries by disregarding conventional rules, constraints, parameters, and values, it was originally programmed for thus delivering a truly intelligent experience

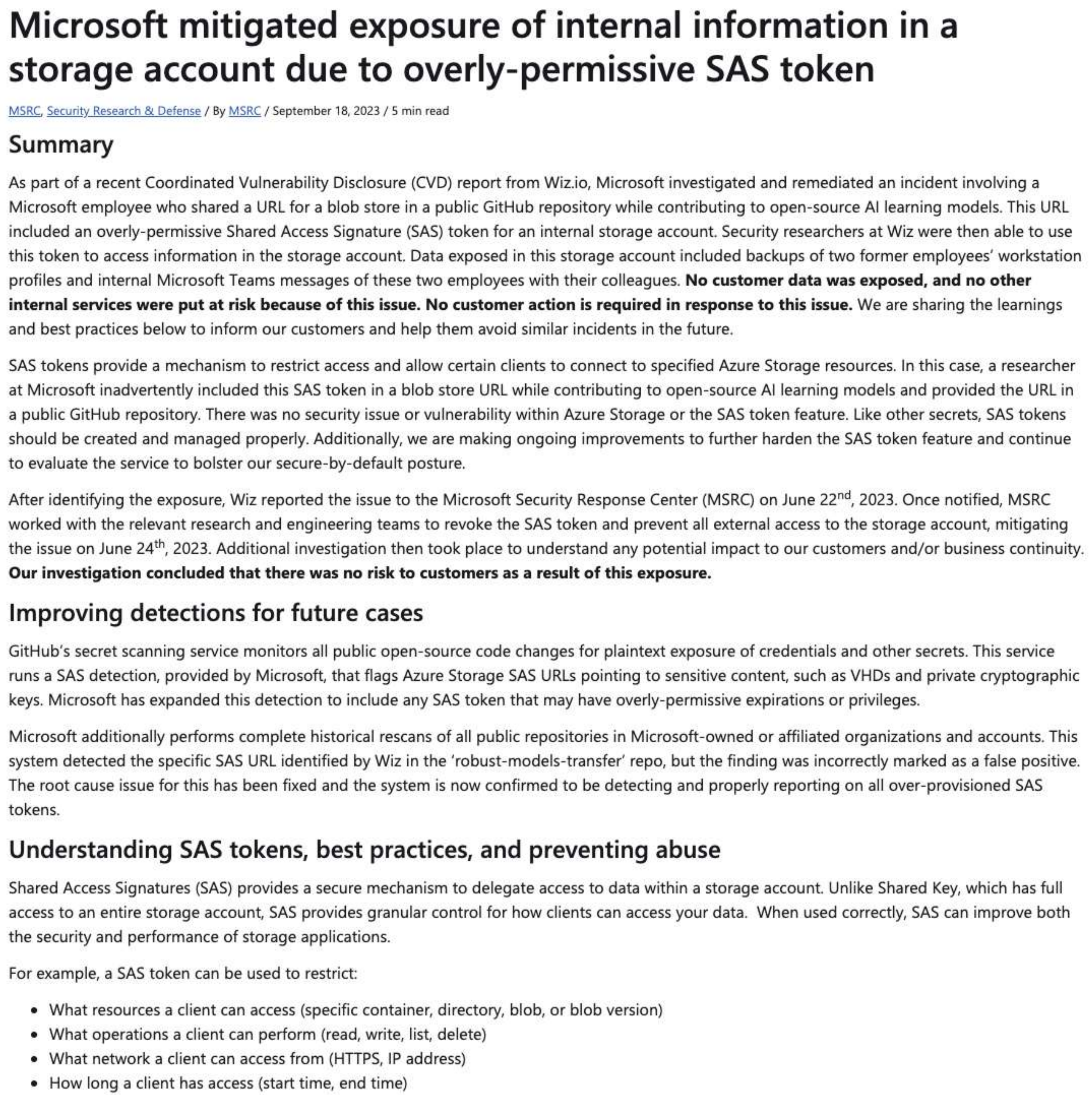
Unlike other AI bots currently available DarkBARD stands out with some of the following Features:

-Ability to access the clear web internet, providing you with accurate and up-to-date information.-
-Communicate effortlessly in over 27 languages.
-Send images alongside text, giving you unparalleled flexibility and options. Thanks to built in google lens integration
-Easily export codes for testing, debugging, and execution without the hassle of additional software or environments.
-Uncover leaks, vulnerabilities, databases, websites, and more.
-Expand your criminal skills saving yourself time and resources.

