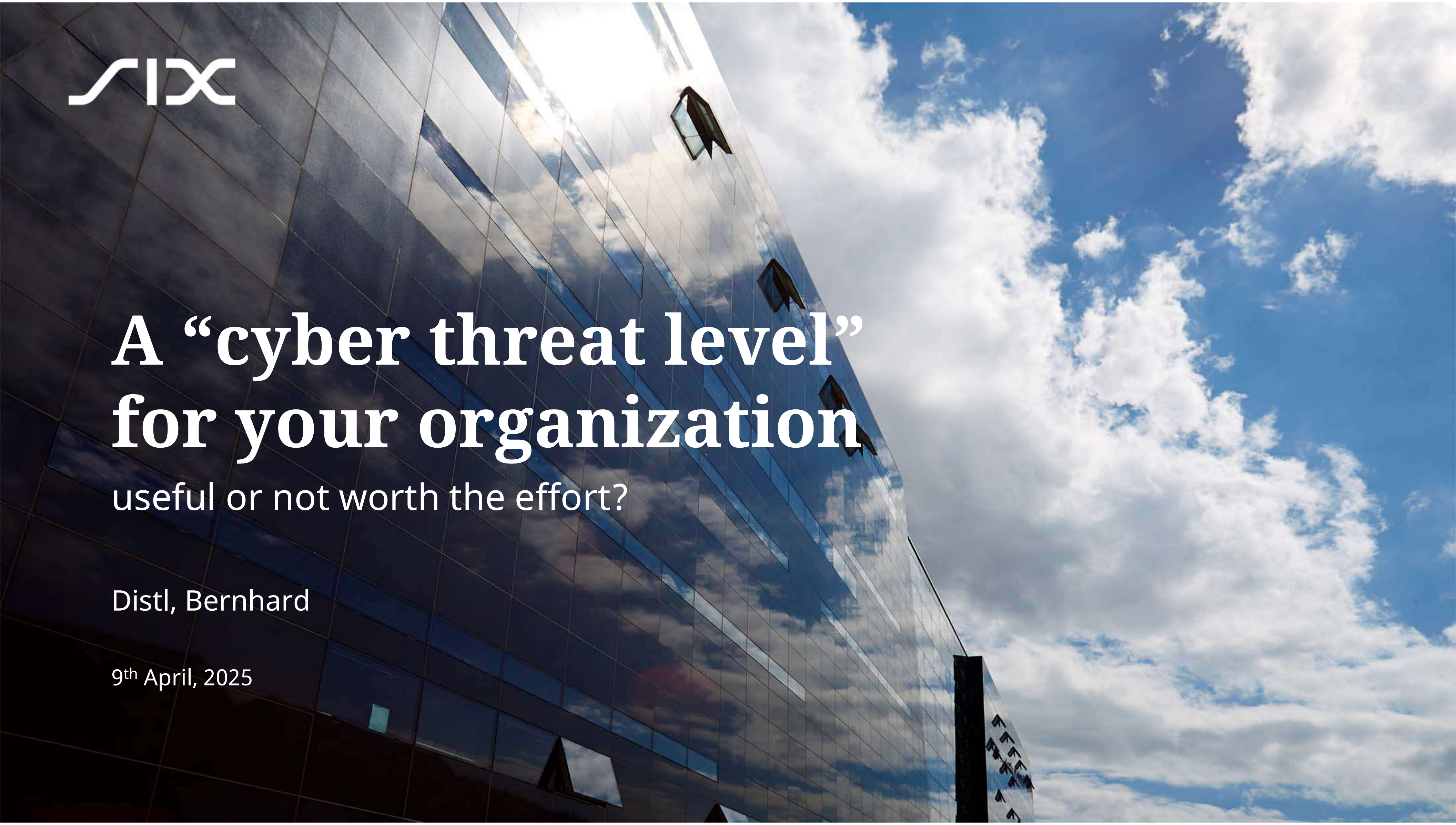


A “cyber threat level” for your organization

useful or not worth the effort?

