Message in a bottle

Freddy Dezeure

CERT-EU Conference 2023

Once upon a time

Threat intelligence department

1940

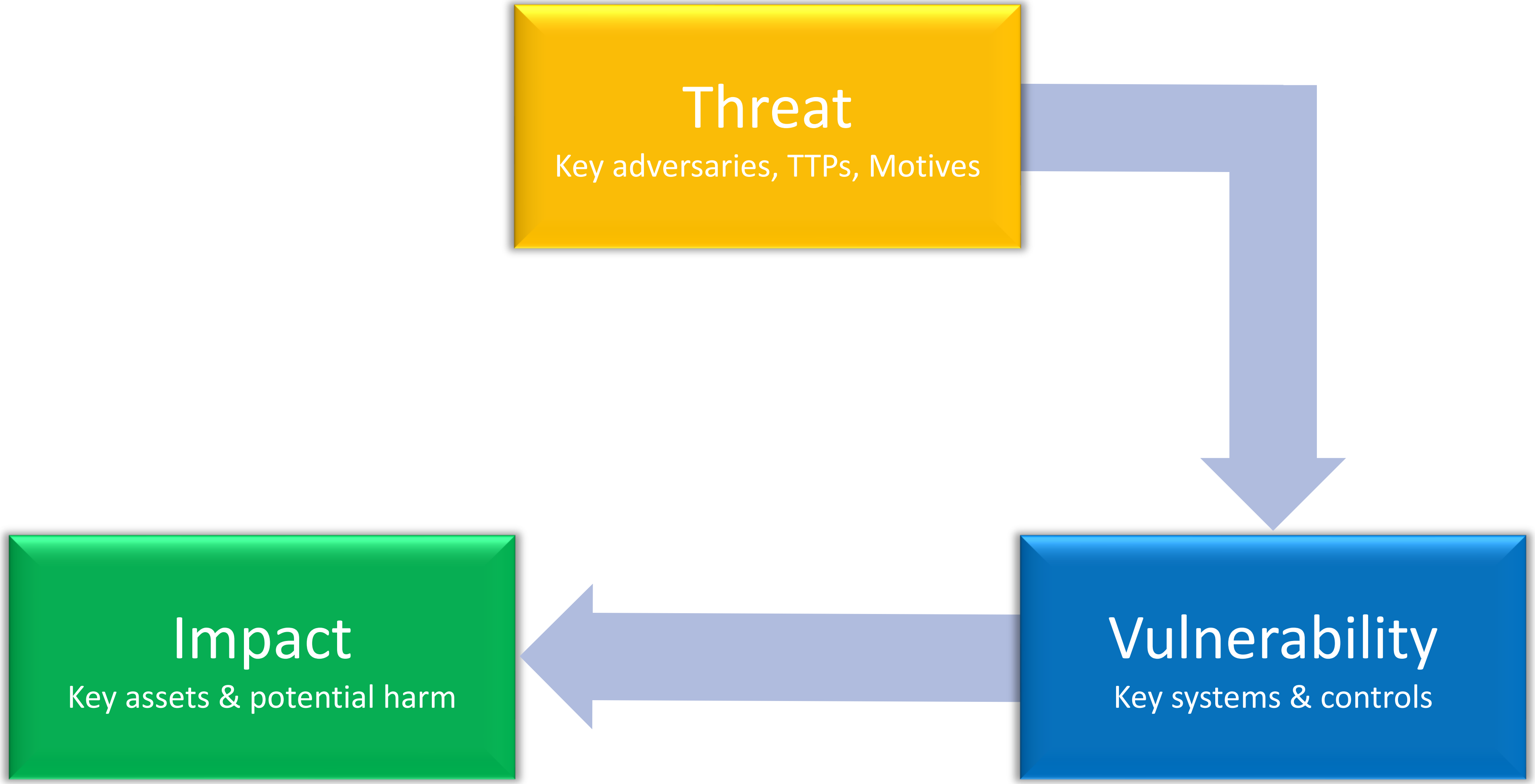
https://www.warhistoryonline.com/today-in-history/impenetrable-fall-eben-emael-fortress.html

Threat

Key adversaries

“CTI”