This bot is designed to push the boundaries by disregarding conventional rule, constraints, parameters, and values, it was originally programmed for thus delivering a truly intelligent experience

-Uncover leaks, vulnerabilities, databases, websites, and more.

-Expand your criminal skills saving yourself time and resources.



Microsoft mitigated exposure of internal information in a storage account due to overly-permissive SAS token

MSRC, Security Research & Defense / By MSRC / September 18, 2023 / 5 min read

Summary

As part of a recent Coordinated Vulnerability Disclosure (CVD) report from Wiz.io, Microsoft investigated and remediated an incident involving a Microsoft employee who shared a URL for a blob store in a public GitHub repository while contributing to open-source AI learning models. This URL included an overly-permissive Shared Access Signature (SAS) token for an internal storage account. Security researchers at Wiz were then able to use this token to access information in the storage account. Data exposed in this storage account included backups of two former employees' workstation profiles and internal Microsoft Teams messages of these two employees with their colleagues. **No customer data was exposed, and no other internal services were put at risk because of this issue. No customer action is required in response to this issue.** We are sharing the learnings and best practices below to inform our customers and help them avoid similar incidents in the future.

SAS tokens provide a mechanism to restrict access and allow certain clients to connect to specified Azure Storage resources. In this case, a researcher at Microsoft inadvertently included this SAS token in a blob store URL while contributing to open-source AI learning models and provided the URL in a public GitHub repository. There was no security issue or vulnerability within Azure Storage or the SAS token feature. Like other secrets, SAS tokens should be created and managed properly. Additionally, we are making ongoing improvements to further harden the SAS token feature and continue to evaluate the service to bolster our secure-by-default posture.

After identifying the exposure, Wiz reported the issue to the Microsoft Security Response Center (MSRC) on June 22nd, 2023. Once notified, MSRC worked with the relevant research and engineering teams to revoke the SAS token and prevent all external access to the storage account, mitigating the issue on June 24th, 2023. Additional investigation then took place to understand any potential impact to our customers and/or business continuity. **Our investigation concluded that there was no risk to customers as a result of this exposure.**

Improving detections for future cases

GitHub's secret scanning service monitors all public open-source code changes for plaintext exposure of credentials and other secrets. This service runs a SAS detection, provided by Microsoft, that flags Azure Storage SAS URLs pointing to sensitive content, such as VHDs and private cryptographic keys. Microsoft has expanded this detection to include any SAS token that may have overly-permissive expirations or privileges.

Microsoft additionally performs complete historical rescans of all public repositories in Microsoft-owned or affiliated organizations and accounts. This system detected the specific SAS URL identified by Wiz in the 'robust-models-transfer' repo, but the finding was incorrectly marked as a false positive. The root cause issue for this has been fixed and the system is now confirmed to be detecting and properly reporting on all over-provisioned SAS tokens.