Distl, Bernhard

9th April, 2025

About me

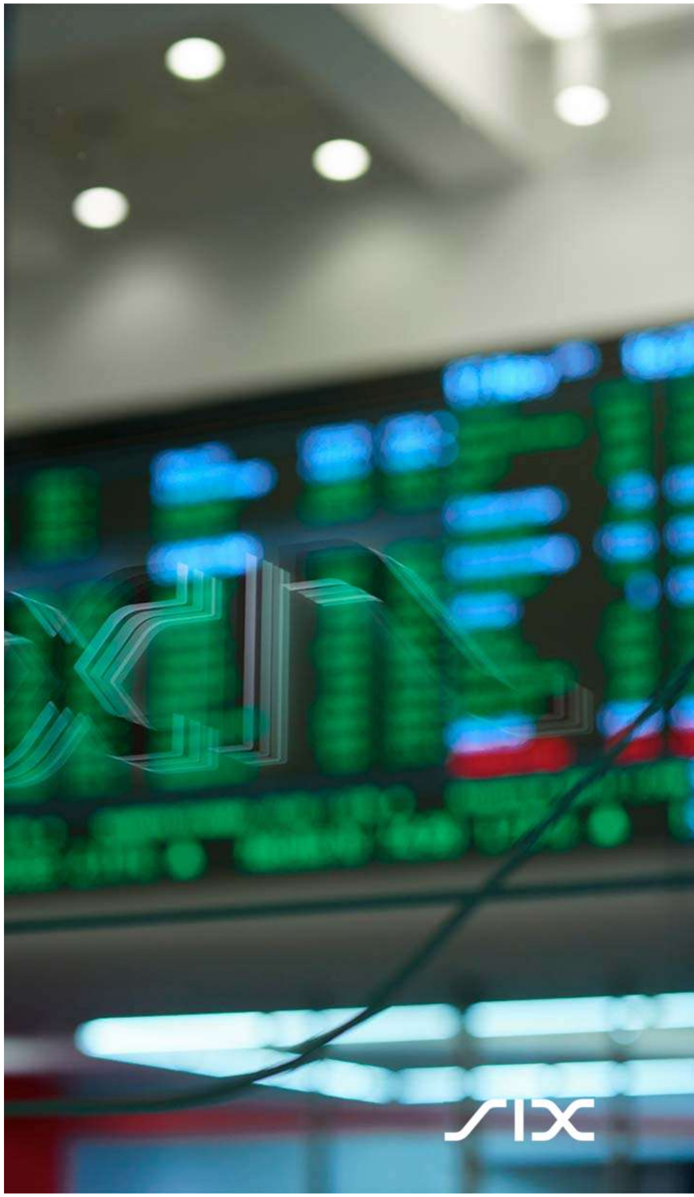
Agenda

Threat levels and cyber threat levels

What data do we need?

Where do we get the data from?

How to make use of your cyber threat level?