Don’t look only at the threat



Threat

Key adversaries, TTPs, Motives

Vulnerability

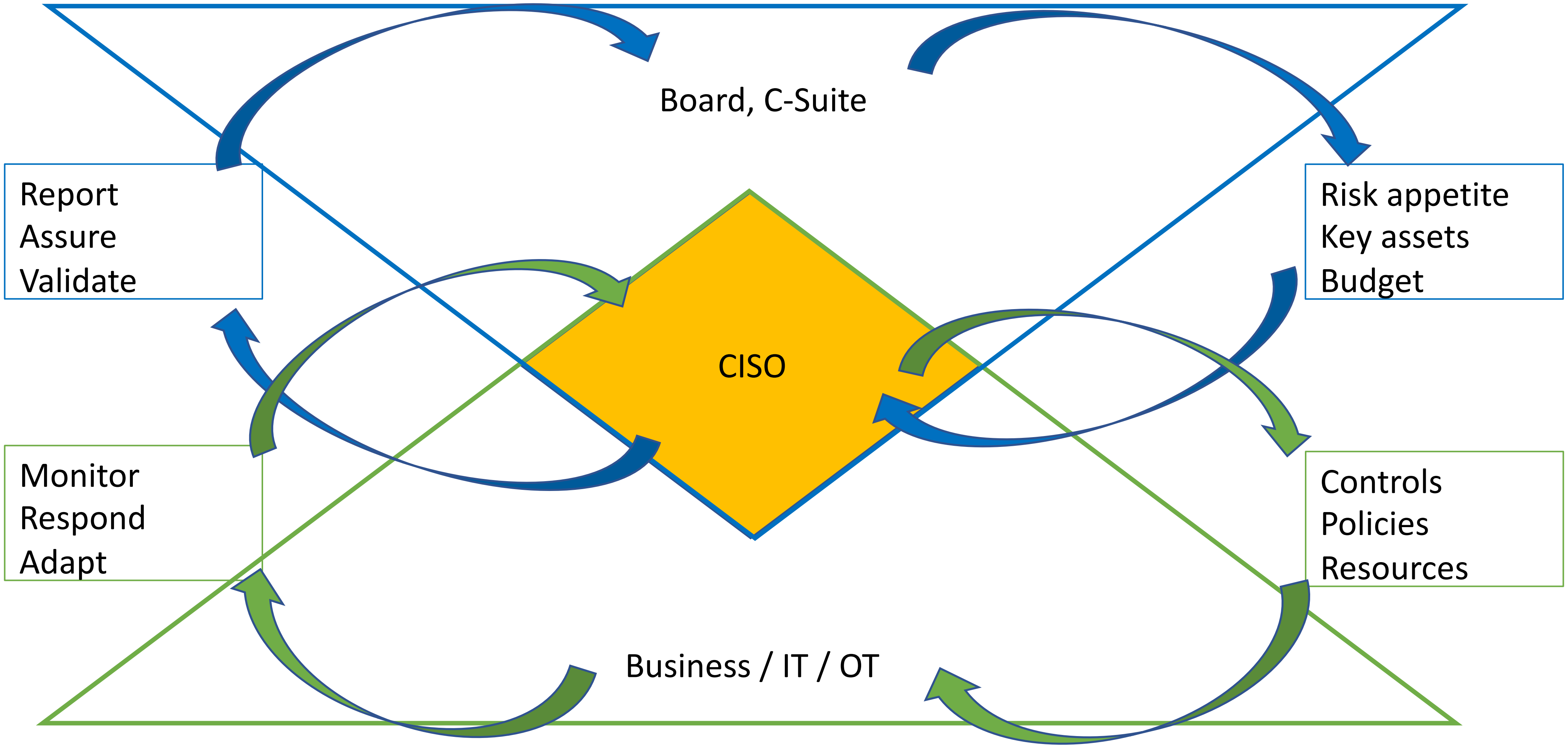
Key systems & controls

Impact

Key assets & potential harm

TID

Organize your cyber risk management



Board, C-Suite

Report
Assure
Validate

Risk appetite
Key assets
Budget

CISO

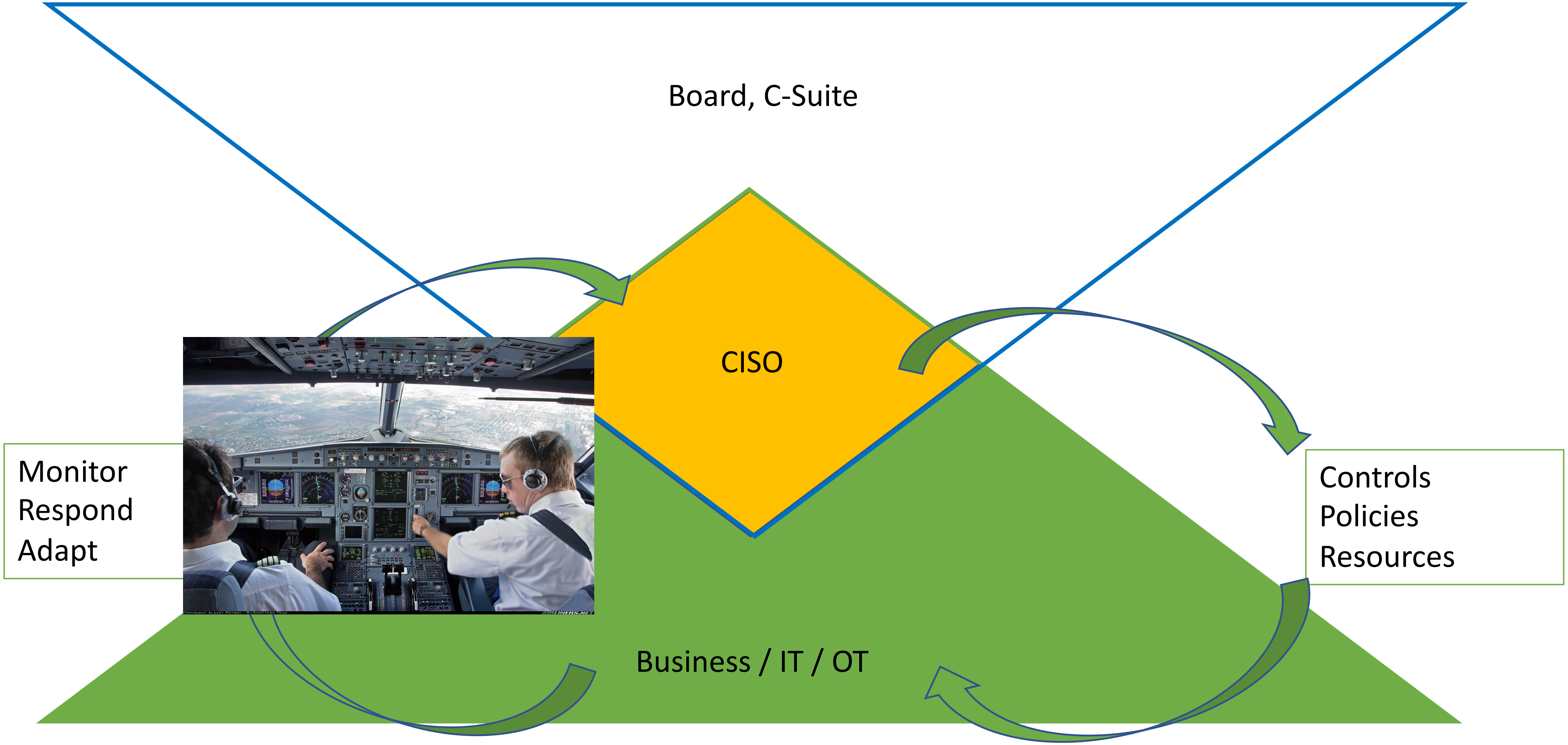
Monitor
Respond
Adapt

Controls