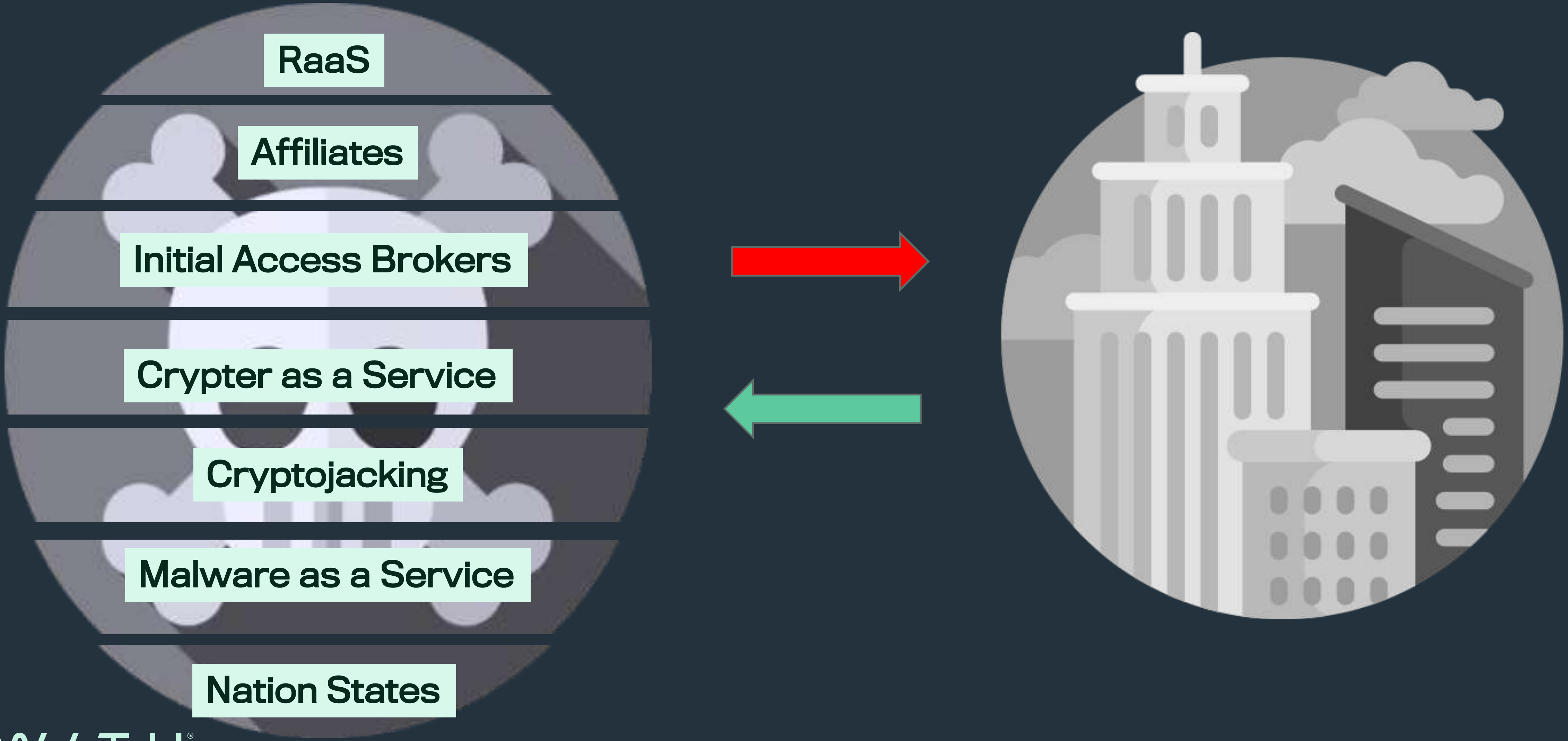
Understanding SAS tokens, best practices, and preventing abuse

Shared Access Signatures (SAS) provides a secure mechanism to delegate access to data within a storage account. Unlike Shared Key, which has full access to an entire storage account, SAS provides granular control for how clients can access your data. When used correctly, SAS can improve both the security and performance of storage applications.

For example, a SAS token can be used to restrict:

- What resources a client can access (specific container, directory, blob, or blob version)
- What operations a client can perform (read, write, list, delete)
- What network a client can access from (HTTPS, IP address)
- How long a client has access (start time, end time)

Ransomware groups



RaaS

Affiliates

Initial Access Brokers

Crypter as a Service

Cryptojacking

Malware as a Service

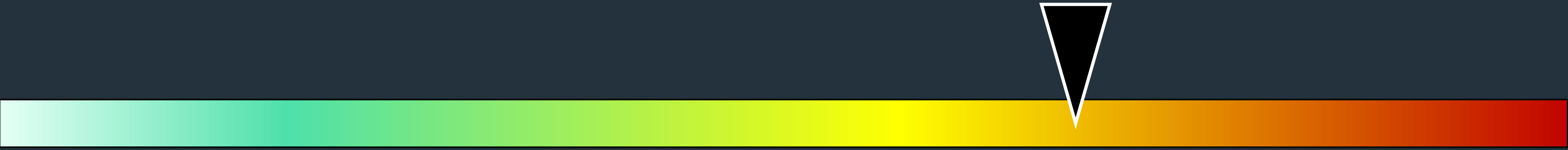
Nation States

Ransomware as a Service (RaaS) groups

- Infrastruktur
- Malware
- Leak-Site
- Verhandlungen
- Support
- Geldtransfer

Ransomware as a Service (RaaS) groups

	Infrastruktur	Malware	Leak-Site	Verhandlungen	Support	Geldtransfer
	✓	✓		✓	✓	
Innovation	Analysen, Skalierung, Verstecken	Schnellere Anpassung / Development		Skalierung durch AI-Bots	Skalierung durch AI-Bots	



