Security at Scale

Mastering Cloud Security in the Cyberwar Era

Cybersecurity Architect & Cybersecurity Community Lead
Siemens AG

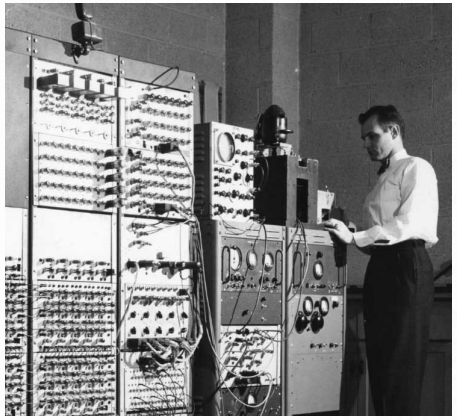
D o m i n i k S o w i n s k i

Agenda

1. Who am I
2. Introductory Thoughts & Recent Numbers
3. Five Example Cases
4. Key Insights & Key Takeaways
5. Summarizing Thoughts
6. References & Further Reads

#Who am I

Dominik Sowinski



Cyber Security Architect

Siemens AG

(Since 2023)

Senior Cloud Security Consultant/Architect

IBM

(from 2019)

...

M.Sc. Information Systems

B.Sc. Information Systems

B.A. Business Administration

& Communication Science

AWS Certified Security Specialist

AWS Certified Solution Architect

Azure Security Technologies

CISA

...

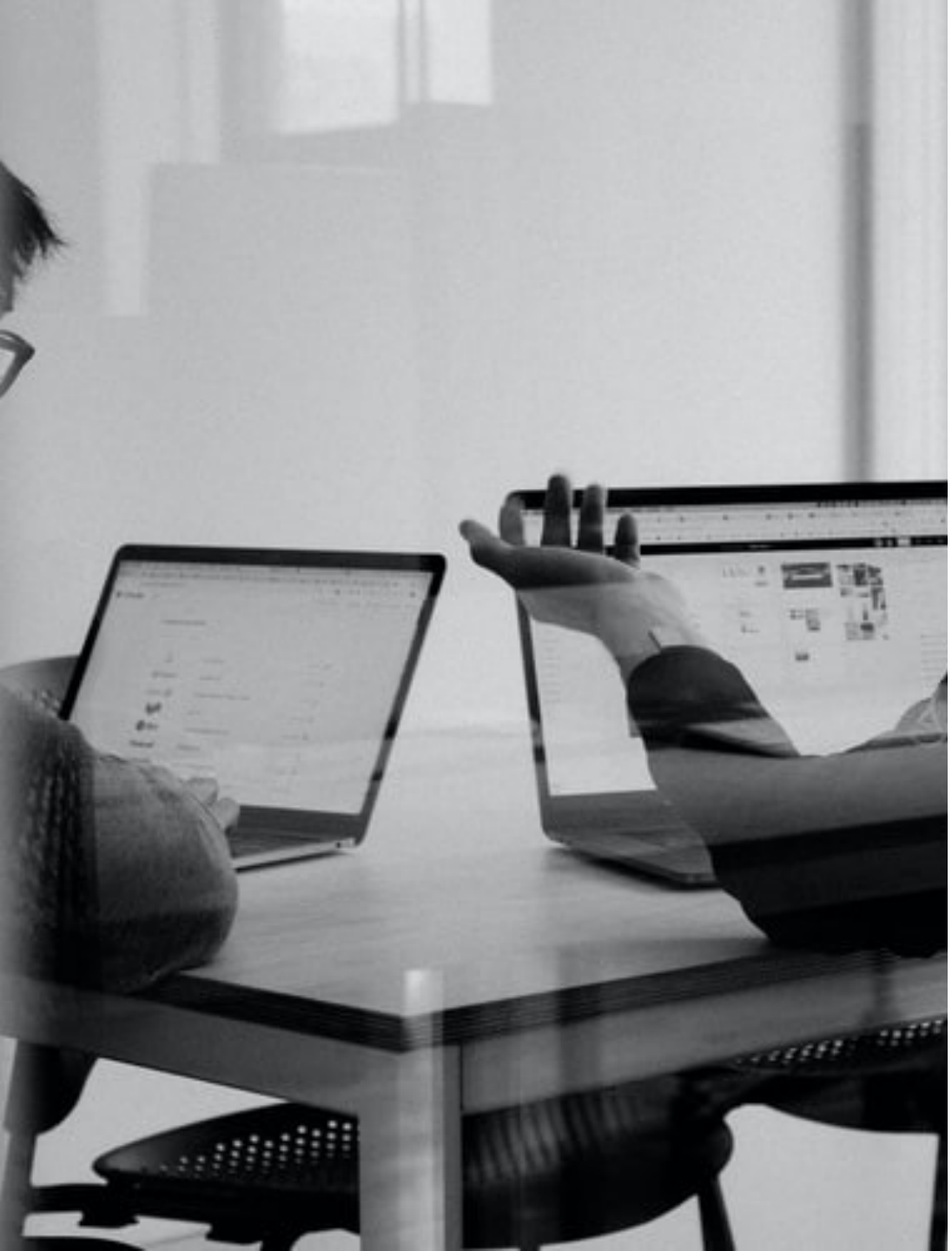
Food for Thought

Cyberwarfare is a distant threat, relevant only to military, governmental entities and critical infrastructure providers

Food for Thought

Cyberwarfare is a distant threat, relevant only to military, governmental entities and critical infrastructure providers

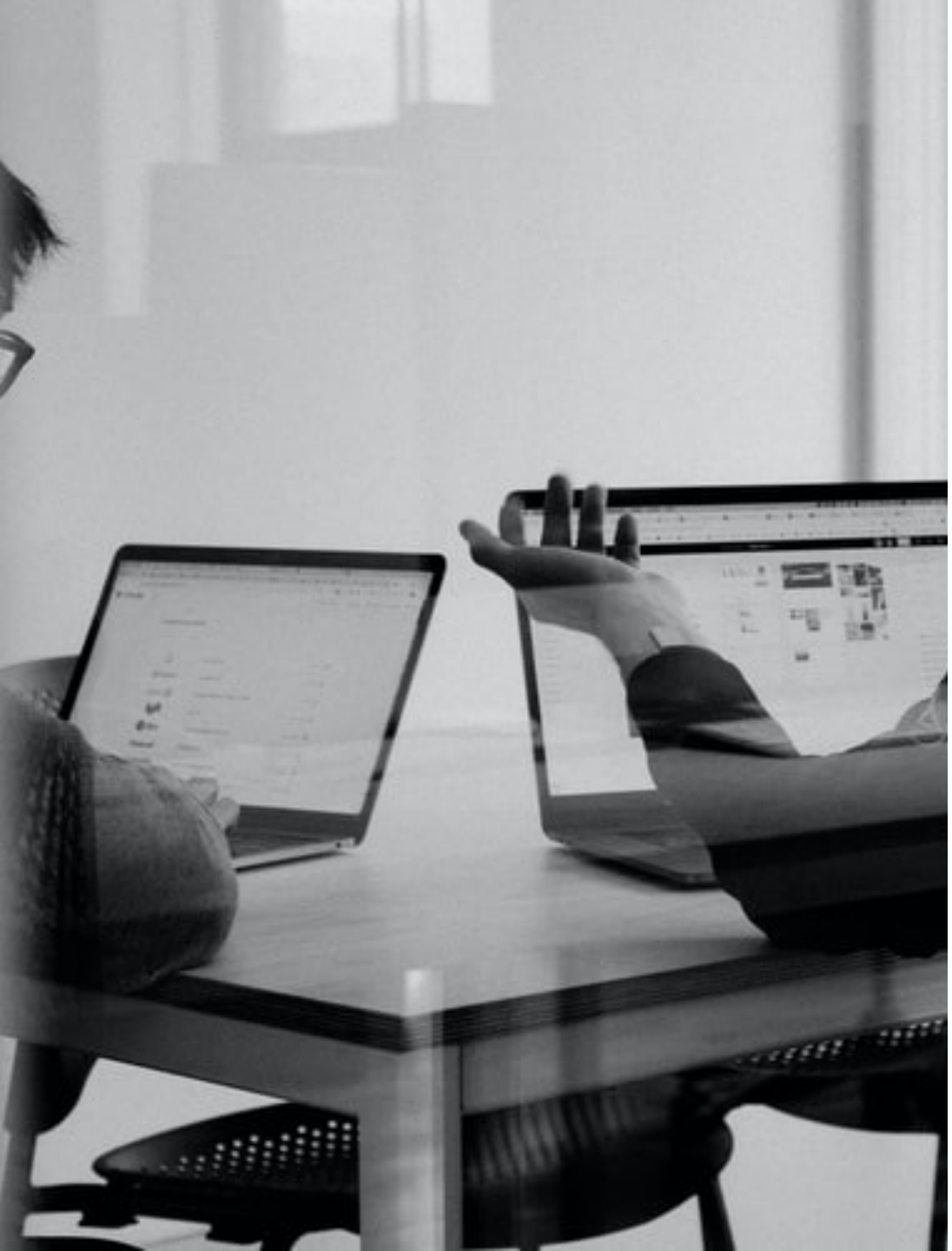
but is it really an exclusive concern?