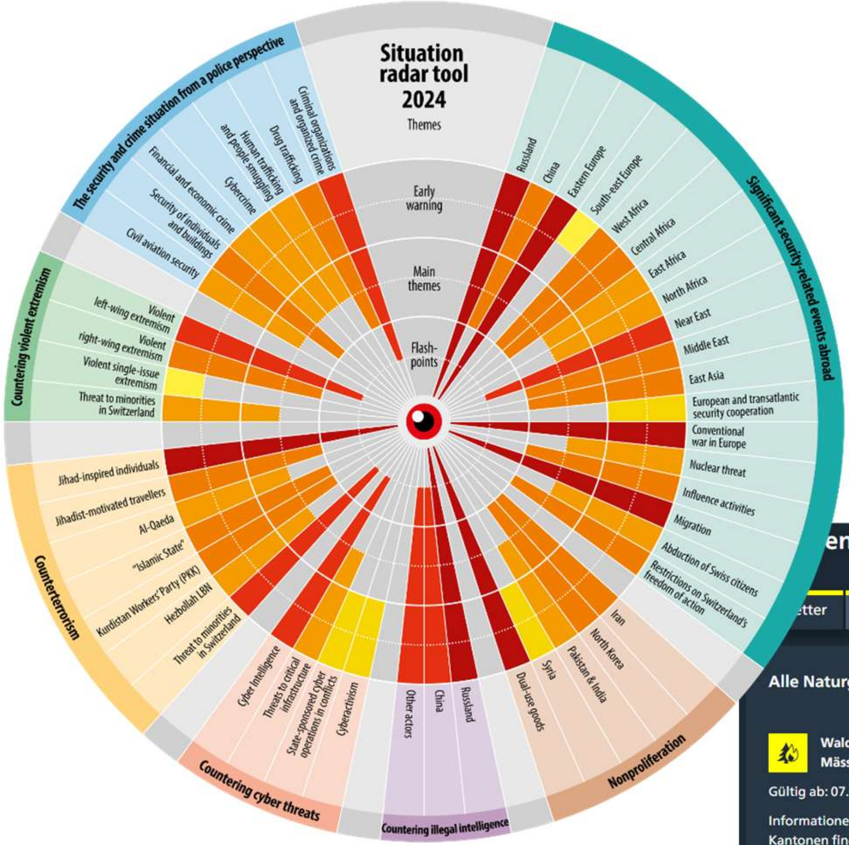


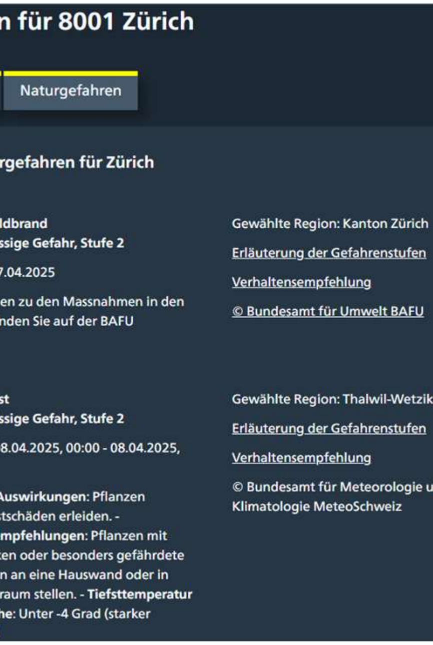
Other threat levels

- Governments
  - Terror
  - Extremism
  - Health (infections)
- Organizations
  - Weather
  - Maritime conditions

All are based on past data (trend) and current data.

An element of forecast is optional.





en für 8001 Zürich

Alle Naturgefahren für Zürich

Waldbrand
Mässige Gefahr, Stufe 2

Gültig ab: 07.04.2025

Informationen zu den Massnahmen in den Kantonen finden Sie auf der BAFU Webseite.

Gewählte Region: Kanton Zürich

Erläuterung der Gefahrenstufen

Verhaltensempfehlung

© Bundesamt für Umwelt BAFU

Frost
Mässige Gefahr, Stufe 2

Gültigkeit: 08.04.2025, 00:00 - 08.04.2025, 08:00

- **Mögliche Auswirkungen**: Pflanzen können Frostschäden erleiden. - **Verhaltensempfehlungen**: Pflanzen mit Vlies abdecken oder besonders gefährdete Topfpflanzen an eine Hauswand oder in einen Innenraum stellen. - **Tiefsttemperatur in Bodennähe**: Unter -4 Grad (starker Bodenfrost)

