Cyber Threat Inform Your Board
Brussels Cybersecurity Summit

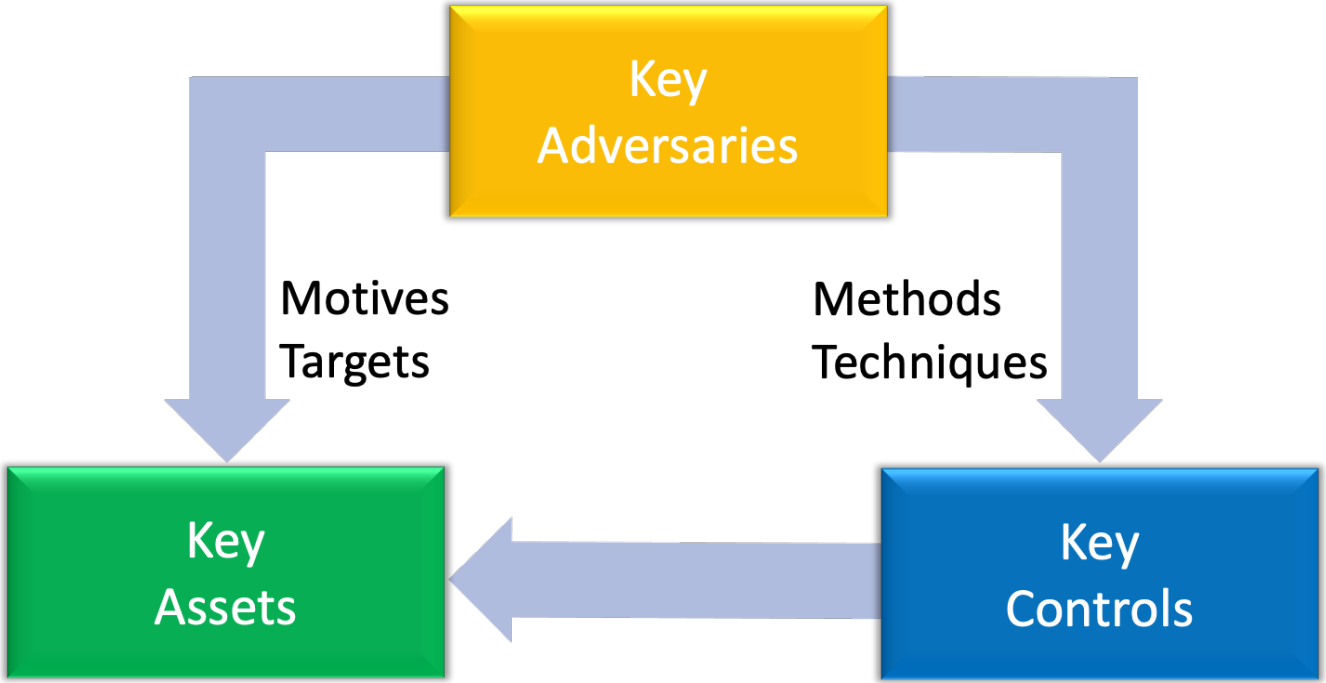
Freddy Dezeure

CT *Intelligence*

CT *Intelligence?*

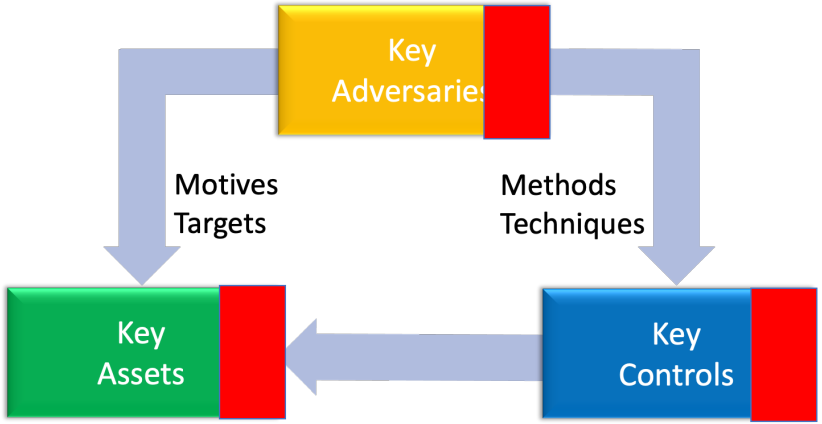
CT *Inform*

CTI Serves To Mitigate Risk



CT *Inform Your Defense*

CT Inform Your Defense



Resilience

Test

Observe

Prevent

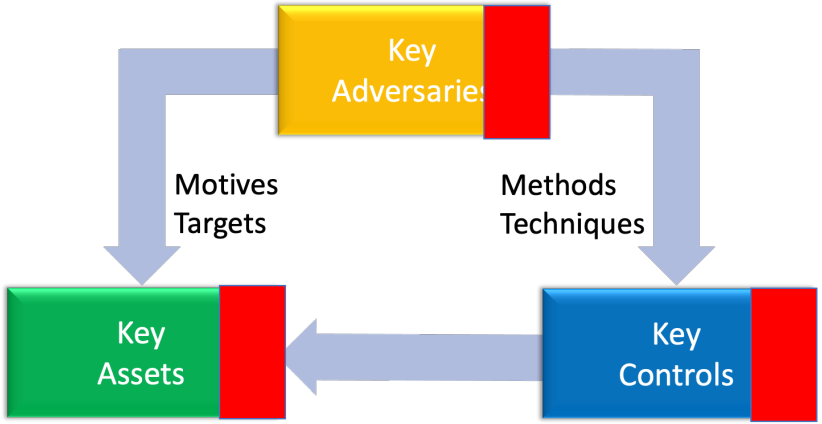
Detect

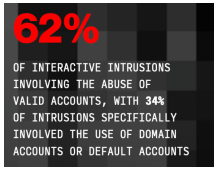
Respond

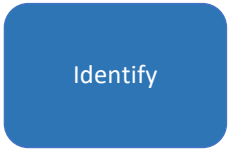
Identify

Test

Current Threat – Credential/Token Theft







CT *Inform Your Board*

Ten Key Insights For Informed Cyber Oversight

1. Evidence rather than compliance
2. Reporting KCIs rather than everything (or KPIs)
3. Threat-informed rather than stale
4. Priorities rather than averages
5. Reporting gaps rather than “all green”
6. Embedded rather than disconnected
7. Transparency of deviations rather than acceptance
8. Risk appetite rather than zero risk
9. Telling the story – risk connection to services
10. Unify cyber regulations – apply selective ‘gold-plating’

Sample Key Controls and KCIs		
KCI 1	Asset Inventory	% assets in the inventory within policy
KCI 2	Privileged accounts	% privileged accounts managed within policy
KCI 3	Timely patching	% high risk patches within N hours # of known exploited vulnerabilities detected
KCI 4	Back-up	Maximum time to recover key assets (% of critical assets recoverable in N hours)
KCI 5	Endpoint protection	% endpoints configured in line with policy
KCI 6	Logs collection	% critical systems onboarded to log collection
KCI 7	Network security	% compliant key network security configurations
KCI 8	Third Party compliance	% compliant key third-party connections
KCI 9	Identity management	% coverage of systems using MFA
KCI 10	Major Incidents	% major cyber incidents with business impact
KCI 11	Risk Acceptance	# risk accepted policy deviations