…probably not

- 2010 - Stuxnet (Siemens)
- 2012 - Shamoon (Saudi Aramco)
- 2014 - Shamoon 2 (Sony Pictures)
- 2017 - NotPetya (Merck)
- 2018 - RAT & Mimikatz (Marriott)

…and many more



...probably not

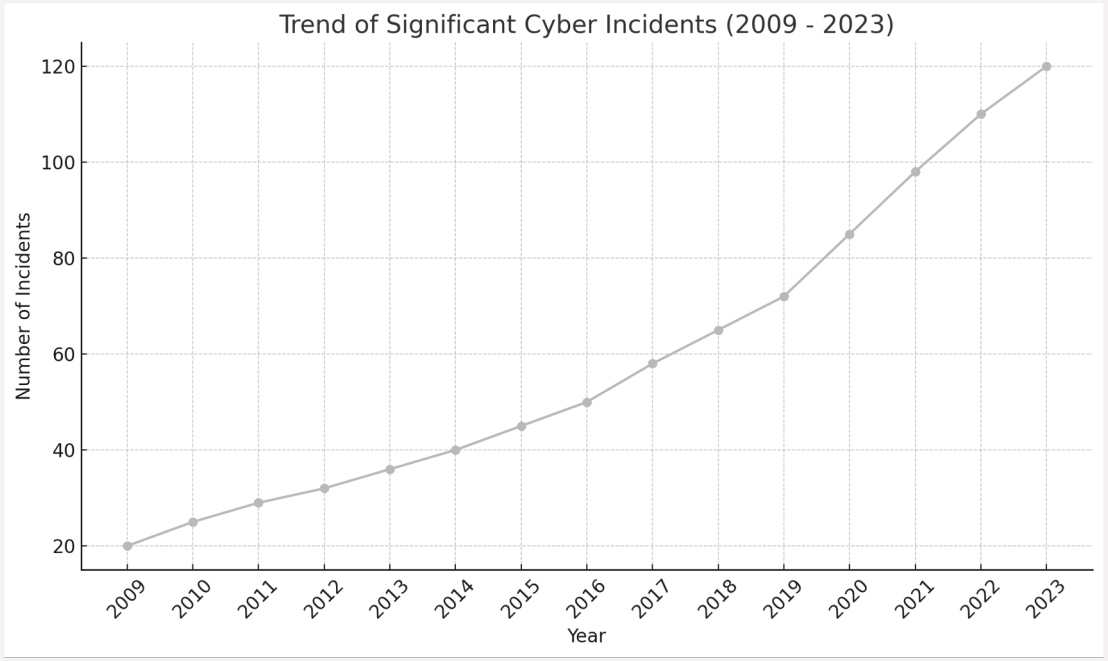
- **2010 - Stuxnet (Siemens)**
  - 200.000 devices damaged or destroyed; millions for Siemens and rework of whole business unit, reputation damage
- **2012 - Shamoon (Saudi Aramco)**
  - 30.000 destroyed workstations – millions to restore and ramp up cybersecurity
- **2014 - Shamoon 2 (Sony Pictures)**
  - $100 million for investigation, remediation, and legal fees, along with reputational damage and operational disruptions
- **2017 - NotPetya (Merck)**
  - $870 million, primarily due to the loss of production and associated recovery costs+
- **2018 - RAT & Mimikatz (Marriott Hotels)**
  - $28 million for legal, consulting, and other expenses related to the breach

Food for Thougth

State-sponsored cyber-attacks are skyrocketing. Attacks on critical infrastructure alone have increased by more than 40% in recent years*.

(*Source: Microsoft Digital Defense Report 2022)

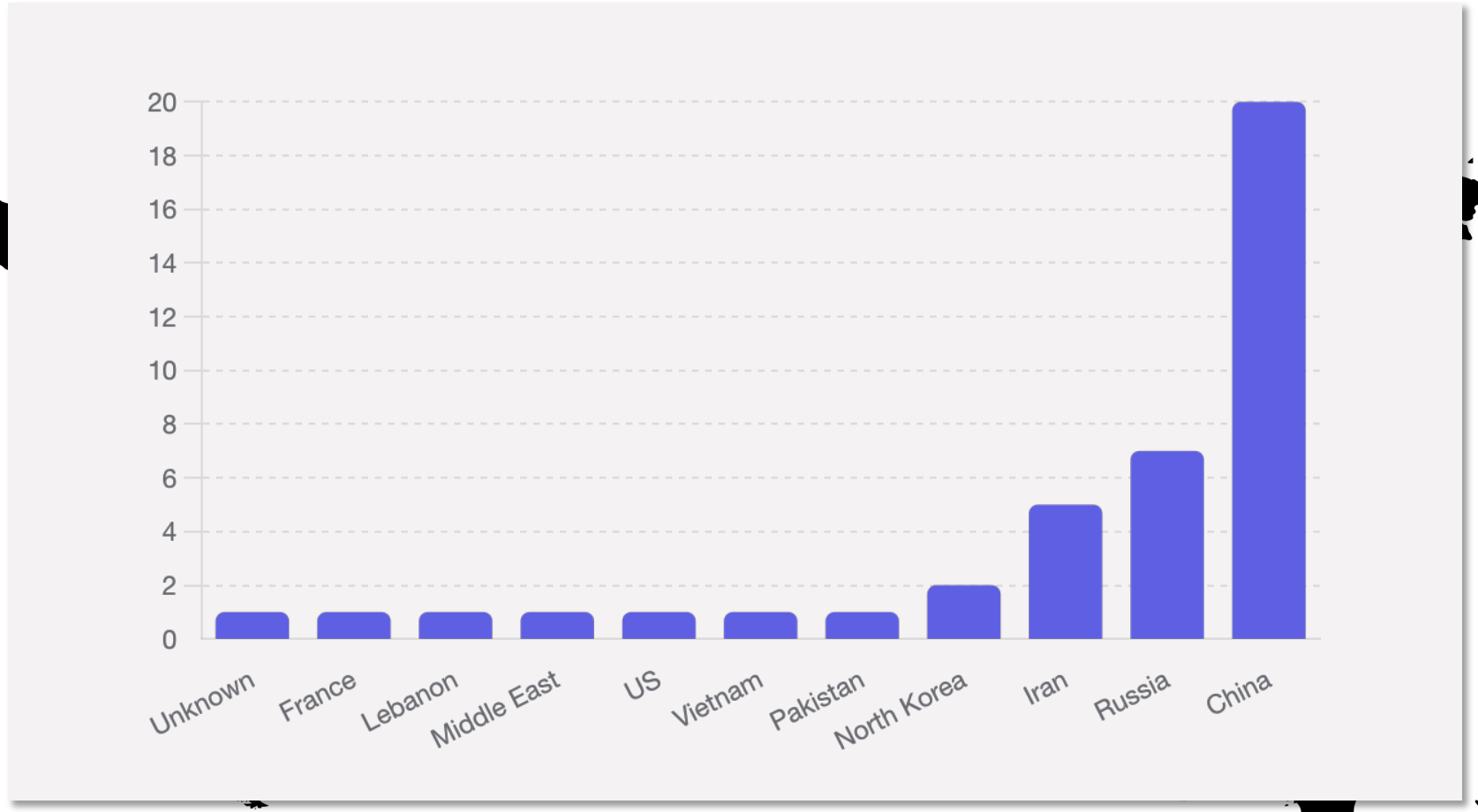
Trend of APT attacks gows up



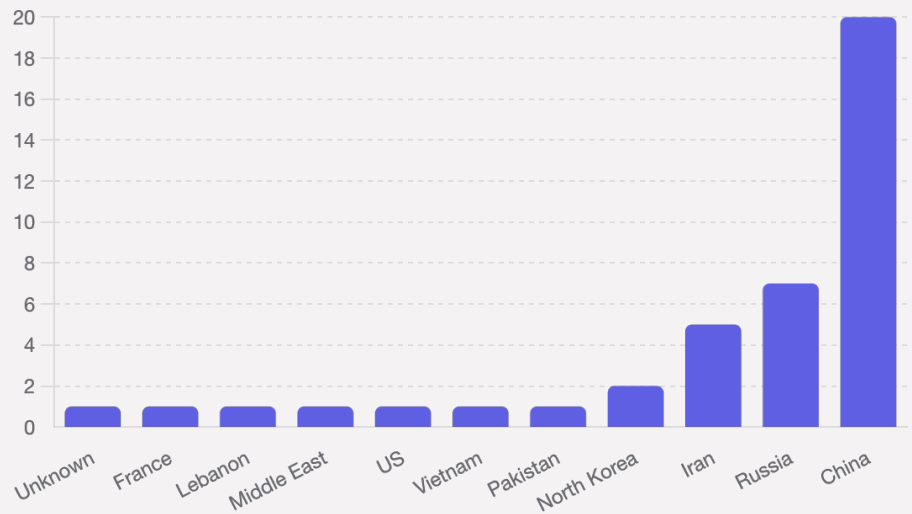
(*Source: https://www.csis.org 2024)