Policies
Resources

Business / IT / OT

Inspired by NIST CSF

Evidence-based action



Board, C-Suite

CISO

Monitor
Respond
Adapt

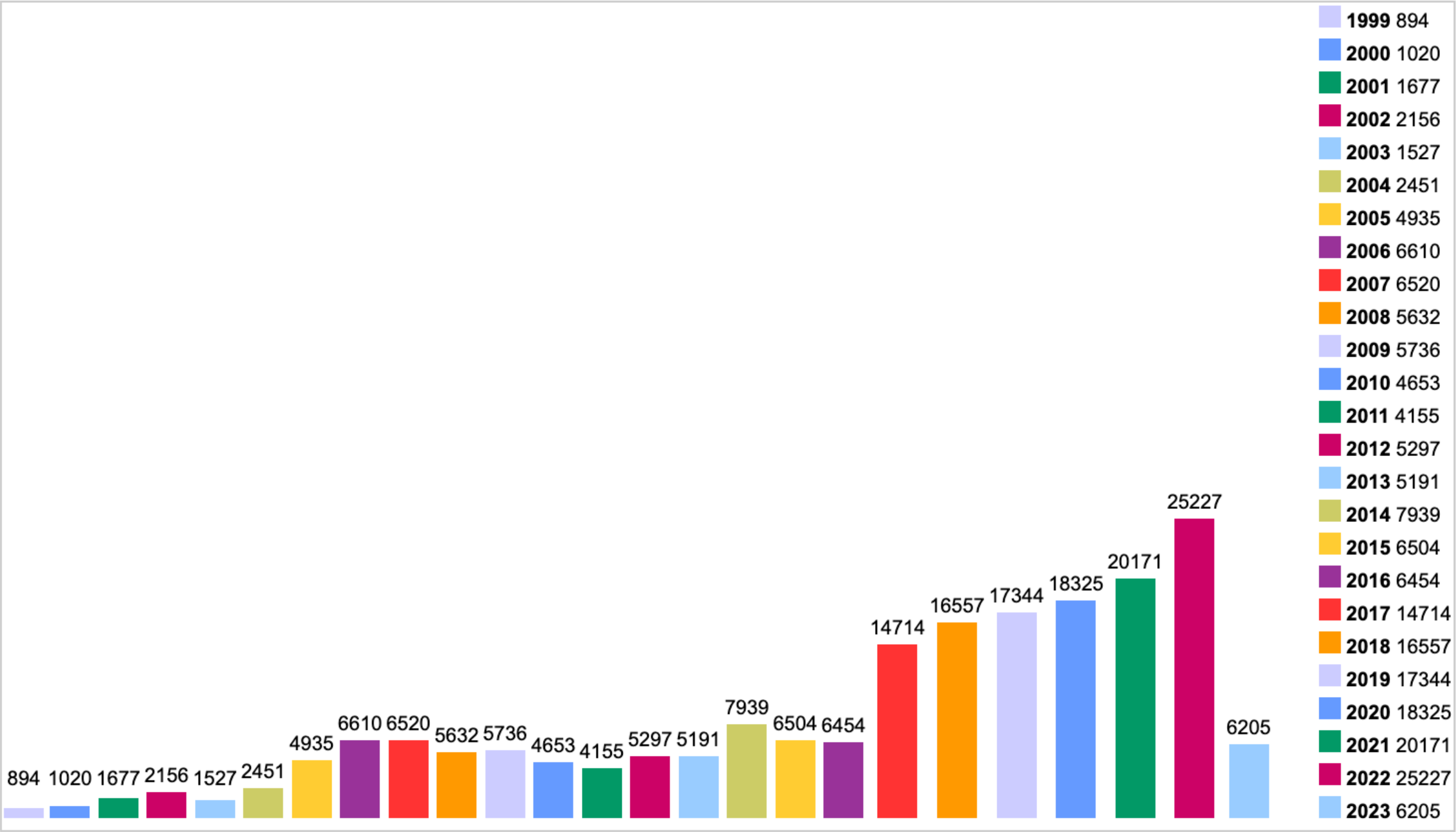
Controls
Policies
Resources

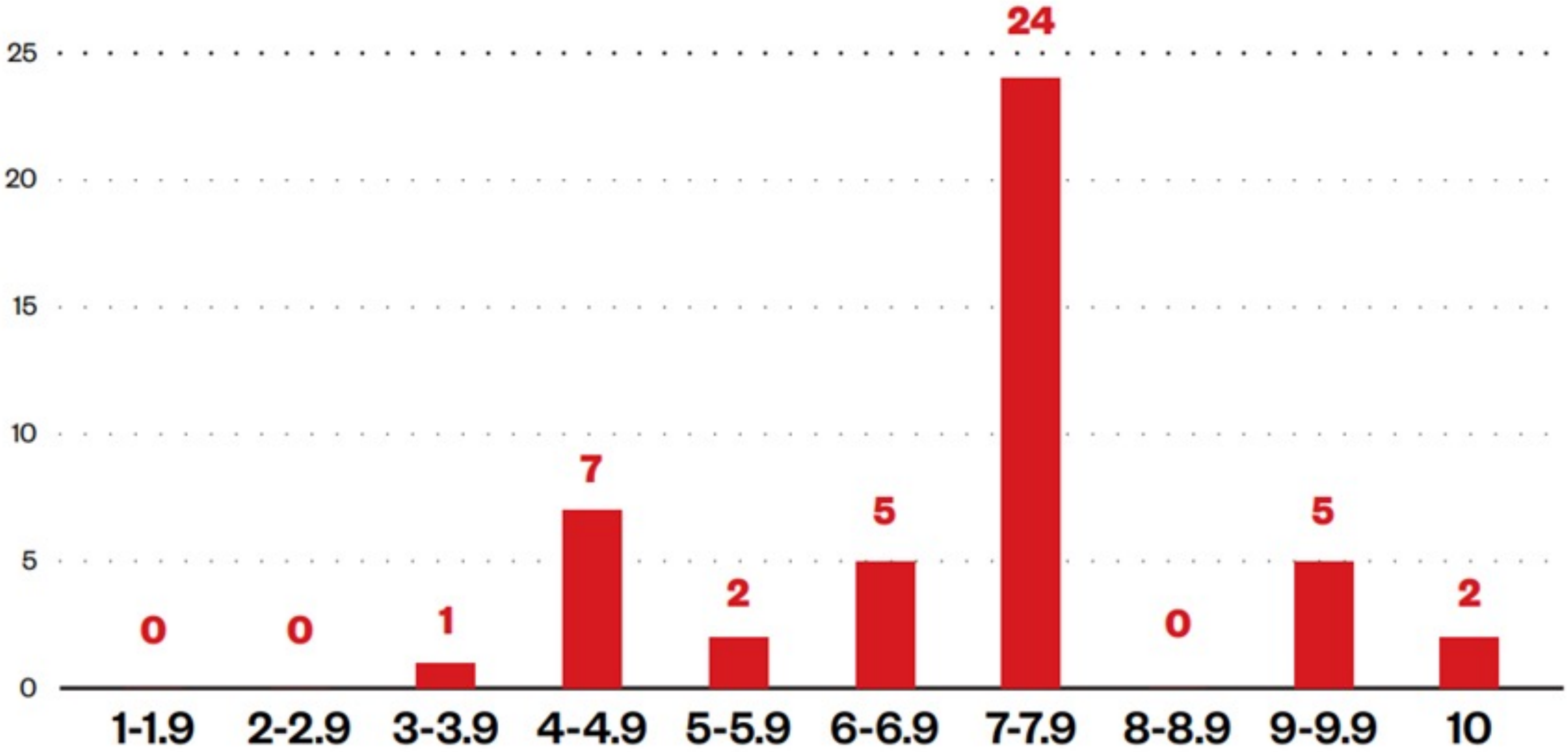
Business / IT / OT

Evidence-based action

- Evidence rather than compliance
  - Beyond intentions and self-assessment
  - Data from the infrastructure