KCI 12	Internet exposed assets security coverage	% of Internet exposed assets covered by security monitoring and regular security assessment
KCI 13	Crown jewel coverage	% of crown jewels covered by security monitoring, vulnerability scanning and regular security assessment
KCI 14	Origin of Security Incidents	% of security incidents related to failures from at least one Key Control Indicator

Impact Of Credential/Token Theft CTI

Sample Key Controls and KCIs		
KCI 1	Asset Inventory	% assets in the inventory within policy
KCI 2	Privileged accounts	% privileged accounts managed within policy
KCI 3	Timely patching	% high risk patches within N hours # of known exploited vulnerabilities detected
KCI 4	Back-up	Maximum time to recover key assets (% of critical assets recoverable in N hours)
KCI 5	Endpoint protection	% endpoints configured in line with policy
KCI 6	Logs collection	% critical systems onboarded to log collection
KCI 7	Network security	% compliant key network security configurations
KCI 8	Third Party compliance	% compliant key third-party connections
KCI 9	Identity management	% coverage of systems using MFA
KCI 10	Major Incidents	% major cyber incidents with business impact
KCI 11	Risk Acceptance	# risk accepted policy deviations
KCI 12	Internet exposed assets security coverage	% of Internet exposed assets covered by security monitoring and regular security assessment
KCI 13	Crown jewel coverage	% of crown jewels covered by security monitoring, vulnerability scanning and regular security assessment
KCI 14	Origin of Security Incidents	% of security incidents related to failures from at least one Key Control Indicator

Sample Board Report

INCIDENTS

4 significant incidents affected EUIBAs this quarter.
In 3 cases the attack started with a compromise of a publicly accessible server (Oracle WebLogic, Microsoft Exchange).