The Threat Landscape - Global View

The Threat Landscape – APT Numbers



The Threat Landscape – APT Numbers

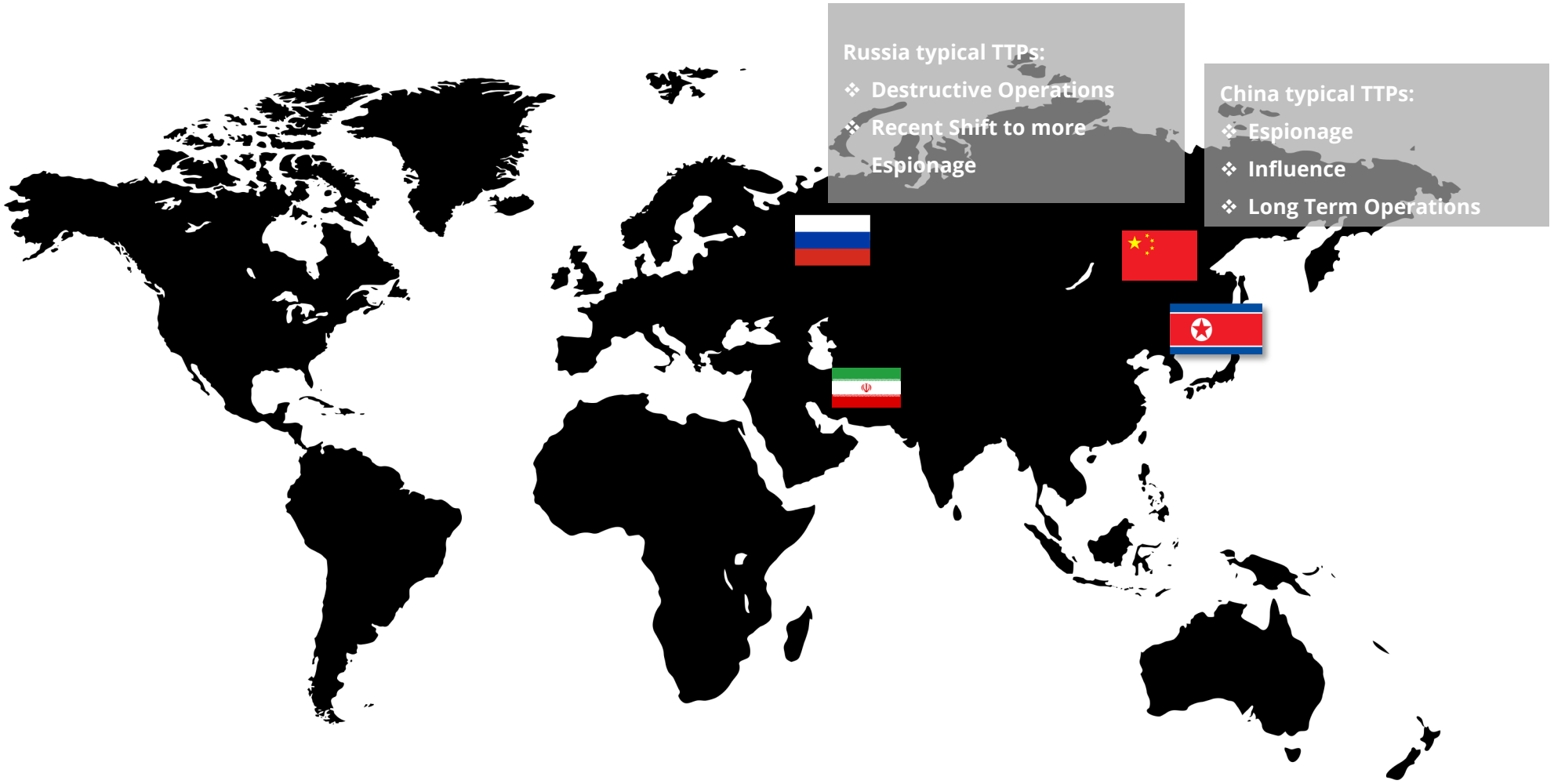


North Korea	Iran	Russia	China
APT 38 (Lazarus Group)	APT 34	Sandworm	Spring Dragon
Kimsuky	APT 35	DEV-0586	Hafnium
	Copy Kittens	The Snake Group	Hurricane Panda
	Clever Kittens	Actinium Group (Garmagedon)	Icefog
	Rocket Kittens	Energetic Bear	APT 1 (Comment Crew)
	Flying Kittens	Red October	APT 2 (Putter Panda)
		APT 28 (Fancy Bear/Strontium)	APT 3 (Gothic Panda)
		APT 29 (Cozy Bear)	APT 4 (Maverick Panda)
			APT 6
			APT 7
			APT 8
			APT 10
			APT 12 (XESHE Group)
			APT 15 (Ke3chang)
			APT 16
			APT 17 (ShellCrew/Deputy Dog)
			APT 18 (Dynamite Panda)
			APT 19 (Deep Panda)
			APT 20 (Violin Panda)
			APT 21 (NetTraveler)
			APT 22
			APT 24
			APT 26
			APT 27 (Emissary Panda)
			APT 30 (Naikon Group)
			APT 31 (Judgement Panda)

The Threat Landscape – The Big Four

2

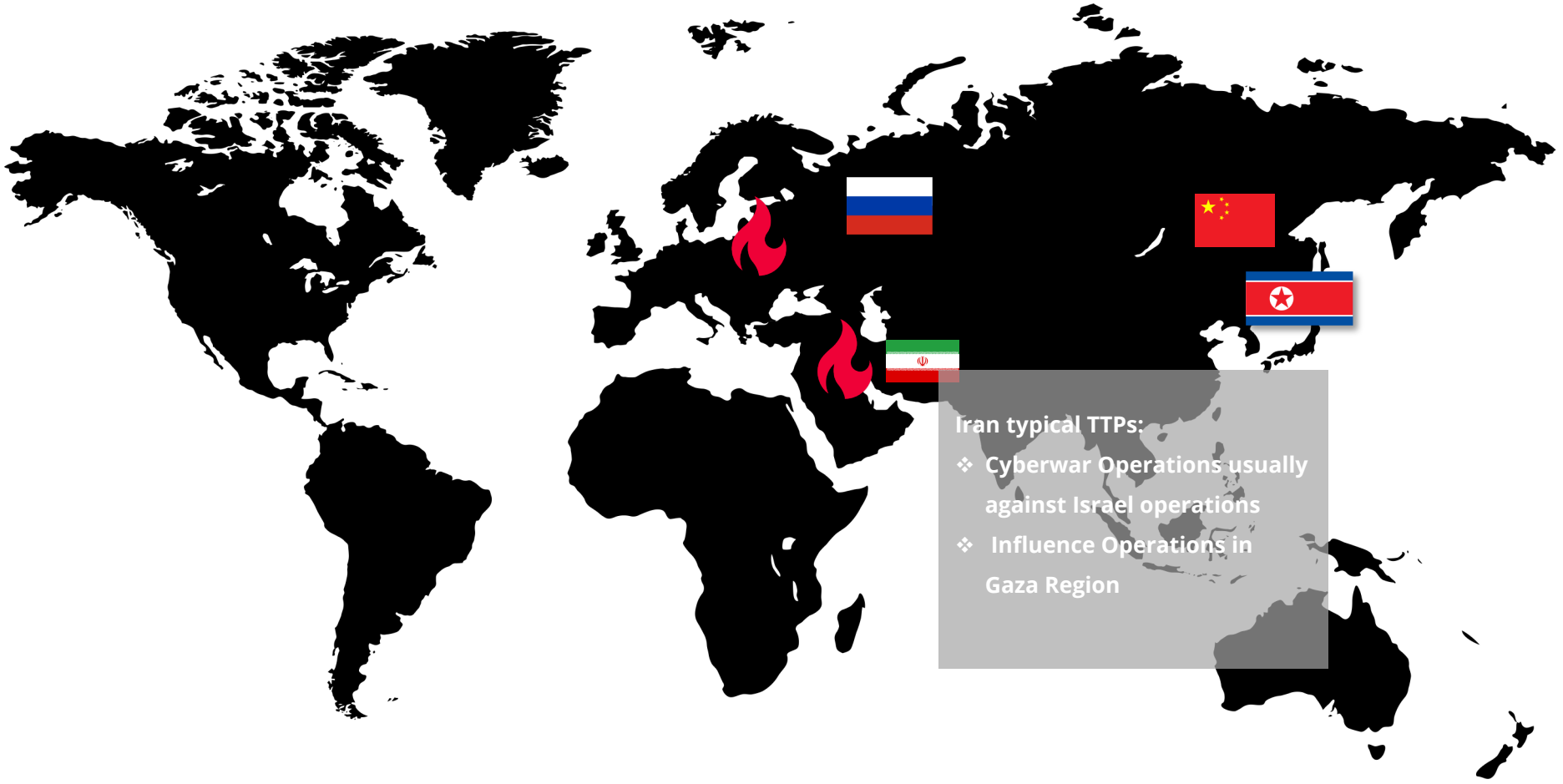
The Threat Landscape – The Big Four



The Threat Landscape – The Big Four

The Threat Landscape – The Big Four

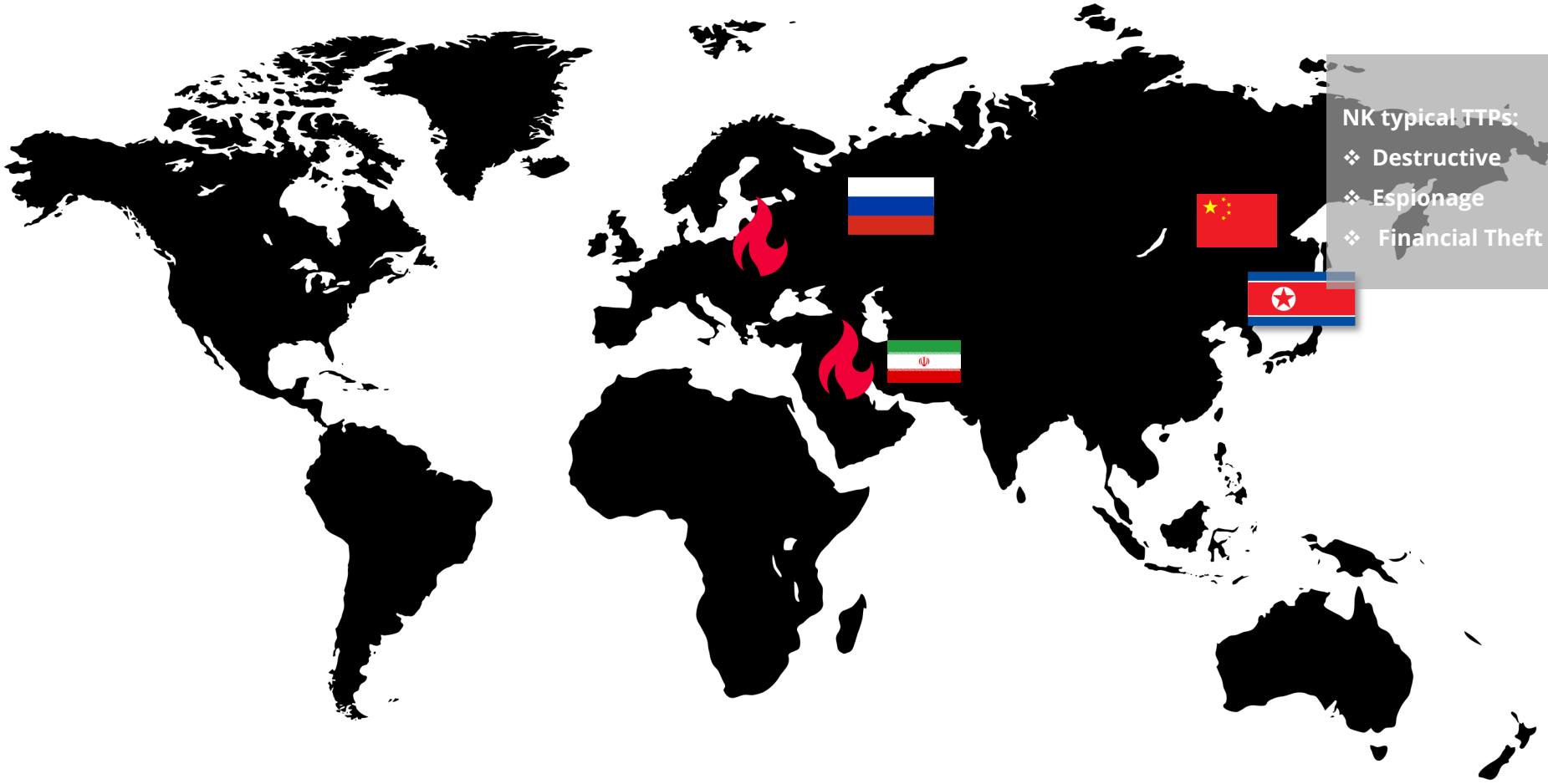
The Threat Landscape – The Big Four



Iran typical TTPs:

- **Cyberwar Operations usually against Israel operations**
- **Influence Operations in Gaza Region**