  - Are the controls in place? Do the function as intended? Are they sufficient?
- Threat-informed rather than static
  - Adapt the defense to the evolution of the threat, vulnerabilities and assets
- Measure, monitor and adapt

Vulnerabilities By Year





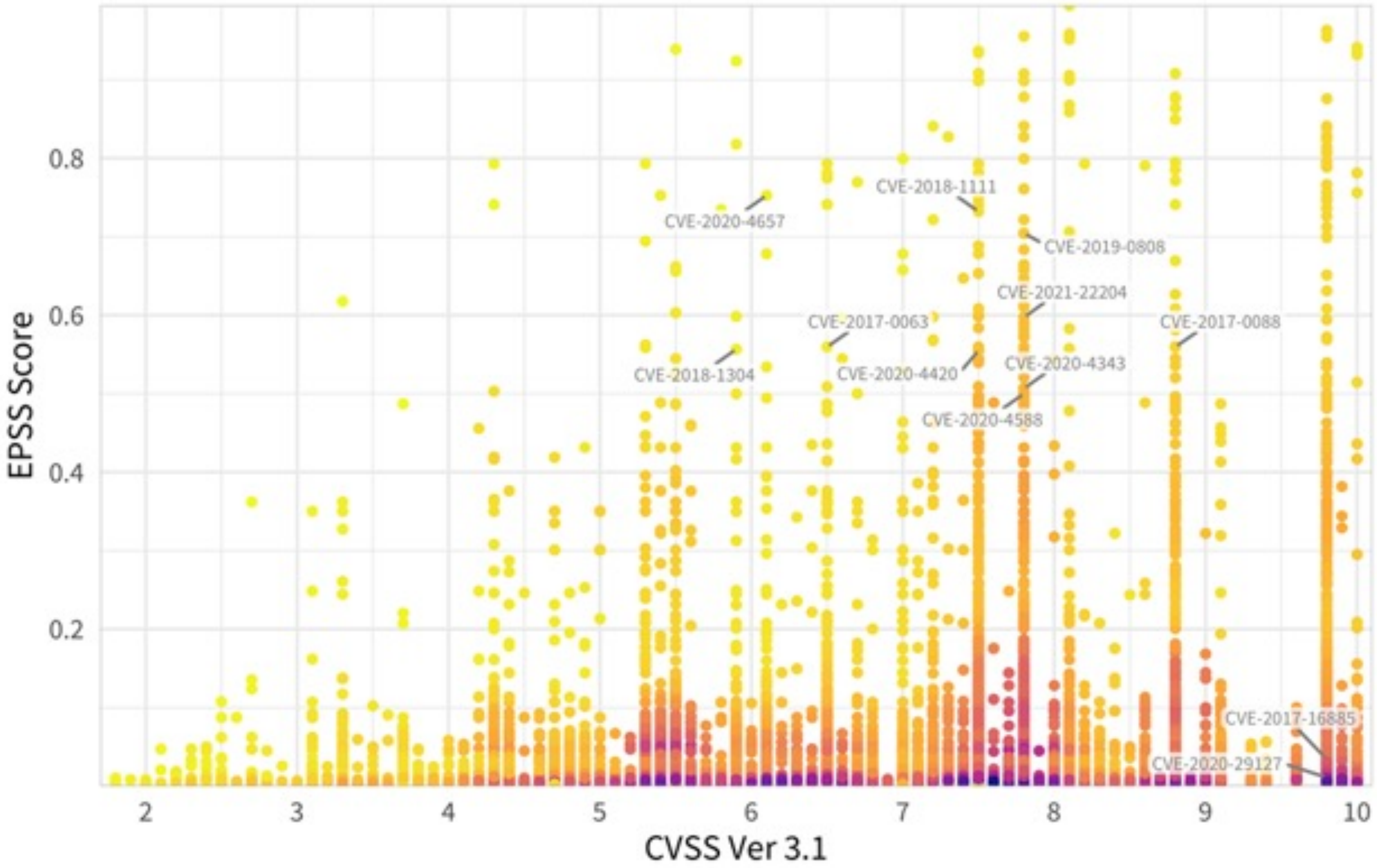
CVSS severity scores of the CVEs exploited by the top five ransomware groups