In the other case, attackers obtained credentials via a phishing campaign.

In at least 3 significant incidents, threat actors successfully exfiltrated data.

Since the beginning of 2021, CERT-EU has already recorded 15 significant incidents, compared to 13 during the whole of 2020 and 8 in 2019.

THREATS

CERT-EU released 26 threat alerts (compared to 20 during Q1 and 22 in Q2).
The top 5 reasons for threat alerts were:

- Active exploitation of zero-days or n-days: Microsoft Exchange, VPNs, etc.
- Recent activity or new tools used by top threat actors
- Sharing actionable data related to TTPs used in significant incidents
- Spear-phishing campaigns directly affecting EUIBAs or sectors of interest
- Active use of commercial mobile spyware

K1	K2	K3	K4	K5
85%	100%	90%	80%	95%

K6	K7	K8	K9	K10
95%	100%	100%	100%	95%

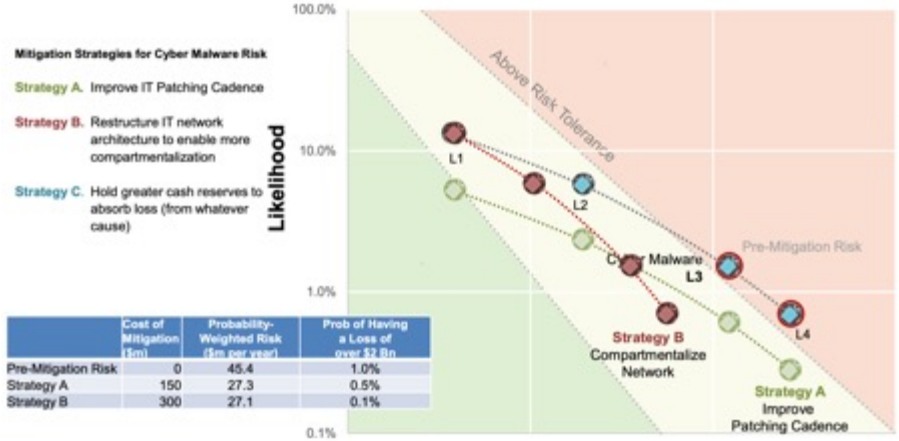
Who?	Group / Malware?	Why?	Trend
Adversary 1	APTX	Adversary known to steal intellectual property in high tech industry.	→
Adversary 2	APTY	State sponsored actor known targeting critical infrastructure	↗
Adversary 3	FINX	Ransomware actor increasingly prevalent and sophisticated	↗