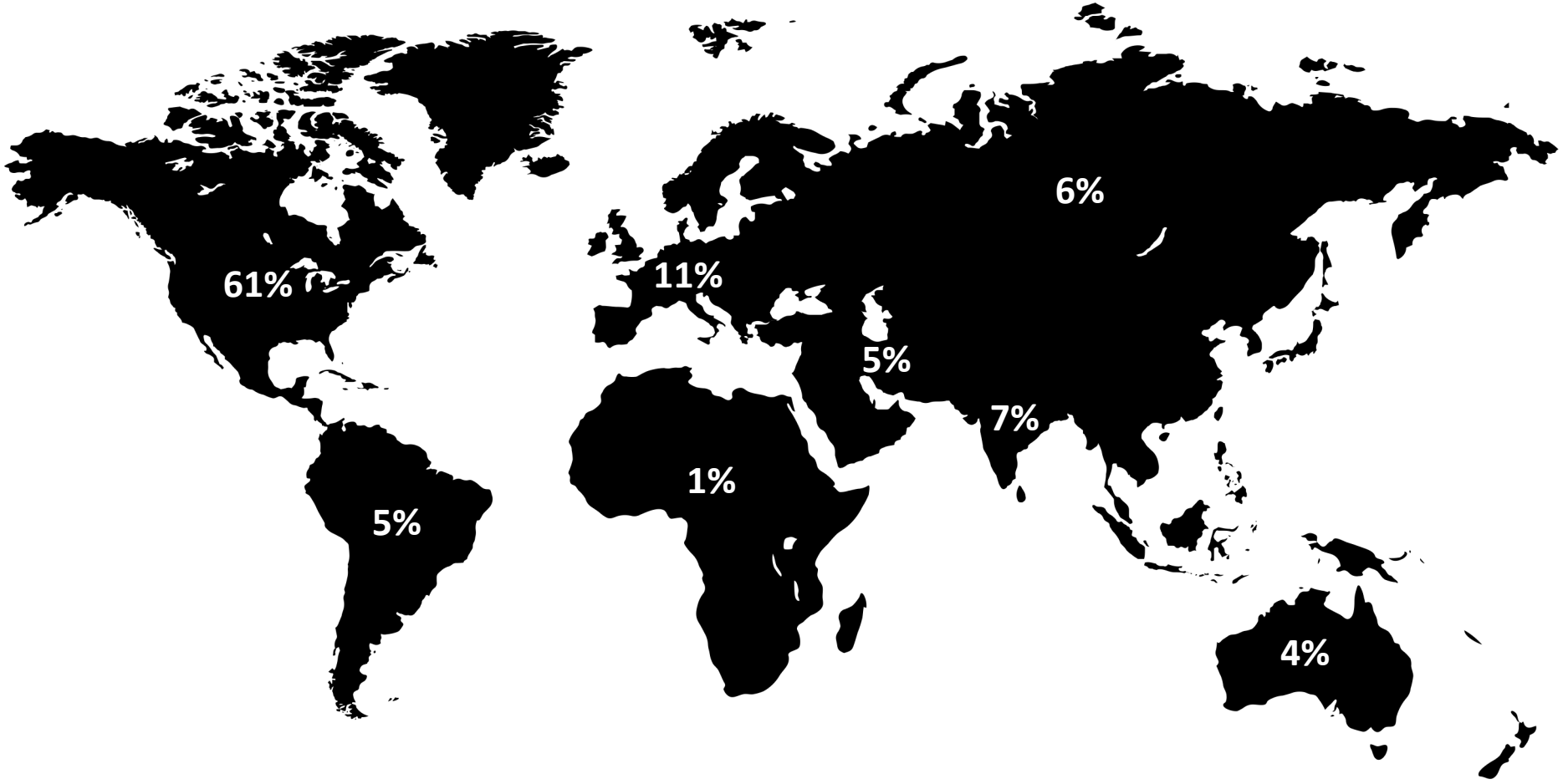
The Threat Landscape – The Big Four

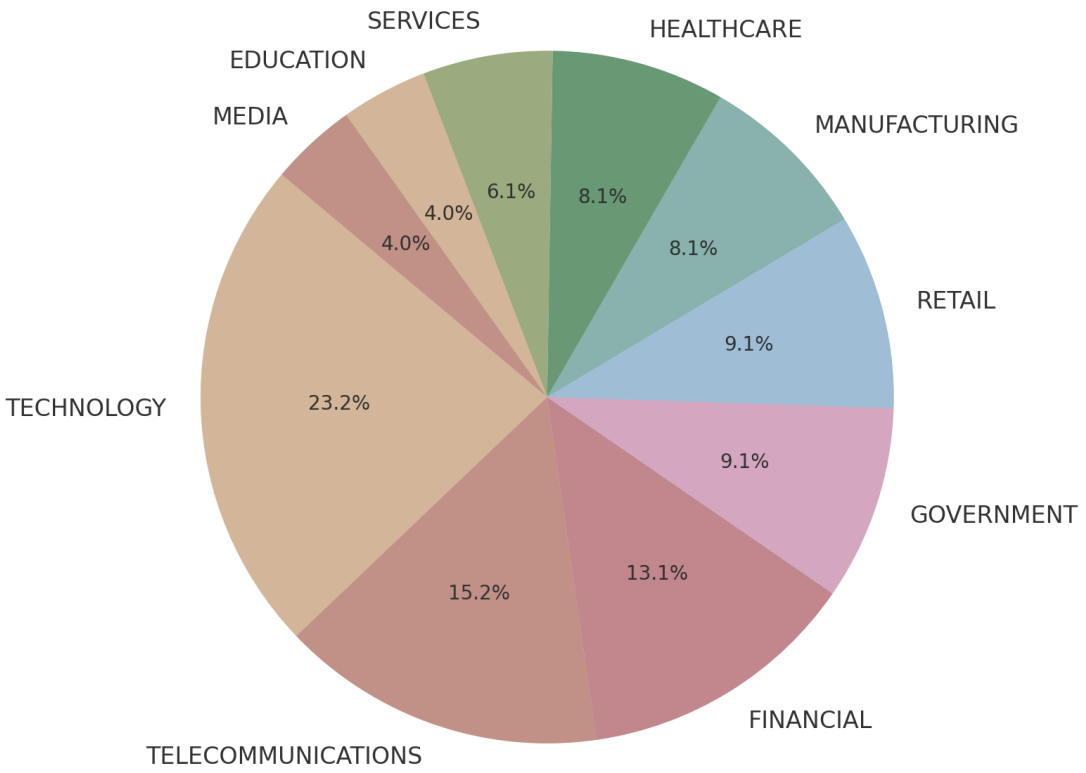


NK typical TTPs:

- **Destructive**
- **Espionage**
- **Financial Theft**

The Threat Landscape – Percentage of Attacks in Geos



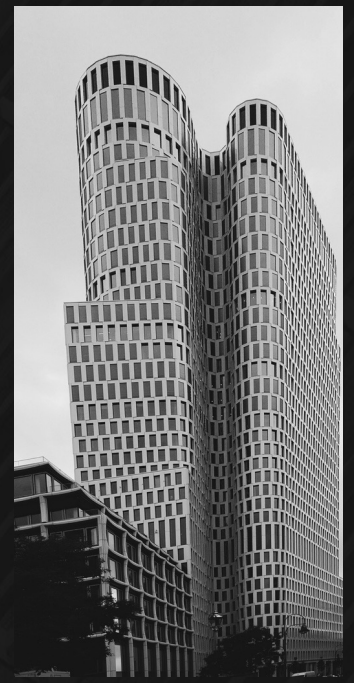


Most Targeted Industries

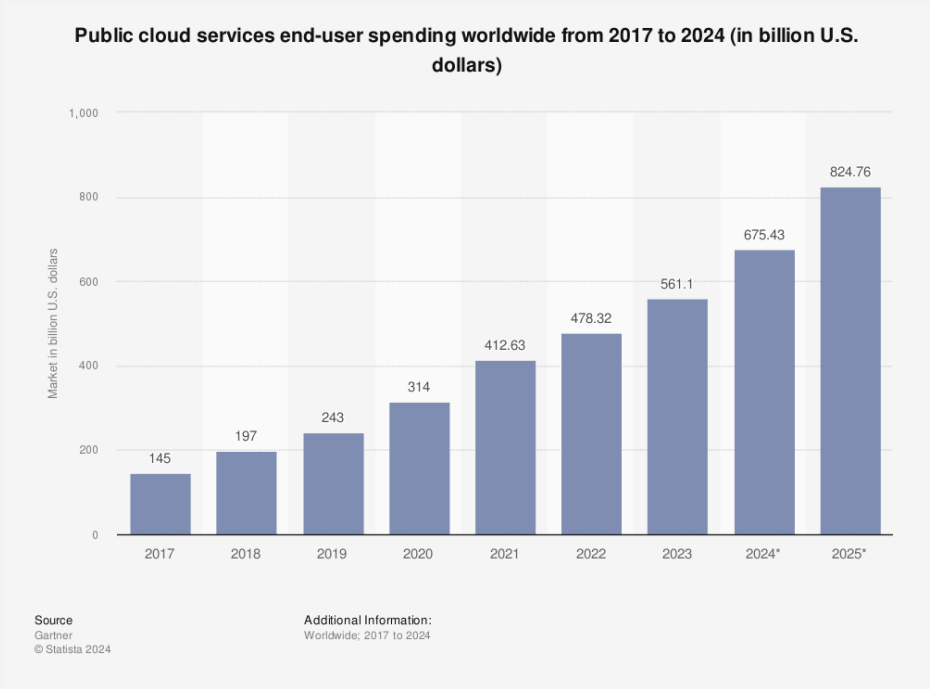
- Global average cost of a successful intrusion**: USD 4.45M**
- **Healthcare has the highest average costs**, followed by Financial, Energy and Technology
- **Phishing** and compromised credentials were the **most common initial attack vectors**
- **Espionage operations increase** and destructive operations decline
- Global Average time to detect and contain a breach up to **277 days (up to 291 in multicloud envrionments)**

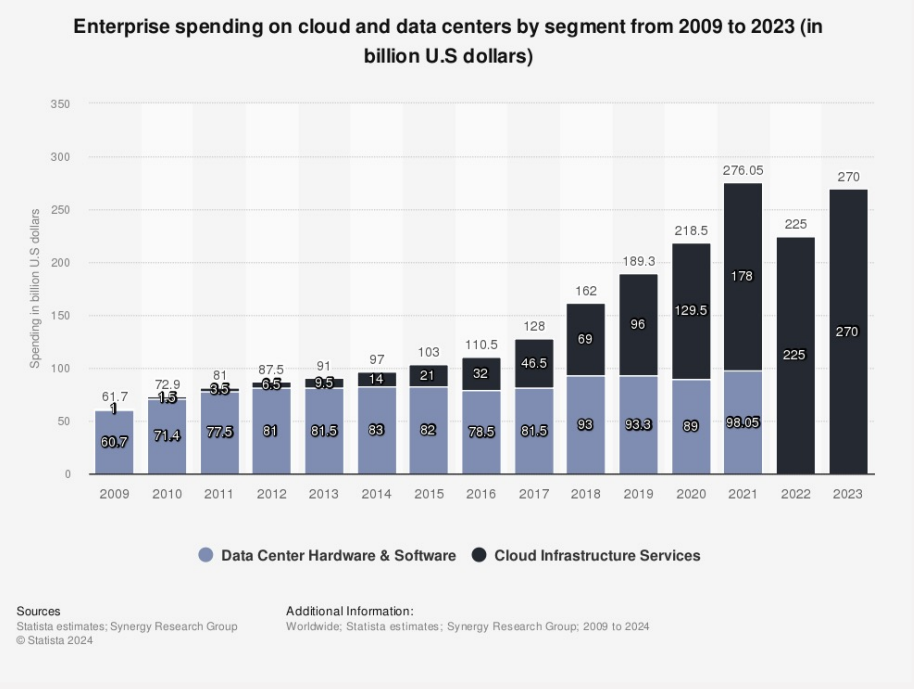
(*Sources: Crowdstrike Threat Report 2023 & Microsoft Threat Report 2023)

Why is Cloud Security so important nowadays?