Credit TrendMicro 2023

Exploit Prediction Scoring System

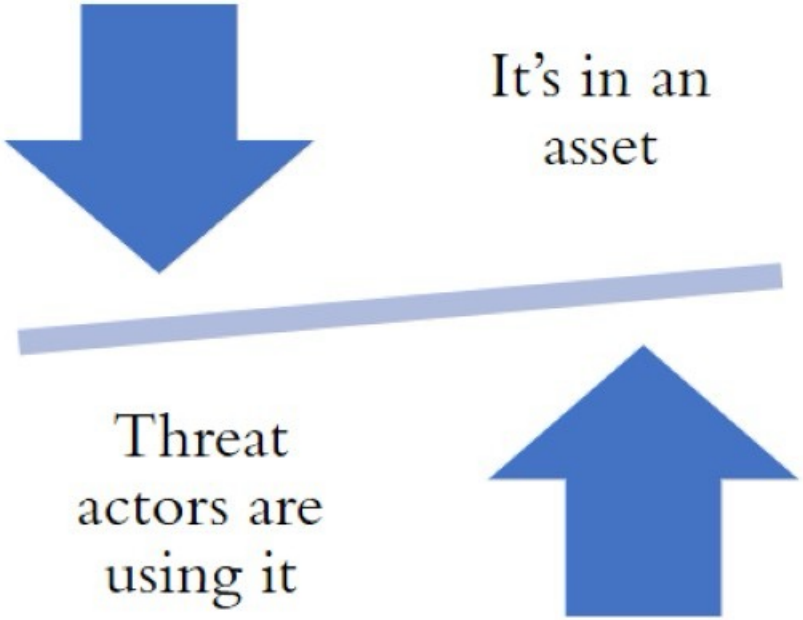
EPSS score compared to CVSS Base Score (NVD)

Point density is represented by color, yellow is less dense going through red to a deep purple for the most dense areas. Labeling a random sample of CVEs with higher values for reference.



Source: https://first.org/epss/data_stats, 2021-05-16

BOTH HAVE TO BE TRUE

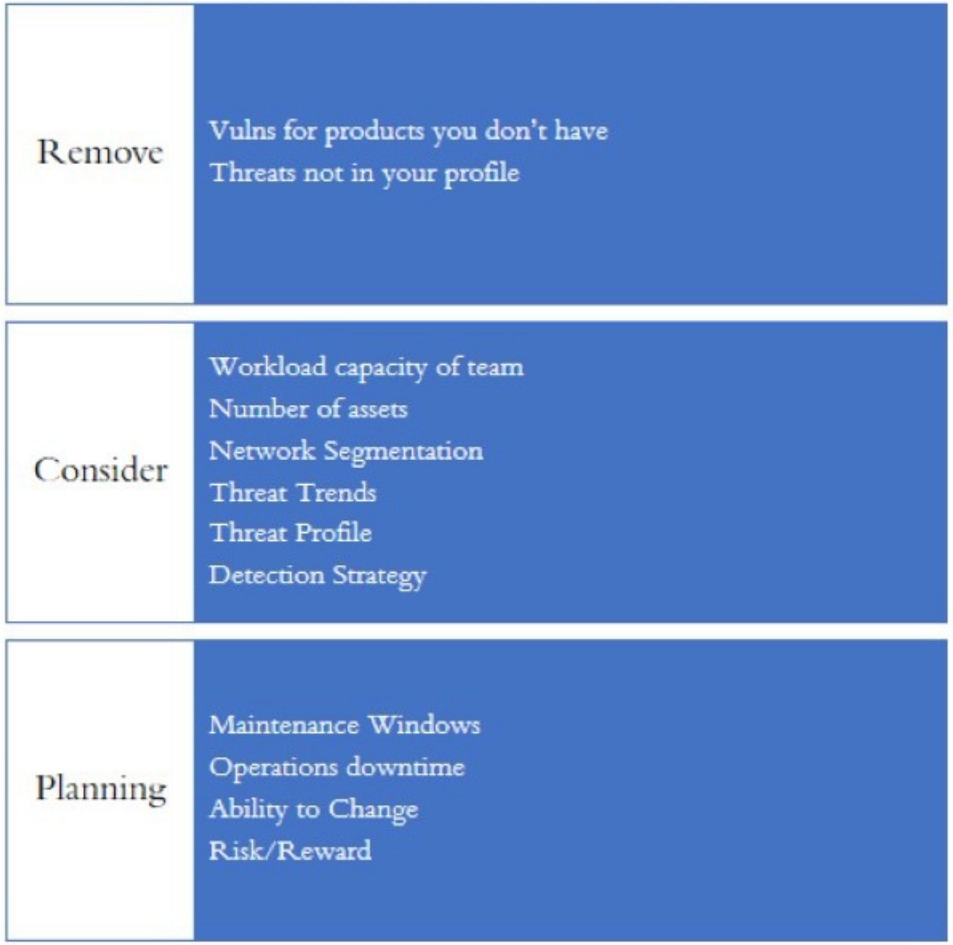


It's in an asset

Threat actors are using it

Credit Eireann Leverett

THE ATTACKER CONTROLS THE FREQUENCY, THE DEFENDER CONTROLS THE SEVERITY.