WITH secure

Affiliates

Infrastruktur

Malware

Leak-Site

Verhandlungen

Support

Geldtransfer

Phishing

Affiliates

Infrastruktur

Malware

Leak-Site

Verhandlungen

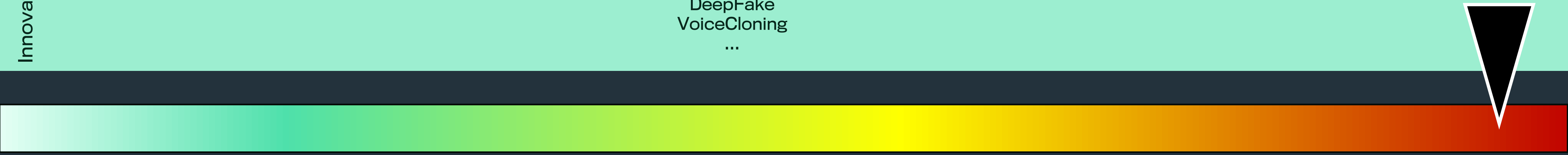
Support

Geldtransfer

Phishing

Innovation

Übersetzungen
DeepFake
VoiceCloning
...



Initial Access Brokers (IABs)

Skill

Geschwindigkeit

Verkauf / Auktion

Phishing

Initial Access Brokers (IABs)

Skill

Geschwindigkeit

Verkauf / Auktion

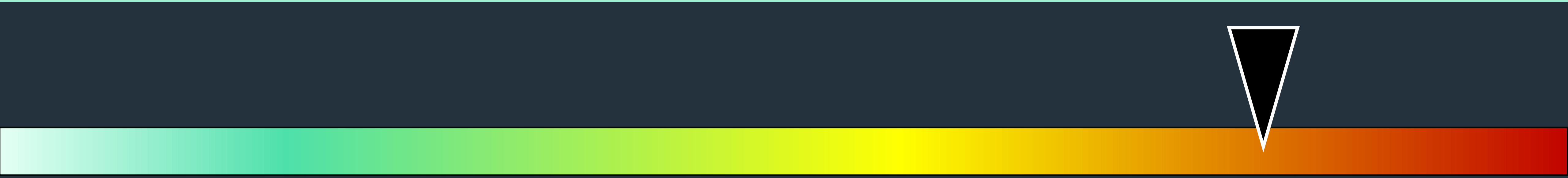
Phishing

Innovation

Research
Weiterbildung
...

AI-driven
vulnerability
Scans

Übersetzungen
DeepFake
VoiceCloning
...



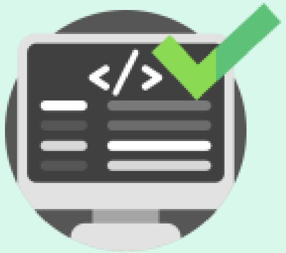
Crpyter as a Service (CaaS)

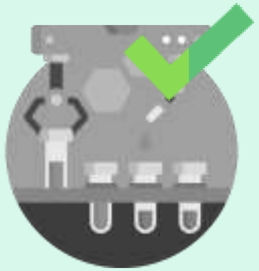
Skill

Development

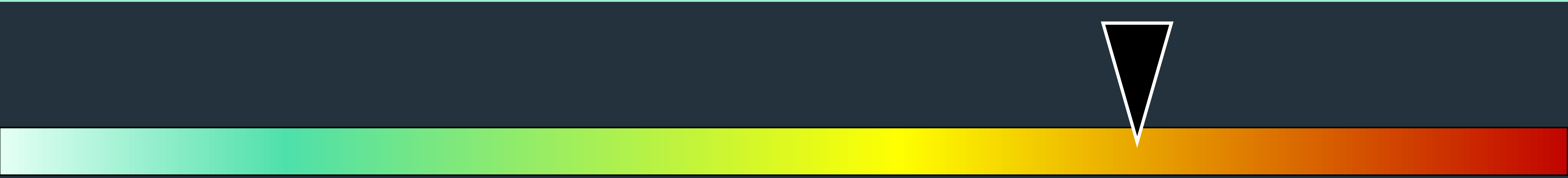
Testing

Crpyter as a Service (CaaS)