Mitigation Strategies for Cyber Malware Risk

Strategy A. Improve IT Patching Cadence

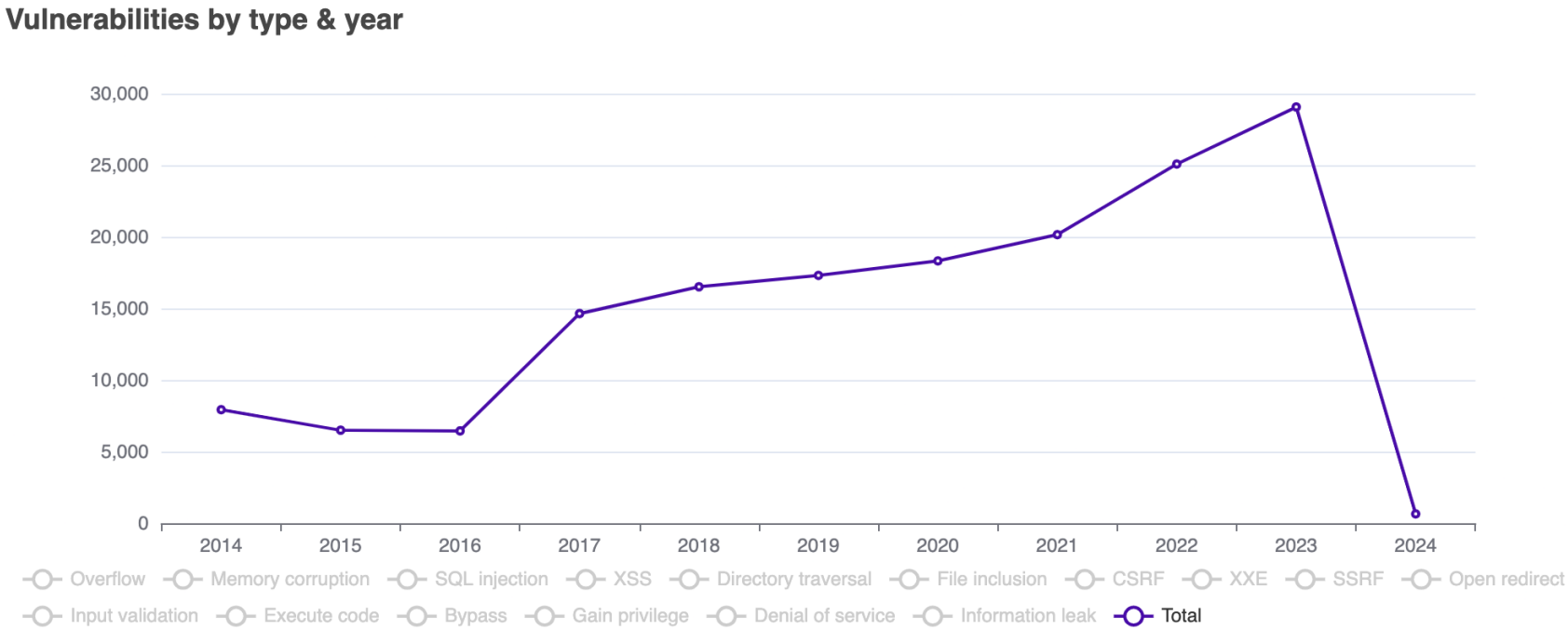
Strategy B. Restructure IT network