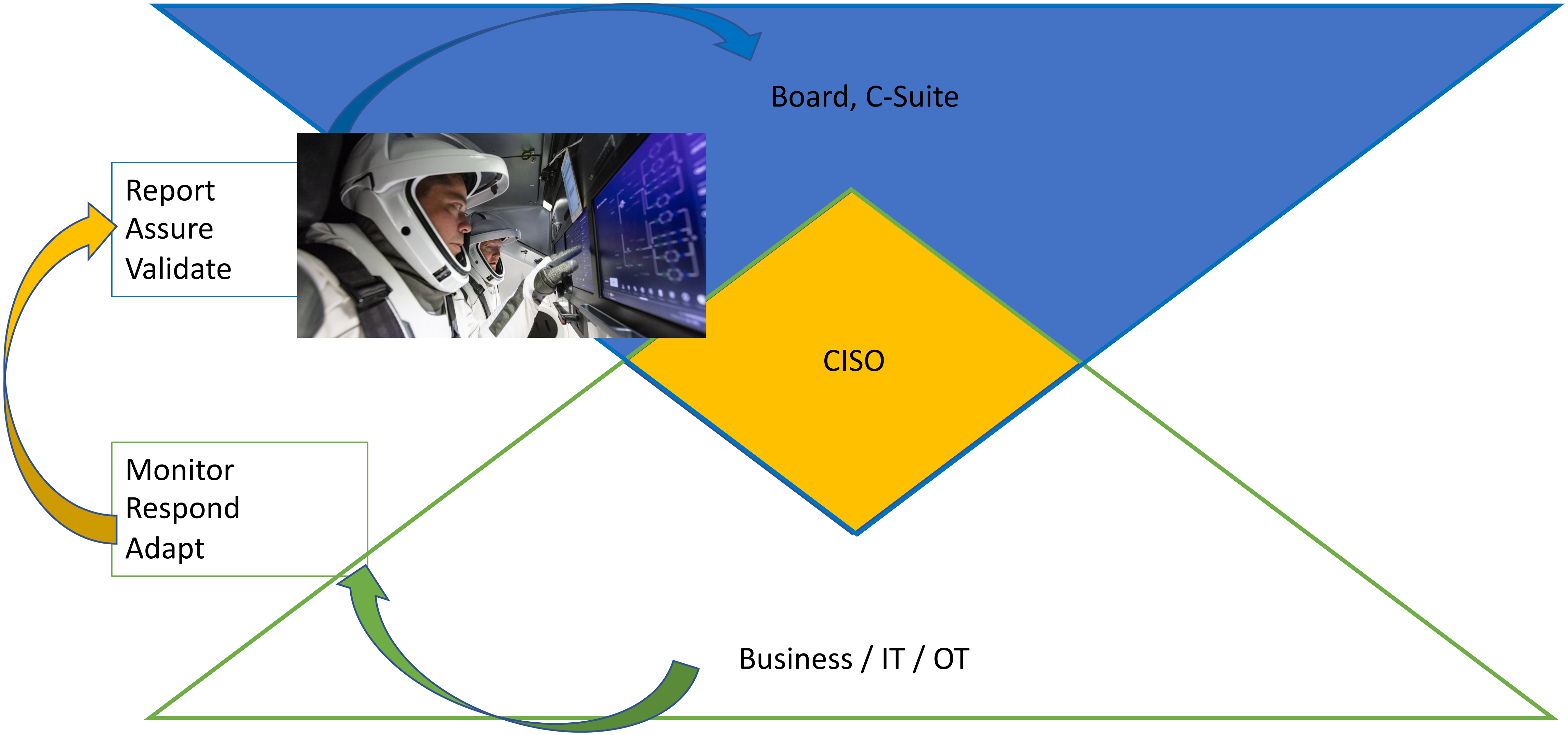
Remove	Vulns for products you don't have Threats not in your profile
Consider	Workload capacity of team Number of assets Network Segmentation Threat Trends Threat Profile Detection Strategy
Planning	Maintenance Windows Operations downtime Ability to Change Risk/Reward

- Number exposed
- Length of exposure
- Asset value
- Kill chain disruption
- Network reachability
- Combinations of above

"My board just patches what is in the news."

Credit Eireann Leverett

Evidence-based reporting



Board, C-Suite

Report
Assure
Validate

CISO

Monitor
Respond
Adapt

Business / IT / OT

Help your Board to have Informed Oversight

- Risk appetite rather than zero risk
- Top10 rather than everything
- Priorities rather than averages
- Reporting gaps rather than “all green”
- Embedded rather than disjointed
- Exceptions rather than acceptance
- Relevant stories
- Peer comparison (if you can)

Key Control Indicators

- Maintain an up-to-date inventory of assets
  - [% accurate key assets] [# rogue devices]
- Produce reliable, safe and secure backup of key assets
  - [% key assets with off-line, secure and tested backups]
- All key data is reliably and safely protected by encryption
  - [% key data encrypted at rest and in transit with keys under your control]
- Enforce multi-factor authentication wherever possible
  - [% implementation of MFA for privileged access accounts]
- Limit users’ permissions to what is strictly necessary
  - [% endpoints with local admin rights]
- Perform timely patching of important vulnerabilities
  - [% high risk patches implemented in time]
- Collect and analyze logs of all key systems
  - [% of key systems onboarded]
- Segment your network to protect your key assets
  - [% gaps found during testing]
- Exceptions/risk acceptance/policy violations

Is our cyber risk sufficiently mitigated?

- Treat cyber risk as a business risk
- Choose one framework (ISO, NIST, CIS, COBIT…)
- **Prioritize**: threats, assets, vulnerabilities/controls
- **Align** internally (CISO, risk, IT/OT operations, audit etc.)
- Go beyond compliance - **measure effectiveness**
- Report to your Board in **their language** and, if possible, **in-person**
- Report **gaps** and trajectory to close them
- Report **exceptions**/acceptance/violations
- **Train** your Board to deal with cyber