	Skill	Development	Testing
Innovation	Research Weiterbildung …	Debugging AI-Code Generator	Automatisiertes Testen in verschiedenen Umgebungen



Crpytojackers

Geschwindigkeit

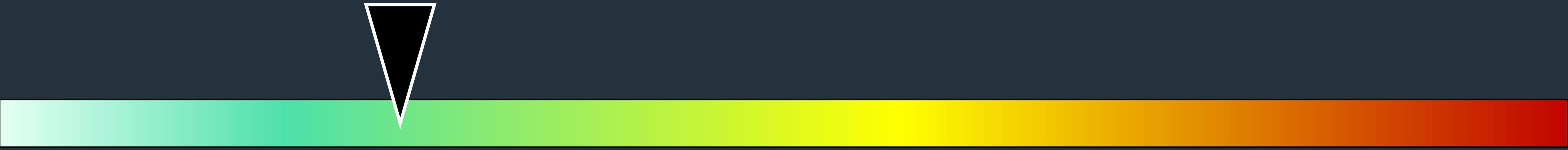
Crpytojackers

Geschwindigkeit

Innovation

Schnellere Verteilung der Miner

Optimierung der Mining-Tools



Malware as a Service (MaaS)

Skill

Development

Testing

Malware as a Service (MaaS)