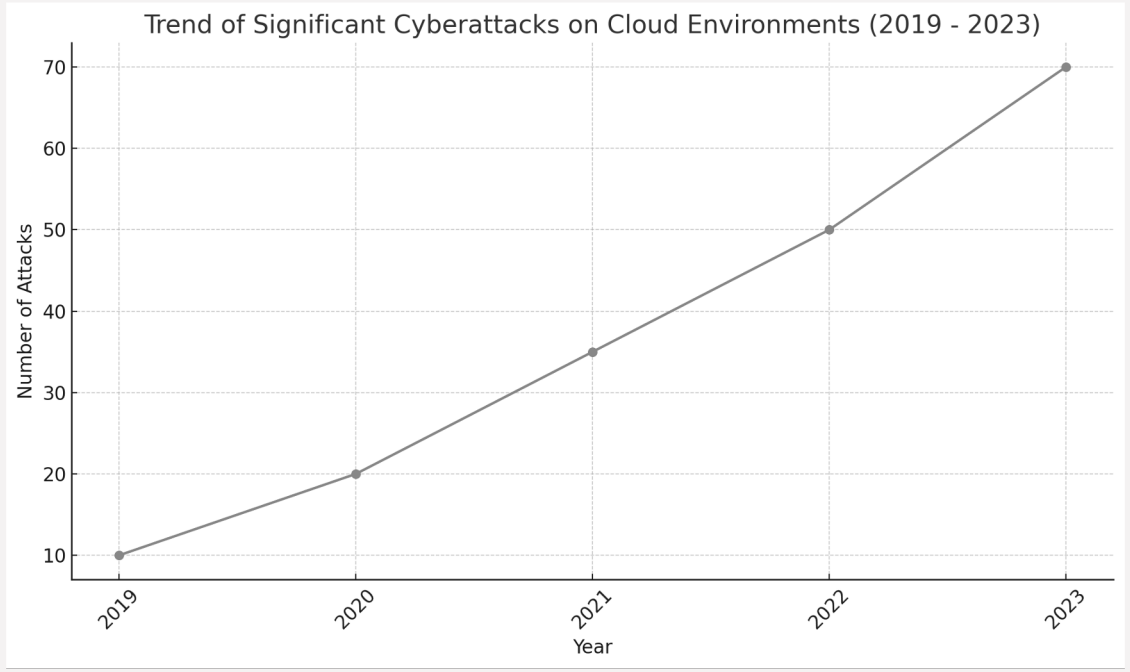
Cloud adoption goes constantly up





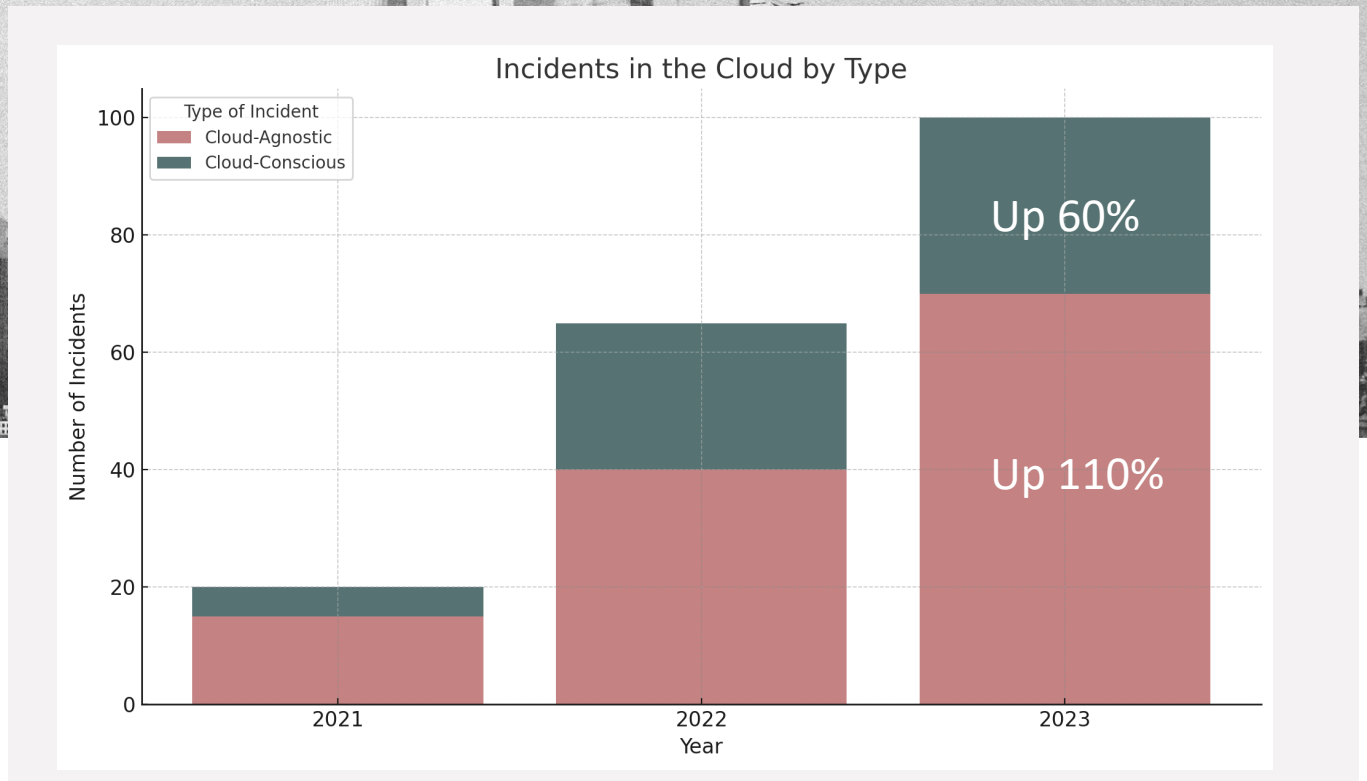
(*Source: https://www.statista.com)

Significant cloud attacks go constantly up



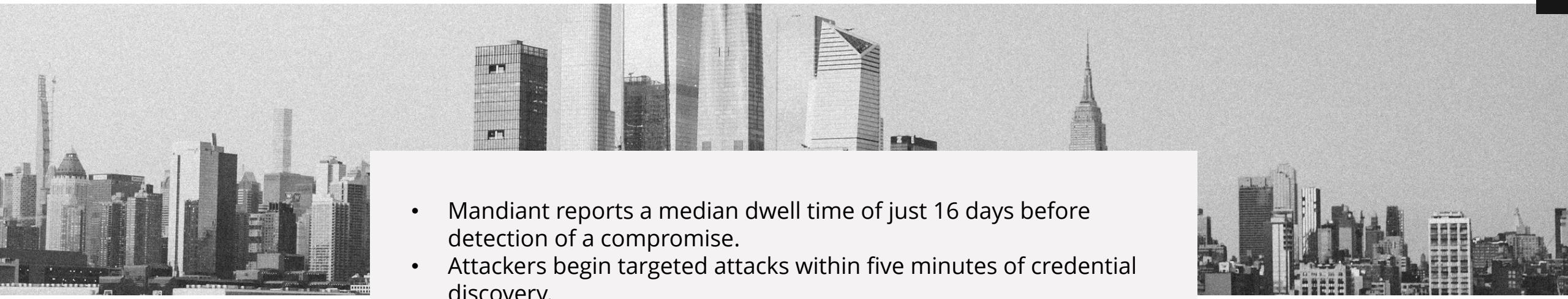
(*Source: https://www.csis.org 2024)

Significant cloud attacks go constantly up



(*Source: Crowdstrike Threat Report 2023)

Cloud attacks happen more automated & faster



- Mandiant reports a median dwell time of just 16 days before detection of a compromise.
- Attackers begin targeted attacks within five minutes of credential discovery.

(*Source: https://sysdig.com/blog/ , August 2023, Mandiant Threat Report 2023)

Some non-nation-state APTs specialized on cloud

Known Cloud Threat Actors

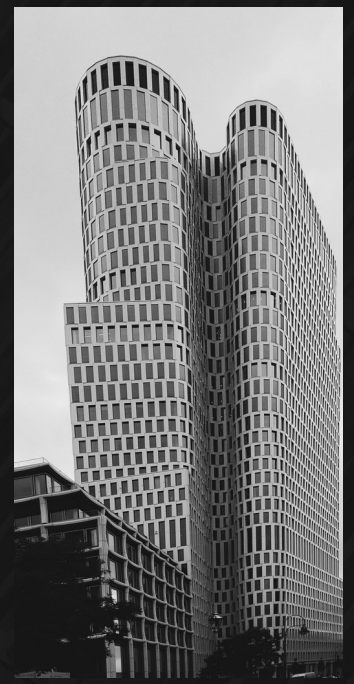
- TeamTNT
- WatchDog
- Kinsing
- Rocke
- 8220

Usual Goals:

1. Cryptojacking
2. Data Exfiltration (financial gain)
3. Sabotage (DDoS etc.)

(*Source: https://sysdig.com/blog/ , August 2023, Mandiant Threat Report 2023)

How can this be approached at industry scale?



Five latest real-life examples

1. LastPass Breach (2022)
2. Operation Cloud Hopper (2017)
3. Captial One Breach (2019)
4. Solar Winds Breach (2022)
5. Microsoft Cosmos DB Breach (2021)

MITRE ATT&CK

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact

LastPass Breach

- **Initial Access:**
  social engineering/ spear phishing
  To compromise developer account for development environment access.

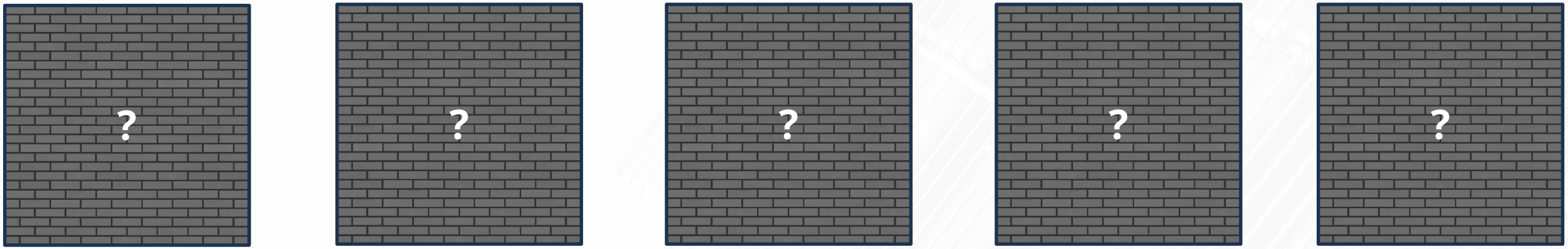
- **Execution:**
  Exploit of unpatched “Plex Vulnerability” on Developer Device

- **Lateral Movement**
  Using the compromised credentials, the attackers infiltrated the AWS S3 storage, which housed encrypted customer vault data and other sensitive information.