architecture to enable more compartmentalization

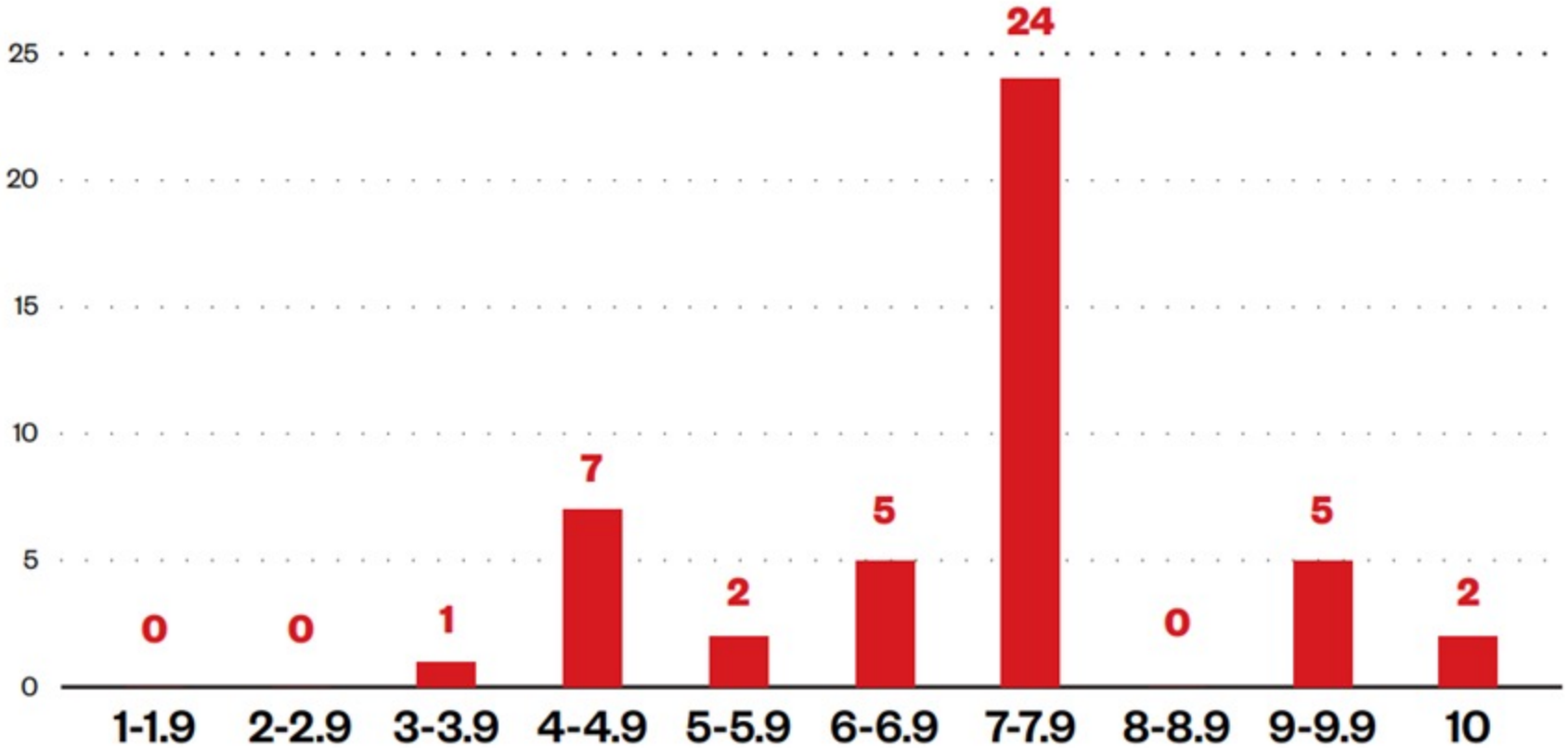
Strategy C. Hold greater cash reserves to absorb loss (from whatever cause)