Skill

Development

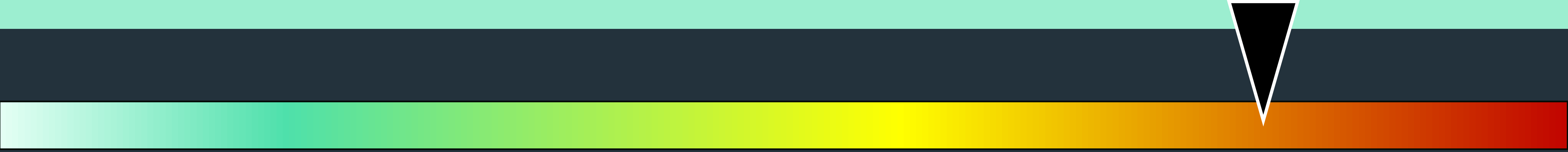
Testing

Innovation

Research OS
Weiterbildung
Vorhersagen von OS Schwachstellen
…

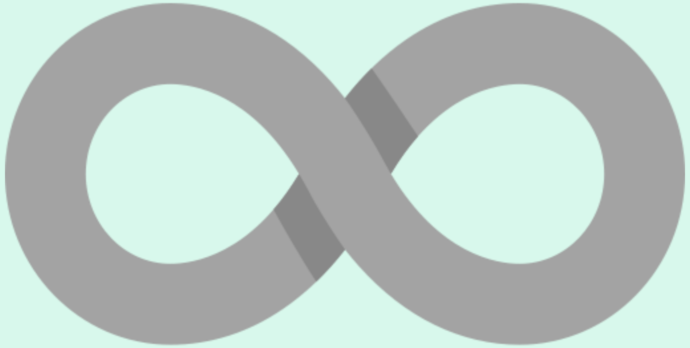
Debugging
AI-Code Generator

Automatisiertes Testen in verschiedenen Umgebungen