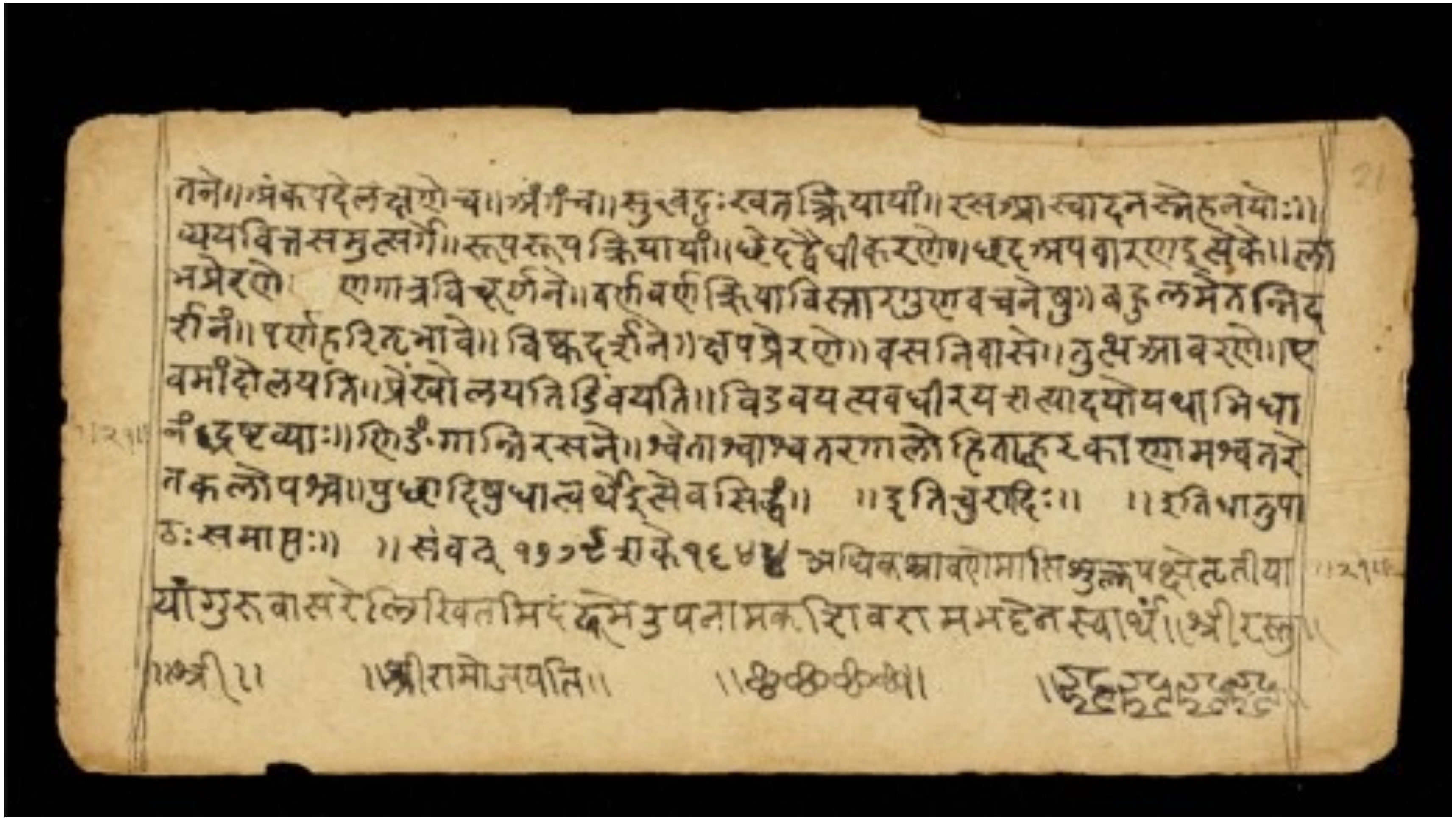
Who delivers the message?

Nobody

The wrong messenger

Too many messengers

Messenger speaking an unknown language

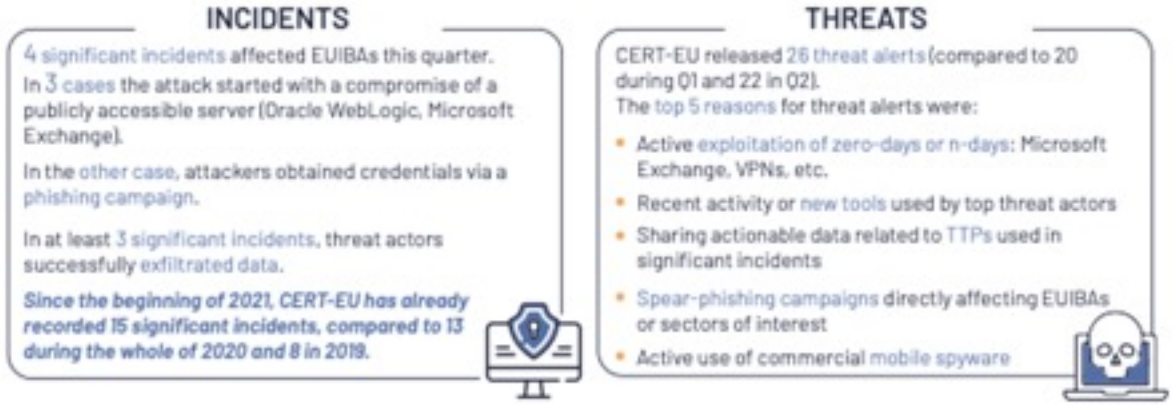


तने॥ अंकपदेलक्षणेच॥ अंगच॥ सुखदुःखतत्क्रियायां॥ रसआस्वादनस्नेहनयोः॥
व्ययवित्तसमुत्सर्गे॥ रूपरूपक्रियायां॥ छेदद्वैधीकरणे॥ छदअपवारणइत्येके॥ ला
भप्रेरणे॥ व्रणगात्रविचूर्णने॥ वर्णवर्णक्रियाविस्तारगुणवचनेषु॥ बहुलमेतन्निद
र्शने॥ पर्णहरितभावे॥ विष्कदर्शने॥ क्षपप्रेरणे॥ वसनिवासे॥ तुत्थआवरणे॥ ए
वमांदोलयति॥ प्रेंखोलयति विडंबयति॥ विडंबयत्यवधीरयतीत्यादयोयथाभिधा
नं द्रष्टव्याः॥ णिङ्‌गार्गिरसने॥ श्वेताश्वाश्वतरगालोडिताह्वरकाणामश्वतरे
तकलोपश्च॥ पुच्छादिषुधात्वर्थइत्येवसिद्धं॥ ॥इतिचुरादिः॥ ॥इतिधातुपा
ठः समाप्तः॥ ॥संवत् १९२९ शके १७९४ अधिकश्रावणेमासिशुक्लपक्षेतृतीया
यांगुरुवासरेलिखितमिदं दमेउपनामकशिवरामभट्टेनस्वार्थं॥ श्रीरस्तु॥
॥श्री॥ ॥श्रीरामोजयति॥ ॥[illegible]॥ ॥[illegible]

Credit: Cambridge University Library

Make sure your message comes across

Example 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.