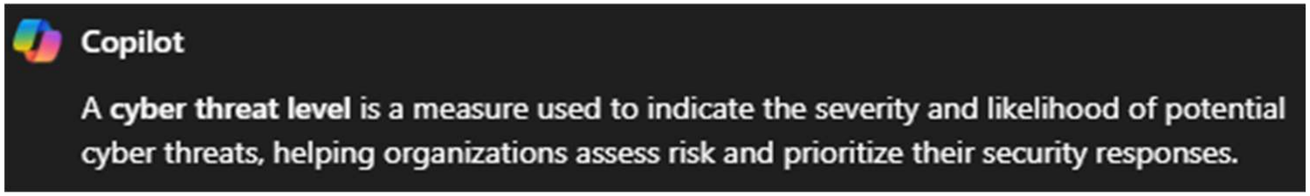
Gewählte Region: Thalwil-Wetzik

Erläuterung der Gefahrenstufen

Verhaltensempfehlung

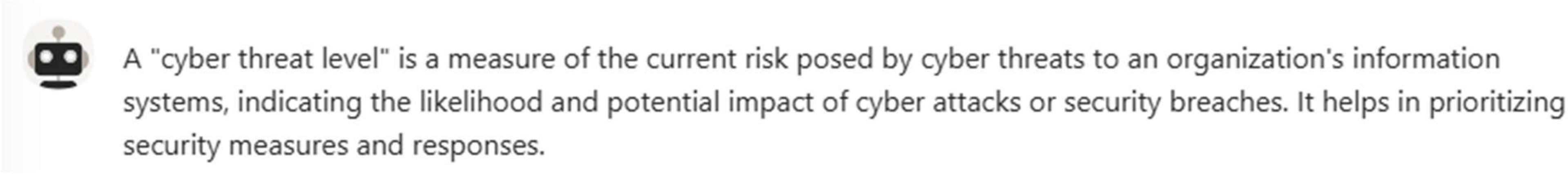
© Bundesamt für Meteorologie u Klimatologie MeteoSchweiz

Cyber threat level – AI definition ;-)



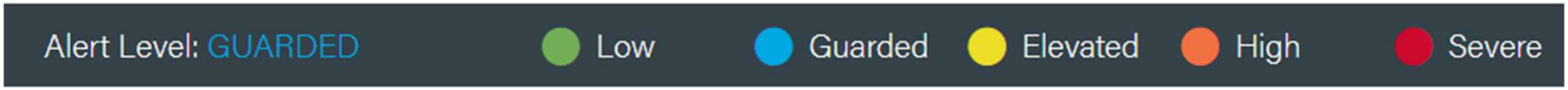
Copilot

A **cyber threat level** is a measure used to indicate the severity and likelihood of potential cyber threats, helping organizations assess risk and prioritize their security responses.

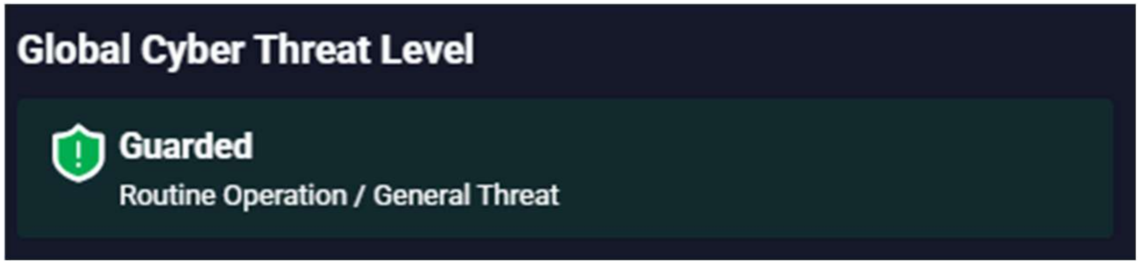


A "cyber threat level" is a measure of the current risk posed by cyber threats to an organization's information systems, indicating the likelihood and potential impact of cyber attacks or security breaches. It helps in prioritizing security measures and responses.

Cyber Threat Level - Examples



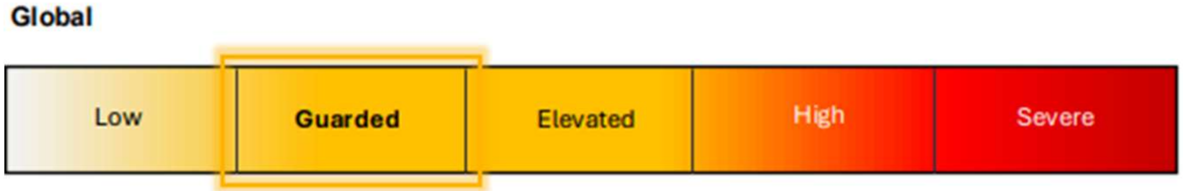
Alert Level: GUARDED ● Low ● Guarded ● Elevated ● High ● Severe



Global Cyber Threat Level

Guarded

Routine Operation / General Threat



Global

Low	Guarded	Elevated	High	Severe

Cyber Threat Level Scale

- Most (cyber) threat levels use a 3-5 step scale
- The «default» level varies with each scale and context.
- The scale is often dependent on the requirements of the audience and what is considered «normal»

Examples:
3 - low / medium / high
4 - low / guarded / elevated / high
5 – low / guarded / elevated / high / severe

Hints for your own scale:

- Keep it simple
- If you use more than 3 levels, make sure you have enough data
- Many customers do not care about a level «below normal»
- Define clear criteria for your levels

What data can you base your cyber threat level on?