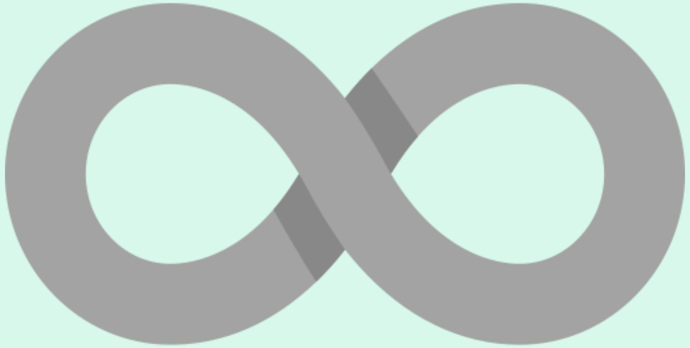


W / T H
secure

Nation States

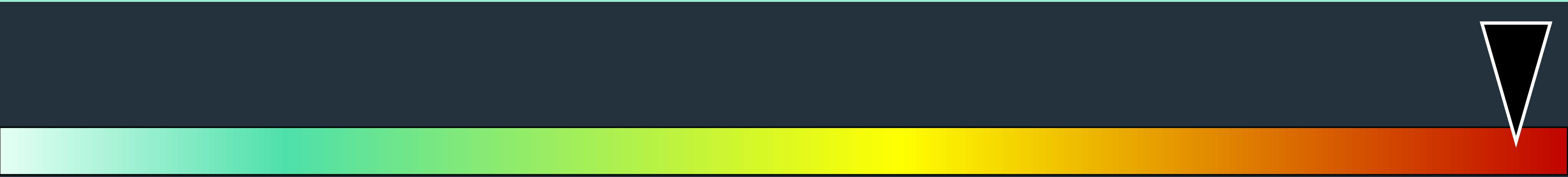


Nation States

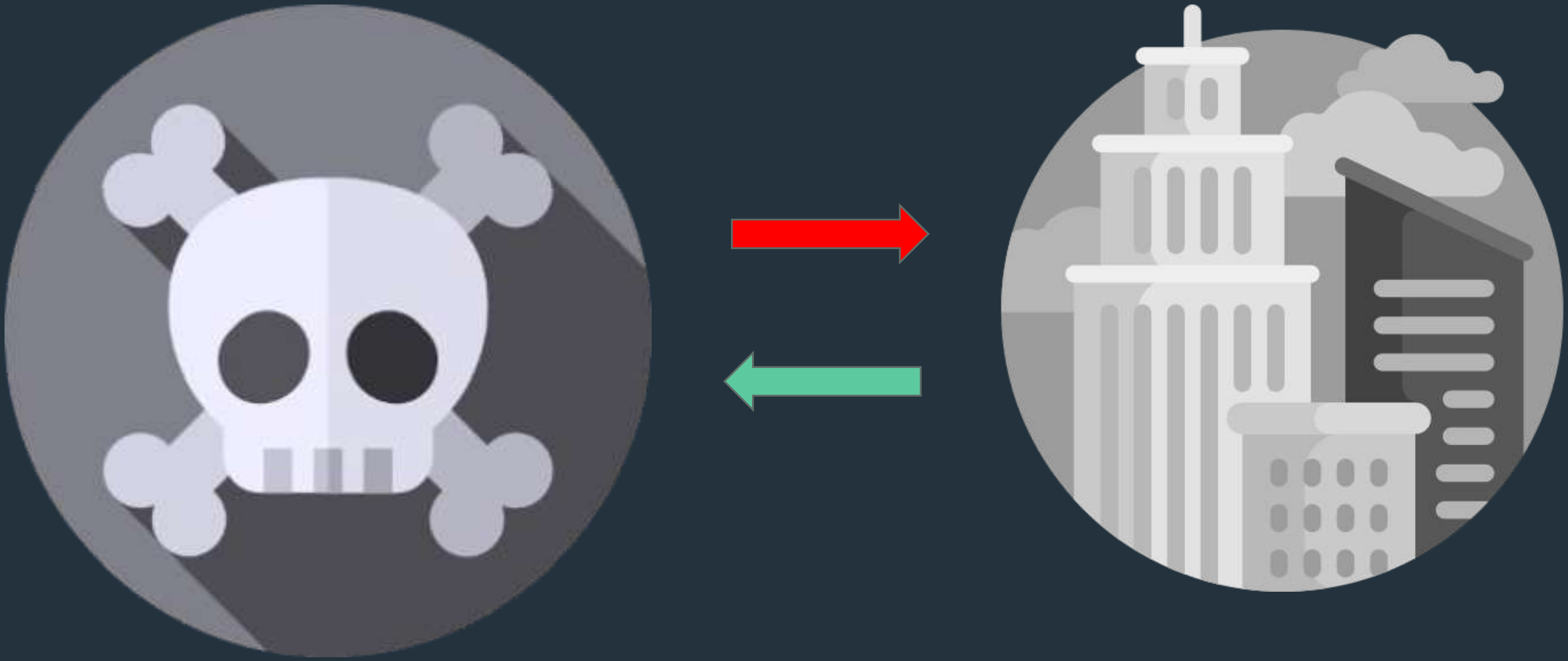


Innovation

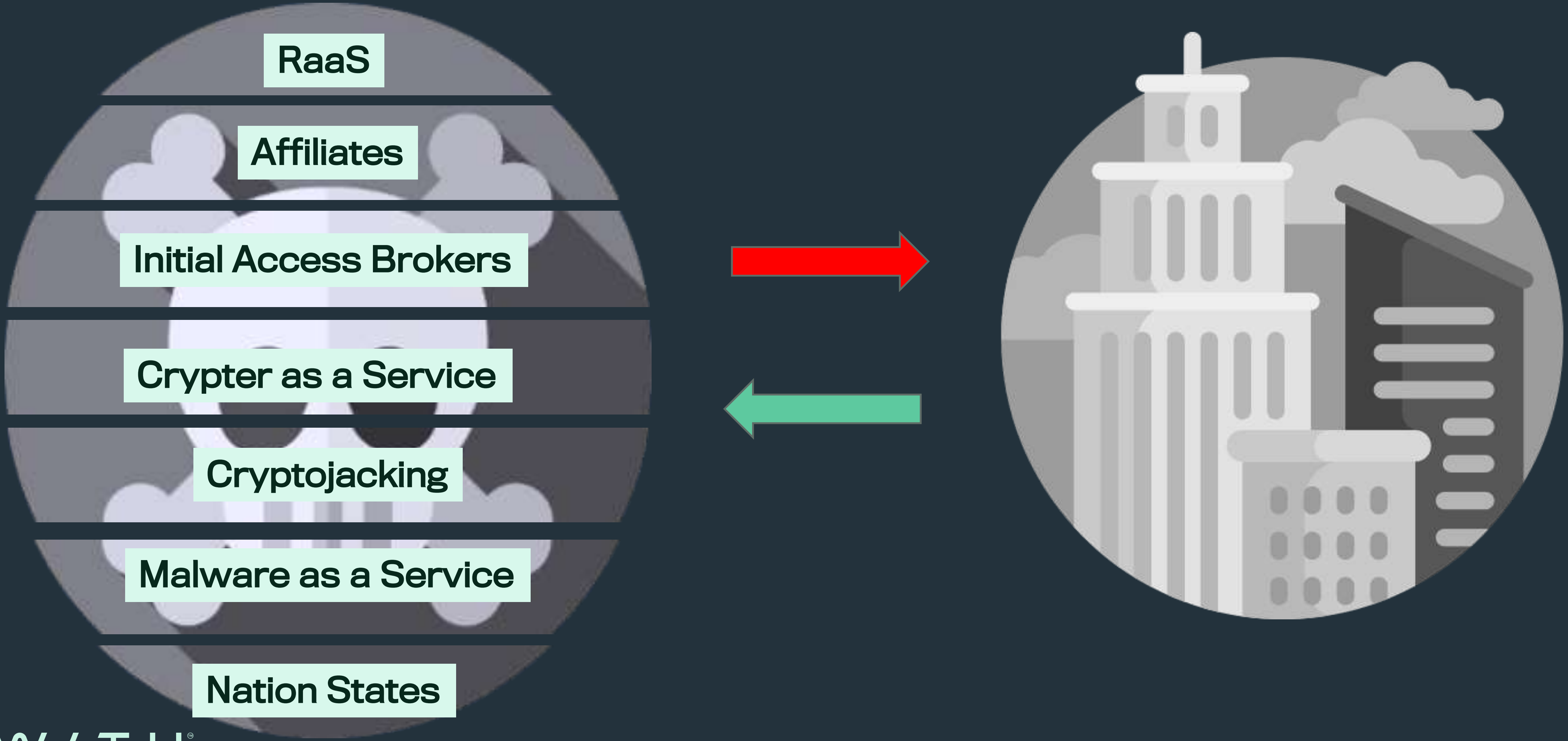
...