- **Exfiltration:**
  Once inside, the attackers were able to exfiltrate encrypted vault data, which, if decrypted, could potentially expose user passwords and other sensitive information.

- **Persistence:**
  The attackers maintained undetected access for an extended period of several months, performing enumeration and information gathering for second stage

Cloud Security at Scale - Level 1



How it could have been prevented

1. Role-Based/ (Attribute-Based) Access Control (RBAC)
2. Multi-Factor Authentication (MFA)
3. Privileged Access Management (PAM)
4. Vulnerability/Patch Management
5. Network Segmentation
6. Encryption and Key Management
7. Continuous (Anomaly) Monitoring and Logging
8. Regular Security Audits and Penetration Testing
9. Secure Development Practices
10. Incident Response Planning

Operation Cloud Hopper

Initial Access:

Attackers from APT10 first gained access to the networks of managed service providers (MSPs) through **phishing emails**

Execution:

Leveraging Remote Access Trojans (RAT) like PlugX, Poison Ivy, ChChes, and Graftor send to MSPs clients

Lateral Movement:

Using the compromised MSP credentials, the attackers infiltrated the cloud environments of various MSP clients, gaining access to sensitive data stored on cloud servers.

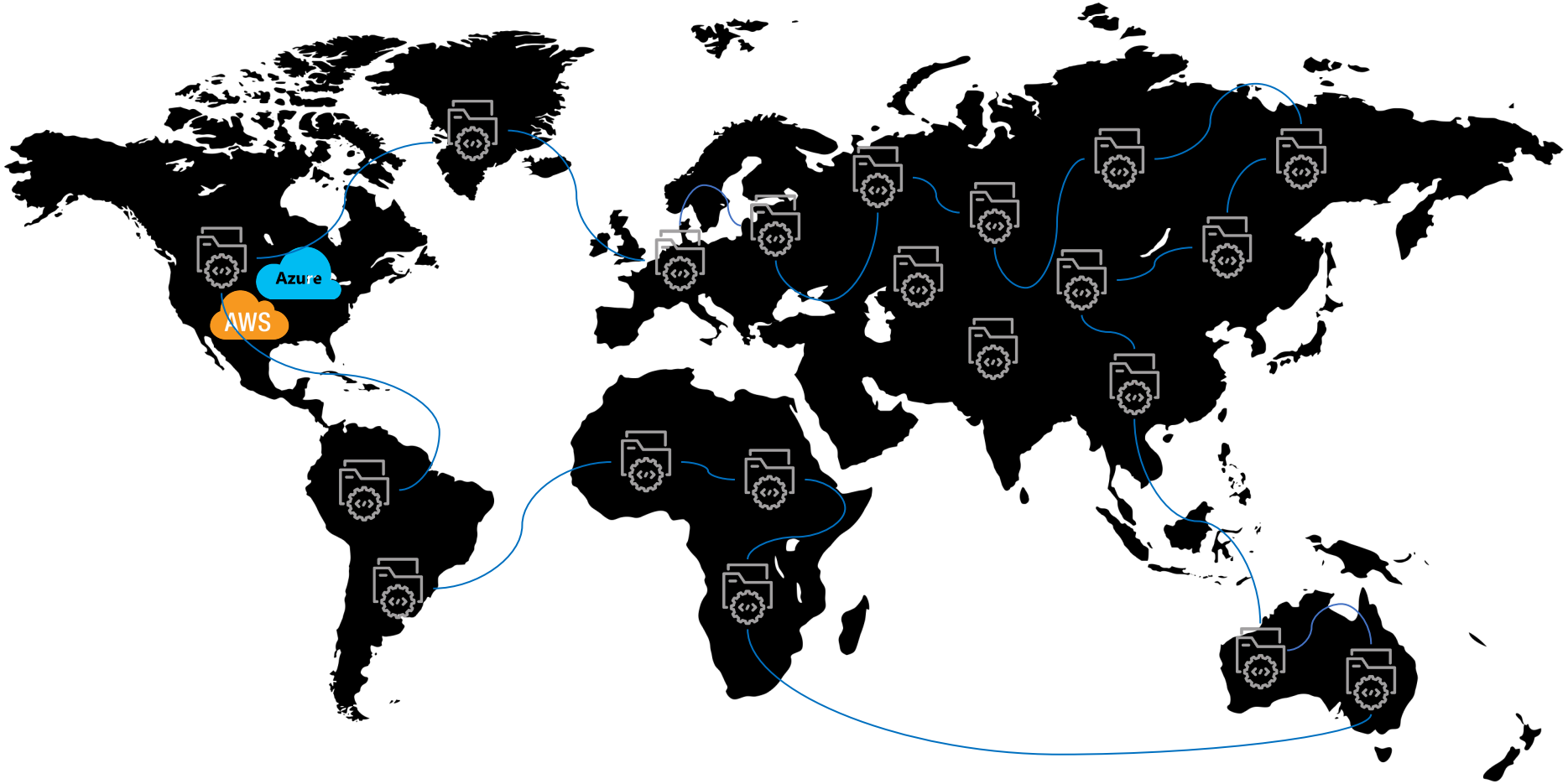
Exfiltration:

Once inside the targeted networks, the attackers were able to exfiltrate sensitive data, including intellectual property, business communications, and personal information from numerous organizations cloud environments.

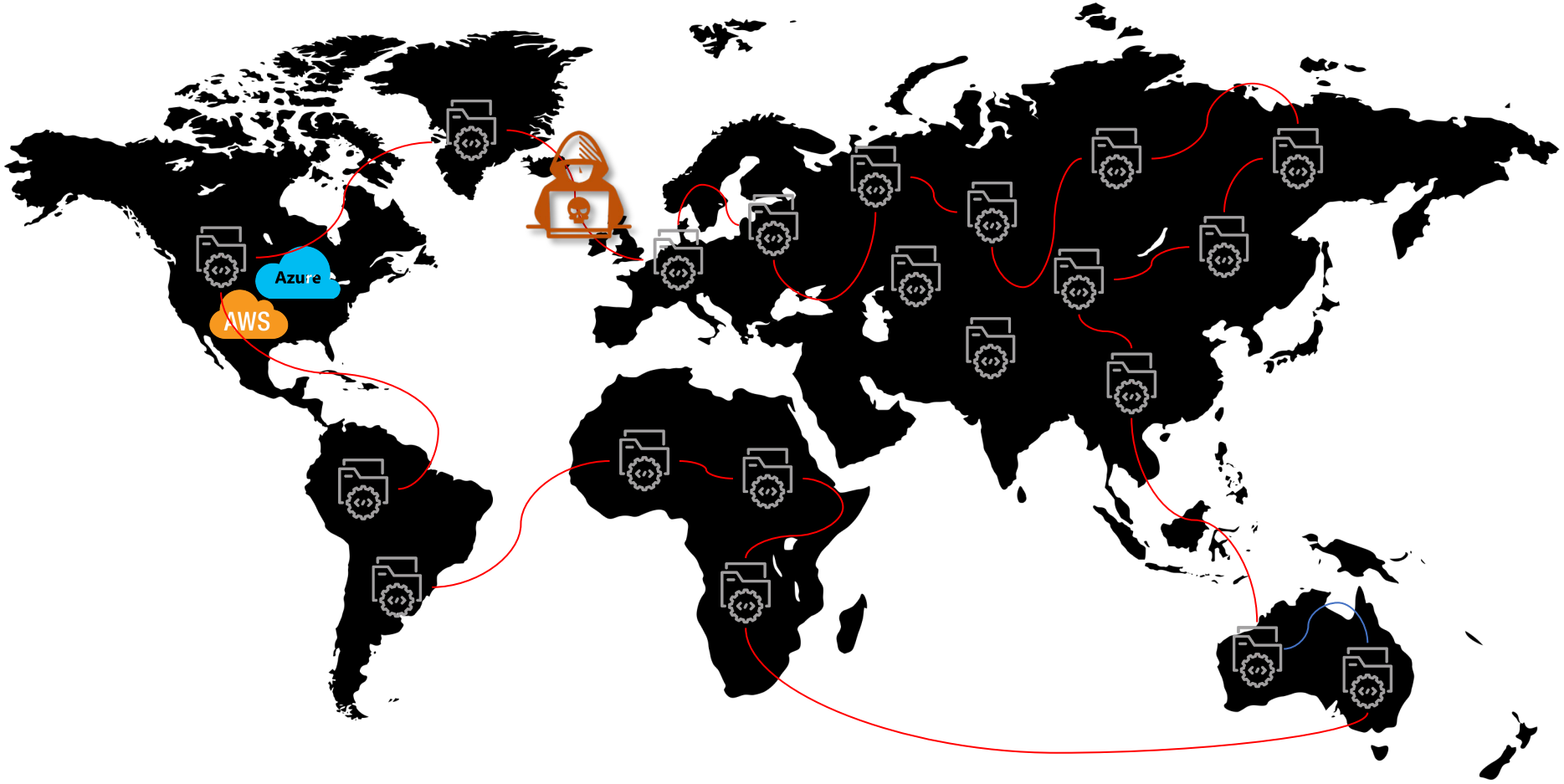
Persistence:

The attackers maintained undetected access for extended periods, using their foothold in MSP networks to pivot into customer systems and continuously harvest data.