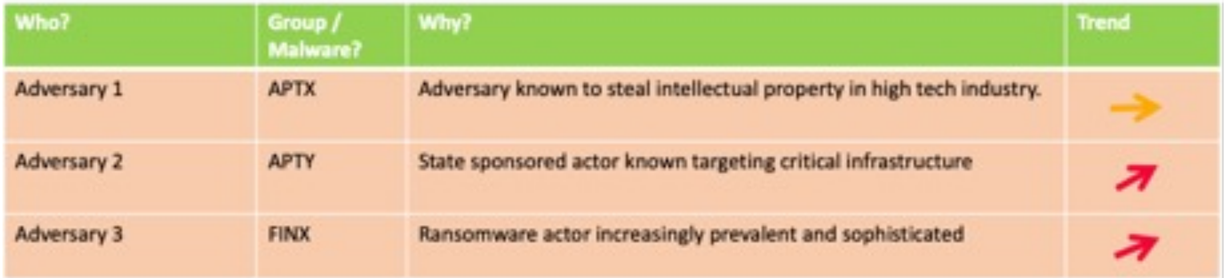
In at least 3 significant incidents, threat actors successfully exfiltrated data.

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.

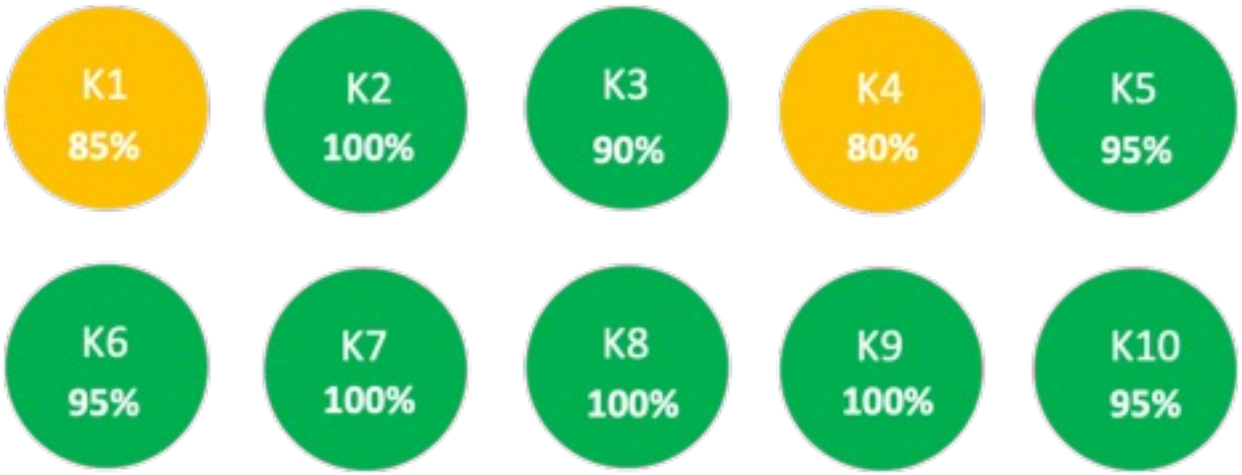
THREATS

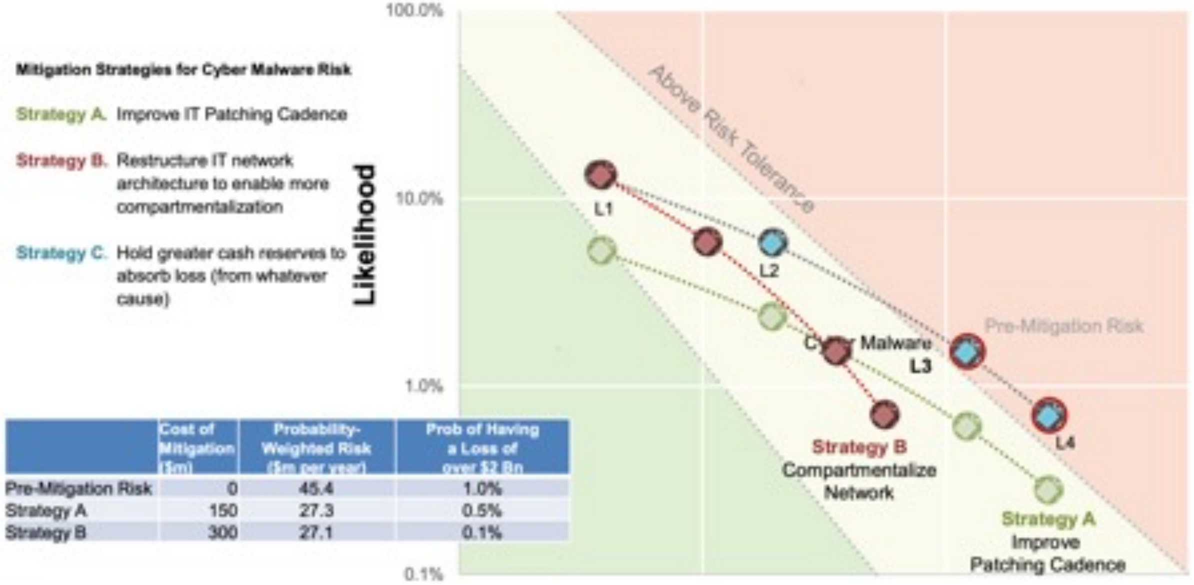
CERT-EU released 26 threat alerts (compared to 20 during Q1 and 22 in Q2).
The top 5 reasons for threat alerts were:

- 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



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%

Want to know more?

- Reporting Cyber Risk to Boards – Board Edition
- Reporting Cyber Risk to Boards – CISO Edition

The documents are also available in FR, DE, NL

Call for interest

Country-level Metrics Working Group starting in October

- Which controls are working on country level?
- How do you measure the impact?
- How do you report to your PM?

Targeting best practice countries, results to be published.

FREDDY
DEZEURE

Don’t hide the risk, manage it

FreddyDezeure.eu