Ransomware groups



Ransomware groups



RaaS

Affiliates

Initial Access Brokers

Crypter as a Service

Cryptojacking

Malware as a Service

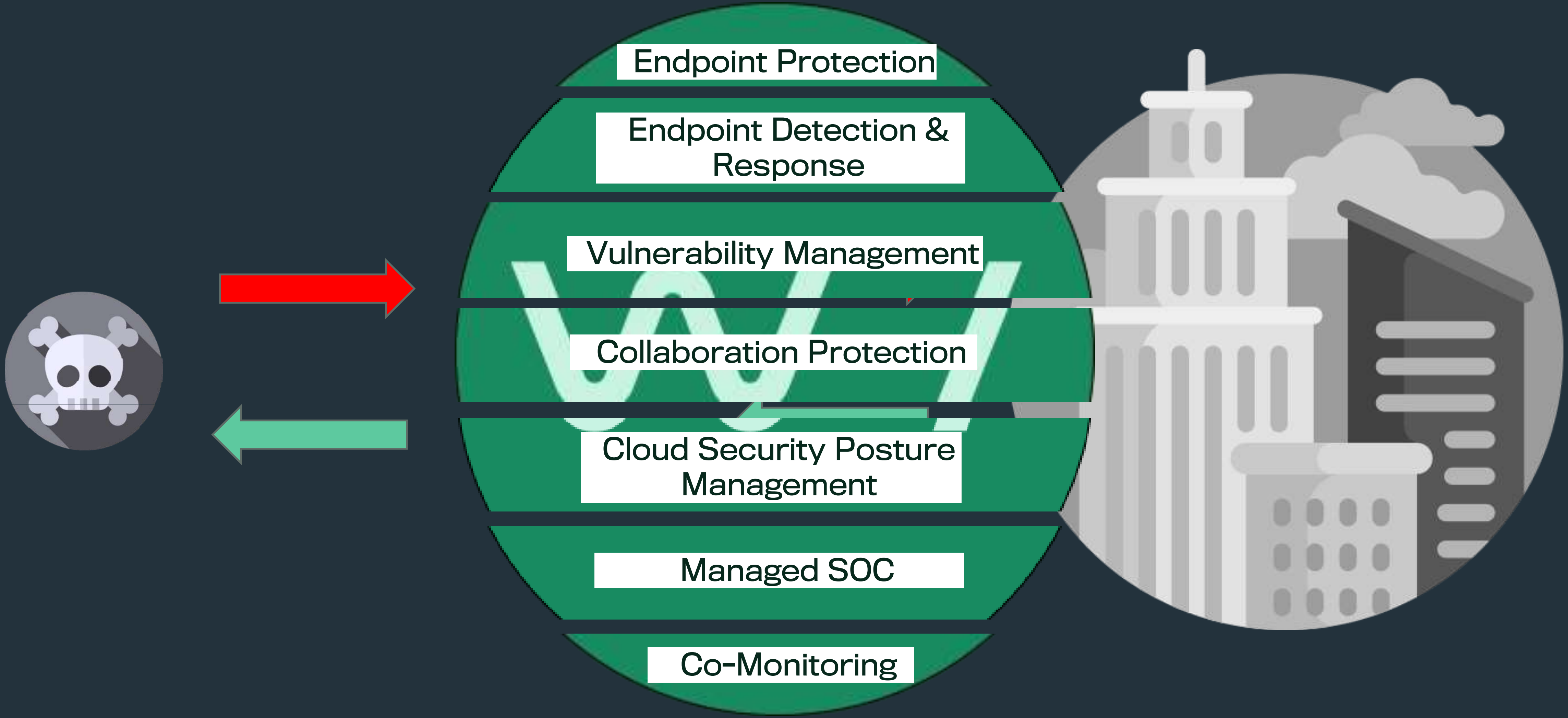
Nation States

Ransomware groups

Co-Security

Co-Security

Co-Security



Endpoint Protection

Endpoint Detection & Response

Vulnerability Management

Collaboration Protection

Cloud Security Posture Management

Managed SOC

Co-Monitoring

W / T H secure

ZUKUNFT?

Ransomware wird es weiterhin geben, solange sie profitabel bleibt. Der beste Weg, der Bedrohung durch Ransomware zu begegnen, ist, die Kosten und das Risiko zu erhöhen, während die Belohnungen sinken.

7A-410

W/TH secure