	Cost of Mitigation ($m)	Probability-Weighted Risk ($m per year)	Prob of Having a Loss of over $2 Bn
Pre-Mitigation Risk	0	45.4	1.0%
Strategy A	150	27.3	0.5%
Strategy B	300	27.1	0.1%

Vulnerability Management





CVSS severity scores of the CVEs exploited by the top five ransomware groups

Credit TrendMicro 2023

Security Vulnerabilities, CVEs, in CISA KEV Catalog

Published in: 2024 January

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9 In CISA KEV Catalog

Sort Results By : Publish Date Update Date CVE Number CVE Number CVSS Score EPSS Score CISA exploit add date

1068 vulnerabilities found

1 2 3 4 5 ..... 40 41 42 43 Copy

CVE-2023-41990

Known Exploited Vulnerability

The issue was addressed with improved handling of caches. This issue is fixed in tvOS 16.3, iOS 16.3 and iPadOS 16.3, macOS Monterey 12.6.8, macOS Big Sur 11.7.9, iOS 15.7.8 and iPadOS 15.7.8, macOS Ventura 13.2, watchOS 9.3. Processing a font file may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited against versions of iOS released before iOS 15.7.1.

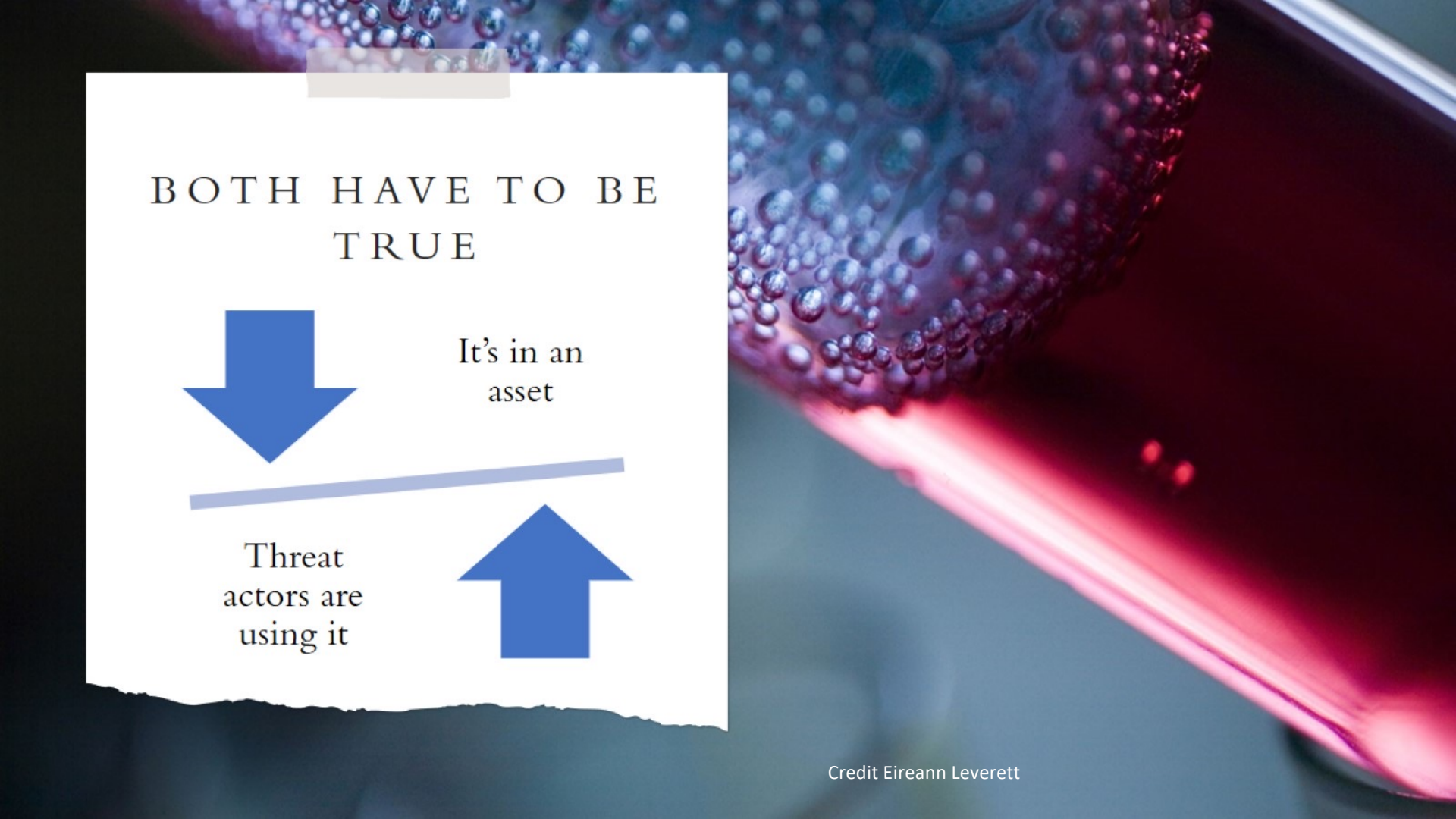
Max CVSS	7.8
Published	2023-09-12
Updated	2024-01-09
EPSS	0.07%
KEV Added	2024-01-08

CVE-2023-38203

Known Exploited Vulnerability

Adobe ColdFusion versions 2018u17 (and earlier), 2021u7 (and earlier) and 2023u1 (and earlier) are affected by a Deserialization of Untrusted Data vulnerability that could result in Arbitrary code execution. Exploitation of this issue does not require user interaction.