The Threat Landscape – Supply Chain Attacks



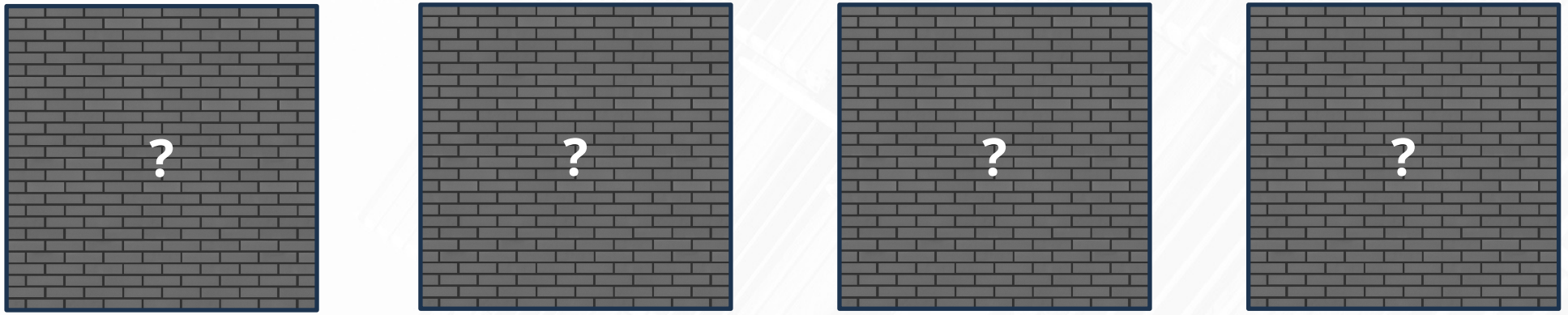
The Threat Landscape – Supply Chain Attacks



Cloud Security at Scale - Level 2

Role-Based/ Attribute-Based Access Control (RBAC)

Multi-Factor Authentication (MFA)



How it could have been (partially) prevented

1. Third-Party Risk Management
2. Secure Software Integrity Checks
3. Multi-Factor Authentication (MFA)
4. Least Privilege Access
5. Data Encryption and Secure Key Management
6. Network Segmentation
7. Continuous Monitoring and Anomaly Detection
8. Supply Chain Transparency and Communication
9. Regular Security Audits and Assessments
10. Security Awareness and Training

Capital One Breach

Initial Access:

The (individual, no nation-state) attacker exploited a misconfigured web application firewall (WAF) that allowed unauthorized requests to internal resources, leveraging SSRF to gain initial access.

Execution:

The attacker used the SSRF vulnerability to access AWS metadata services, which exposed sensitive credentials. These credentials allowed further access to the company's infrastructure.

Lateral Movement:

Using the obtained credentials, the attacker moved laterally within Capital One's AWS environment, including accessing Amazon S3 buckets that contained sensitive data.

Exfiltration:

The attacker was able to exfiltrate data from these S3 buckets, which included approximately 100 million records containing personal information such as Social Security numbers, bank account details, and credit scores.

Persistence:

The attacker maintained undetected access over a period, allowing extensive data extraction. The breach was discovered when the attacker posted details of the stolen data on GitHub there likely used by state-sponsored actors afterwards

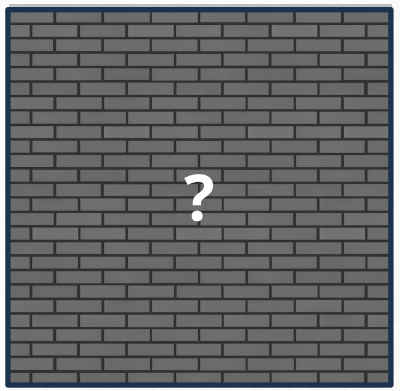
Cloud Security at Scale - Level 3

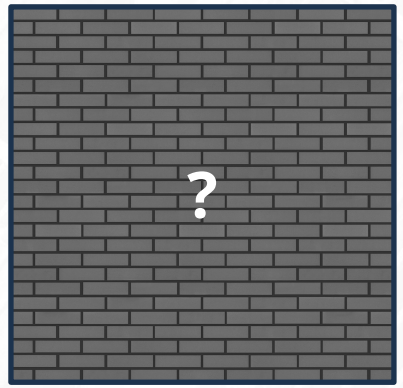
Role-Based/ Attribute-Based Access Control (RBAC)

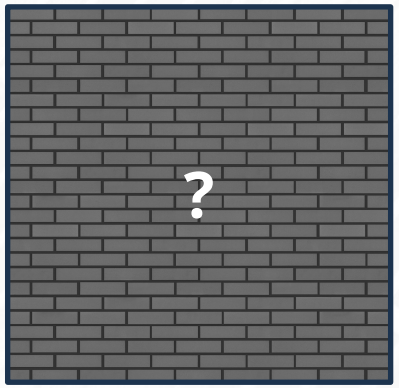
Multi-Factor Authentication (MFA)

Third Party Supplier Risk Management

Network Segmentation

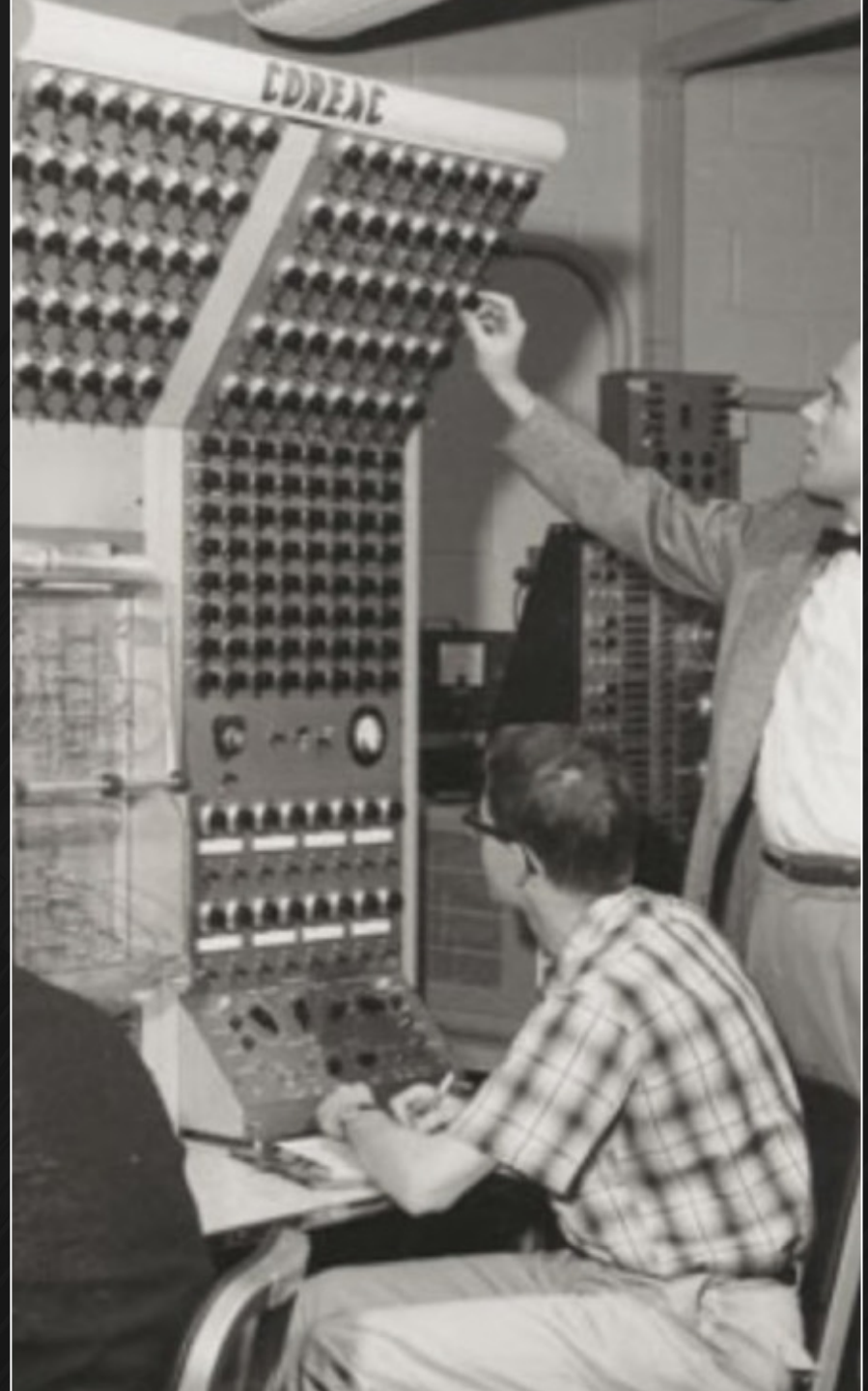






How it could have been prevented

1. Cloud Security Posture Management
2. Automation and Infrastructure as Code (IaC)
3. Continuous Monitoring and Compliance
4. Secure Coding Practices (Input Validation)
5. API Security Best Practices
6. Centralized Management and Governance
7. Role-Based Access Control (RBAC) and Multi-Factor Authentication (MFA)
8. Configuration Drift Management
9. Incident Response and Recovery Plans



SolarWinds Attack

Initial Access:

APT29 (Cozy Bear) compromised the SolarWinds software development environment, inserting malicious code into Orion software updates.

Execution:

The compromised updates contained Sunburst malware, creating a backdoor for attackers in systems that installed the updates.

Lateral Movement:

Attackers used the Sunburst backdoor to move laterally within networks, accessing sensitive data and systems, including cloud environments.

Exfiltration:

Data including emails and documents were exfiltrated. Attackers targeted high-value information and mimicked legitimate traffic to avoid detection.

Persistence:

The attackers maintained access for 6 – 12 months, using techniques like disabling security tools and legitimate credentials to evade detection.

Cloud Security at Scale - Level 4

Role-Based/ Attribute-Based Access Control (RBAC)

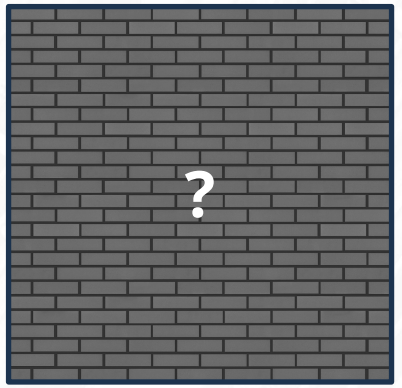
Multi-Factor Authentication (MFA)

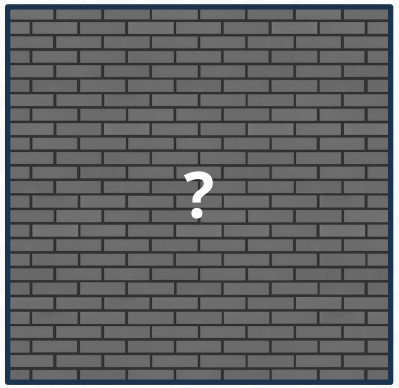
Third Party Supplier Risk Management

Network Segmentation

Centralized Configuration Management

Automation & Infrastructure as Code





How it could have been (partially) prevented

1. Third-Party Risk Management
2. Secure Software Integrity Checks
3. Multi-Factor Authentication (MFA)
4. Least Privilege Access
5. Data Encryption and Secure Key Management
6. Network Segmentation
7. Continuous Monitoring and Anomaly Detection
8. Supply Chain Transparency and Communication
9. Regular Security Audits and Assessments
10. Security Awareness and Training

Microsoft Cosmos DB Breach

Initial Access:

Attackers exploited a misconfiguration in the Jupyter Notebook feature of Azure Cosmos DB, auto-enabled without customer notification, allowing access to sensitive data and controls.

Execution:

The misconfiguration allowed privilege escalation, giving attackers access to secrets, including certificates and private keys, providing admin access to multiple Cosmos DB accounts.