Data types to consider

- Industry sector information [sharing / buying]

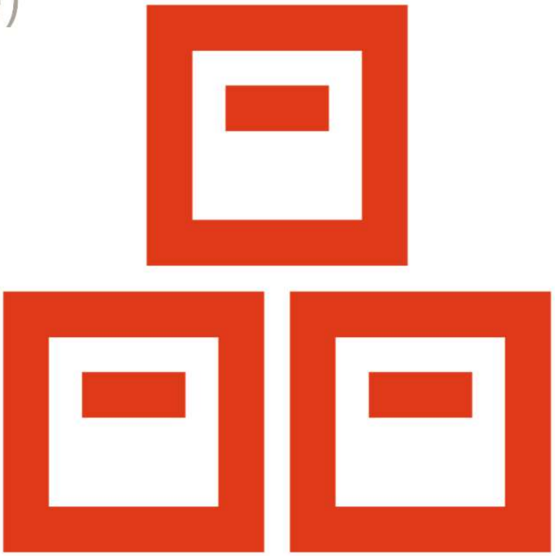
- Geographical information [sharing / buying]

- Global information [sharing / buying]

- Company data [your collection]

Industry sector specific data

- Which company types are targeted? (target details within the sector)
- How are companies in the same sector targeted? (attack types)
- How frequently are they targeted? (attack volume)
- Which threat actors have been identified?



Sources

- Open source collection (DIY)
- Commercial providers
- Information sharing organizations

Geograpical and global data

- Are areas where your company is active targeted? (target details within location)
- What attacks are reported within your geographies? (attack types)
- What are the properties of the reported attacks? (attack volume, quality)
- Which threat actors have been identified?

Sources

- Open source collection (DIY)
- Commercial providers
- Information sharing organisations

Challenges with sector and geographical data

- Commercial (OSINT) providers have a limited visibility
- Information sharing initiatives may overlap (constituency, area, sector)
- International and multi-sector companies may only provide overall numbers
- Shared IT infrastructure prevents attribution to geography for multinational companies

- Sharing initiatives for specific geography/sector may not exists -> start building communities

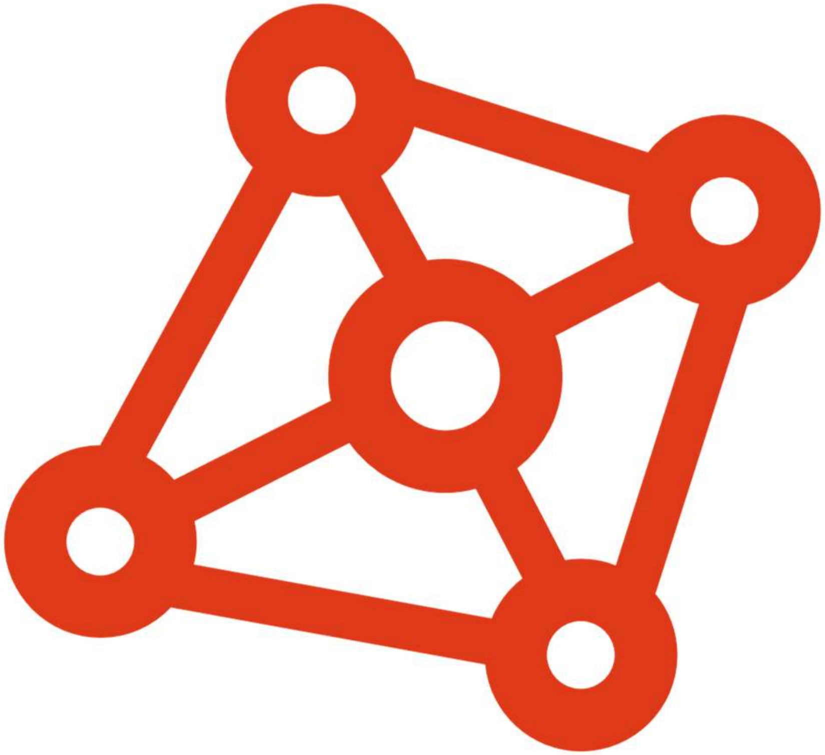
Company data overview

- Security incidents

- Vulnerabilities

- Security perimeter

- OSINT (incl. dark web)