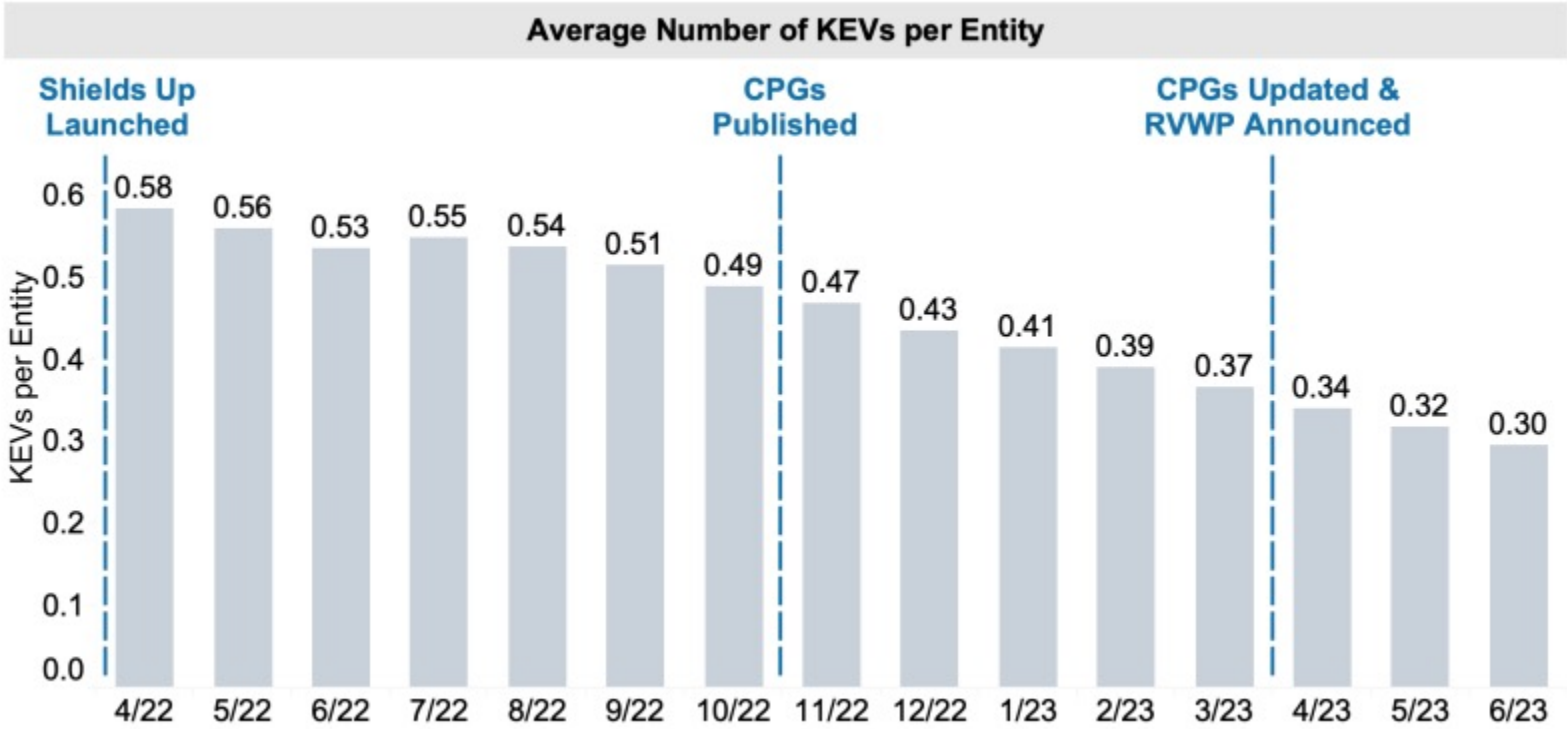
Max CVSS	9.8
Published	2023-07-20
Updated	2024-01-09
EPSS	50.97%
KEV Added	2024-01-08


BOTH HAVE TO BE TRUE
It's in an asset
Threat actors are using it
Credit Eireann Leverett

Impact Of KEV CTI

Sample Key Controls and KCIs		
KCI 1	Asset Inventory	% assets in the inventory within policy
KCI 2	Privileged accounts	% privileged accounts managed within policy
KCI 3	Timely patching	% high risk patches within N hours # of known exploited vulnerabilities detected
KCI 4	Back-up	Maximum time to recover key assets (% of critical assets recoverable in N hours)
KCI 5	Endpoint protection	% endpoints configured in line with policy
KCI 6	Logs collection	% critical systems onboarded to log collection
KCI 7	Network security	% compliant key network security configurations
KCI 8	Third Party compliance	% compliant key third-party connections
KCI 9	Identity management	% coverage of systems using MFA
KCI 10	Major Incidents	% major cyber incidents with business impact
KCI 11	Risk Acceptance	# risk accepted policy deviations
KCI 12	Internet exposed assets security coverage	% of Internet exposed assets covered by security monitoring and regular security assessment
KCI 13	Crown jewel coverage	% of crown jewels covered by security monitoring, vulnerability scanning and regular security assessment
KCI 14	Origin of Security Incidents	% of security incidents related to failures from at least one Key Control Indicator

CISA Metrics On KEVs



Credit CISA Cybersecurity Performance Goals

Want to know more?

White paper published in September 2023

Ten key insights for informed cyber oversight

The document is available in EN, FR, DE, NL, IT, ES, PT, EL, PL, RO

One More Thing: Security By Default

What if Microsoft, Google and AWS would implement baseline security controls by default for their whole customer base?

Opinion paper published in December 2023:

Digital Sovereignty Is Impossible Without Big Tech

Don’t hide the risk, manage it

FreddyDezeure.eu