Lateral Movement:

With obtained credentials, attackers accessed management panels of various Cosmos DB accounts, enabling them to manipulate sensitive customer data.

Exfiltration:

While no direct data exfiltration was confirmed, the attackers could potentially access and alter critical data, including obtaining authentication tokens.

Persistence:

Attackers accessed Azure Service Fabric instances over the internet, maintaining persistent access without further notice in the beginning. Attackers could have been month up to years persistent in client systems.

Cloud Security at Scale - Level 5

Role-Based/ Attribute-Based Access Control (RBAC)

Multi-Factor Authentication (MFA)

Third Party Supplier Risk Management

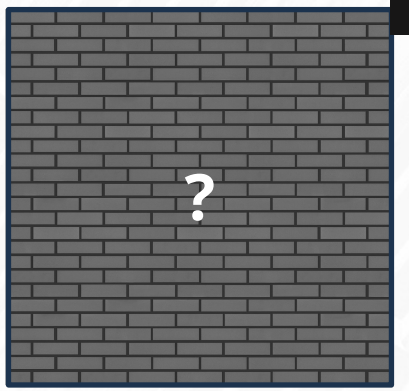
Network Segmentation

Centralized Configuration Management

Automation & Infrastructure as Code

Vulnerability & Patch Management

SBOM



How it could have been (partially) prevented

1. Third-Party Risk Management
2. Security Testing (Penetration Testing)
3. Multi-Factor Authentication (MFA)
4. Least Privilege Access
5. Data Encryption and Secure Key Management
6. Network Segmentation
7. Continuous Monitoring and Anomaly Detection
8. Supply Chain Transparency and Communication
9. Regular Security Audits and Assessments
10. Security Awareness and Training

My Key Insights

4

Role-Based/ Attribute-Based Access Control (RBAC)

Multi-Factor Authentication (MFA)

Third Party Supplier Risk Management

Network Segmentation

Centralized Configuration Management

Automation & Infrastructure as Code

Vulnerability & Patch Management

SBOM

Encryption & Secrets Management

SDLC (esp. Testing)

My Key Insights

4

Proper Identity and Access Management

Threat & Risk Management (& BIA)

Configuration Management & SDLC

Vulnerability Management

Encryption & Network Segmentation

My Key Insights

Maturity

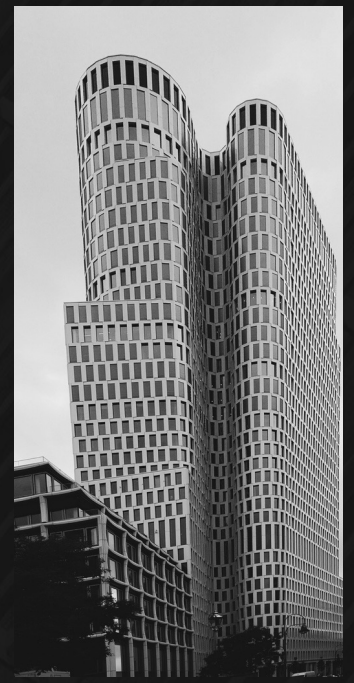
PAM	Anomaly Detection (AI)	Regular Audits, Central Policies (SCPs)	Automated Remediation	DLP, Confidential Computing
Federation (for External Connections)	Integrity Checking, Code Signing	API Security, Input Validation	SBOM, Continuous Monitoring	Data Classification
MFA, ABAC, RBAC	Third Party Supplier Security Checks	Drift Detection, Templates, hard. Images	Security Testing, Penetration Testing	Micro-Segmentation
Least Privilege Enforcement	Threat Modelling	SCA, SAST, DAST	CSPM, CNAPP	Zero Trust
Proper Identity and Access Management	**Threat & Risk Management (& BIA)**	**Configuration Management & SDLC**	**Vulnerability Management**	**Encryption & Network Segmentation**

My Key Insights

Maturity

Training & Awareness				
PAM	Anomaly Detection (AI)	Regular Audits, Central Policies (SCPs)	Automated Remediation	DLP, Confidential Computing
Federation (for External Connections)	Integrity Checking, Code Signing	API Security, Input Validation	SBOM, Continuous Monitoring	Data Classification
MFA, ABAC, RBAC	Third Party Supplier Security Checks	Drift Detection, Templates, hard. Images	Security Testing, Penetration Testing	Micro-Segmentation
Least Privilege Enforcement	Threat Modelling	SCA, SAST, DAST	CSPM, CNAPP	Zero Trust
Proper Identity and Access Management	**Threat & Risk Management (& BIA)**	**Configuration Management & SDLC**	**Vulnerability Management & Testing**	**Encryption & Network Segmentation**

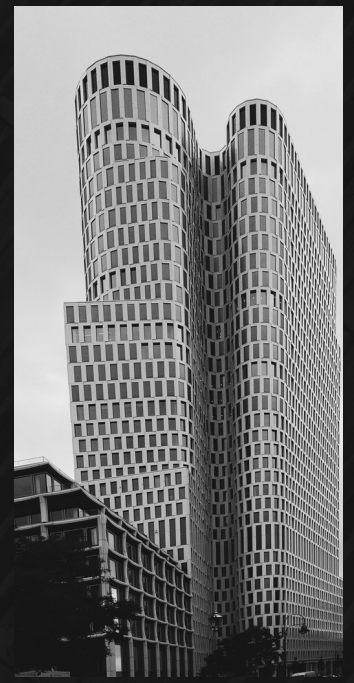
Key Takeaways



Key Takeaways

Basic Hygiene could protect 99% of cloud attacks:

- MFA
- Regular Updates
- Sensitive Data Encryption
- Monitoring



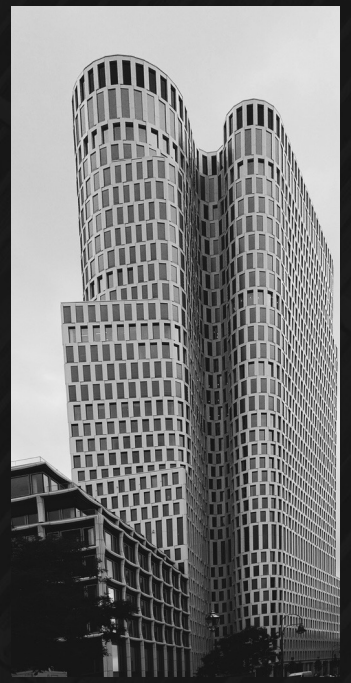
Key Takeaways

Basic Hygiene could protect 99% of cloud attacks:

- MFA
- Regular Updates
- Sensitive Data Encryption
- Monitoring
- Least Privilege

Supply chain attacks and exploitation of trusted software allow adversaries to maximize their ROI/Impact of attacks

→ one of the biggest challenges in Cloud Security and needs to be addressed



Key Takeaways

Basic Hygiene could protect 99% of APT cloud attacks:

- MFA
- Regular Updates
- Sensitive Data Encryption
- Monitoring
- Least Privilege

Supply chain attacks and exploitation of trusted software allow APT adversaries to maximize their ROI/Impact of attacks

→ one of the biggest challenges in Cloud Security and needs to be addressed

Phishing (Credential Theft) also #1 APT Attack Vector with Cloud Attacks

Key Takeaways

AI aided automated APT/Cyberwarfare activities are advancing:

- Snowflake data breach by UNC5537 (May 15, 2024)
- New York Times source code theft (June 3, 2024)
- Gitloker malicious OAuth apps (June 10, 2024)

Most active in Cyber realm:

- **North Korea**
- **Iran**
- **Russia**
- **China**

Supply chain attacks and exploitation of trusted software allow APT adversaries to maximize their ROI/Impact of attacks

→ one of the biggest challenges in Cloud Security and needs to be addressed

Phishing (Credential Theft) also #1 APT Attack Vector with Cloud Attacks

Key Takeaways

Basic Hygiene could protect 99% of APT cloud attacks:

- MFA
- Regular Updates
- Sensitive Data Encryption
- Monitoring
- Least Privilege

Most active in Cyber realm:

- **North Korea**
- **Iran**
- **Russia**
- **China**

A **proper security baseline** can be the Foundation for higher security maturity

Supply chain attacks and exploitation of trusted software allow APT adversaries to maximize their ROI/Impact of attacks

→ one of the biggest challenges in Cloud Security and needs to be addressed

Phishing (Credential Theft) also #1 APT Attack Vector with Cloud Attacks

Final Thought

Final Thought

Cyberwarfare is a distant threat, relevant only to military, governmental entities and critical infrastructure providers

What do you think?

References & Further Reads

Capital One

1. https://dl.acm.org/doi/10.1145/3546068
2. https://techmonitor.ai/technology/cybersecurity/capital-one-hack-aws-paige-thompson
3. https://www.capitalone.com/digital/facts2019/
4. https://owasp.org/Top10/A10_2021-Server-Side_Request_Forgery

Solar Winds:

1. https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know
2. https://www.spektrum.de/news/solarwinds-ein-hackerangriff-der-um-die-welt-geht/1819187
3. https://ieeexplore.ieee.org/abstract/document/9579611

Microsoft Chaos DB:

1. https://securityaffairs.com/124510/hacking/chaosdb-flaw-technical-details.html
2. https://msrc.microsoft.com/blog/2021/08/update-on-vulnerability-in-the-azure-cosmos-db-jupyter-notebook-feature/

Cloud Hopper:

1. https://www.trendmicro.com/vinfo/de/security/news/cyber-attacks/operation-cloud-hopper-what-you-need-to-know
2. https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/

LastPass:

1. https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-pandemic-eleven-deep-dive
2. https://www.keepersecurity.com/blog/de/2022/12/23/lastpass-breach-what-you-should-know
3. https://blog.lastpass.com/posts/2023/03/security-incident-update-recommended-actions

Statistics

1. https://sysdig.com/blog/2023-global-cloud-threat-report/
2. https://go.crowdstrike.com/global-threat-report-2024
3. https://www.breaches.cloud
4. https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/targeted-attacks-six-components
5. https://services.google.com/fh/files/misc/m-trends-2024.pdf
6. https://www.cisa.gov
7. https://www.rand.org/topics/cyber-warfare.html
8. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
9. https://cert.europa.eu
10. https://unit42.paloaltonetworks.com

Might be Interesting:

1. https://attack.mitre.org/#
2. https://learning.oreilly.com/library/view/software-supply-chain/
3. Comprehensive Study on APTs:
4. https://link.springer.com/article/10.1007/s11227-016-1850-4#Sec10
5. https://www.arcserve.com/blog/
6. https://www.armis.com/newsroom/press/armis-state-of-cyberwarfare-and-trends-report-2022-2023-highlights-global-it-and-security-professionals-sentiment-on-cyberwarfare/
7. https://www.bmi.bund.de/DE/themen/sicherheit/spionageabwehr-wirtschafts-und-geheimschutz/wirtschaftsschutz/wirtschaftsschutz-node.html