Company data details (examples)

Security incidents	Vulnerabilities	Security perimeter	OSINT
• Number of true positive incidents (by type) • Detected TTPs • Noteworthy incidents flagged by SOC	• Affected assets • Exposed to Internet • Exploit available • Patching time frames	• Firewall • Web application firewall (WAF) • DDoS protection • Mail gateway • VPN / RAS devices • MFA services • Authentication logs	• Social media • Domain registrations • Brand / Logo abuse • Dark web
• SOC report • True positive phishing • Phishing TTPs • Reported CEO fraud • Brute force incidents • Data leak incidents	• Vulnerability scanner result • Threat intelligence tools for CVEs • Vulnerability management policy & exceptions	• Malware emails (malware type) • CEO Fraud emails • WebApp vulnerability exploits • DDoS mitigation actions • Failed login attempts (MFA)	• Executive impersonation • Leaked credentials • Phishing sites

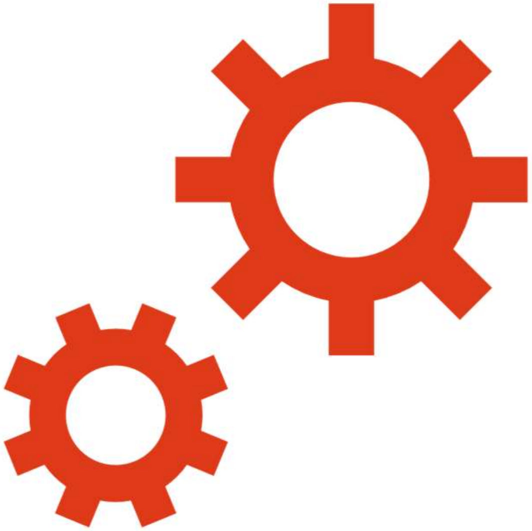
What to do with your cyber threat level?

Cyber threat level audience

- Risk & Security
- Cyber security
- Upper management
- Operational teams

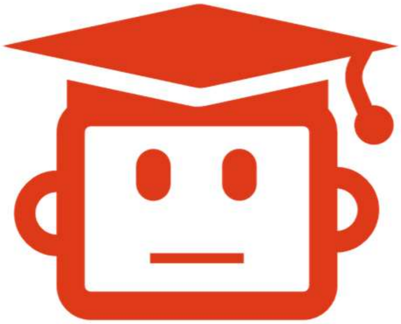
Cyber threat level use

- Situational awareness
- Align cyber security teams activities
- Adjust activity focus
  - specific hunting activities
  - increased monitoring (e.g. frequency)
  - faster communication
  - additional detection rule activation



Cyber threat level lessons learned

- Finding & making data available takes time
- Data analysis and trend generation needs some refinement
- Aligning all stakeholders is important
- Do threat level internally for a while to get experience
- Properly justify each threat level change
- Do not change the threat level too frequently (use experience and your definition)
- Clear responsibility who decides on the level is needed



Thank you

Disclaimer

This material has been prepared by SIX Group Ltd, its subsidiaries, affiliates and/or their branches (together, “SIX”) for the exclusive use of the persons to whom SIX delivers this material. This material or any of its content is not to be construed as a binding agreement, recommendation, investment advice, solicitation, invitation or offer to buy or sell financial information, products, solutions or services. It is solely for information purposes and is subject to change without notice at any time. SIX is under no obligation to update, revise or keep current the content of this material. No representation, warranty, guarantee or undertaking – express or implied – is or will be given by SIX as to the accuracy, completeness, sufficiency, suitability or reliability of the content of this material. Neither SIX nor any of its directors, officers, employees, representatives or agents accept any liability for any loss, damage or injury arising out of or in relation to this material. This material is property of SIX and may not be printed, copied, reproduced, published, passed on, disclosed or distributed in any form without the express prior written consent of SIX.