GRID RESILIENCE STARTS WITH GIS

Why securing spatial intelligence is critical for utilities and networks?

fortum
Powering a thriving world

AGENDA

- GIS & SECURITY OF SUPPLY
- KILLCHAIN WALKTHROUGH
- VULNERABILITIES
- MITIGATION STRATEGIES

Modern geospatial information systems serve a dual role:

- Critical national assets enabling societal functions
- Compelling and vulnerable targets that can be exploited to disrupt these functions.

Protecting GIS directly supports security of supply, protection of critical infrastructures, and the ability to operate securely within the current spatio-temporal atmosphere.

fortum
Powering a thriving world

ISO22300 STANDARD DEFINITION

Preparedness:

Activities and systems implemented before potential disruptions, which can be used to prevent incidents, protect operations, mitigate impacts, respond effectively, and enable recovery.

Resilience:

Ability to adapt to and withstand changes in the operating environment.

fortum
Powering a thriving world

“It is not the strongest species that survive, nor the most intelligent, but the ones responsive to change

- Charles Darwin

fortum
Powering a thriving world

WHOAMI

Versatile Geek
GIS & Cyber entusiast

MSc, Geography
MEng, Cybersecurity
Doctoral Researcher, Military Technology:

Geospatial Information Systems at the nexus of cyber and hybrid warfare

https://www.linkedin.com/in/suvi-tuulia-haakana/

suvi.haakana@gmail.com

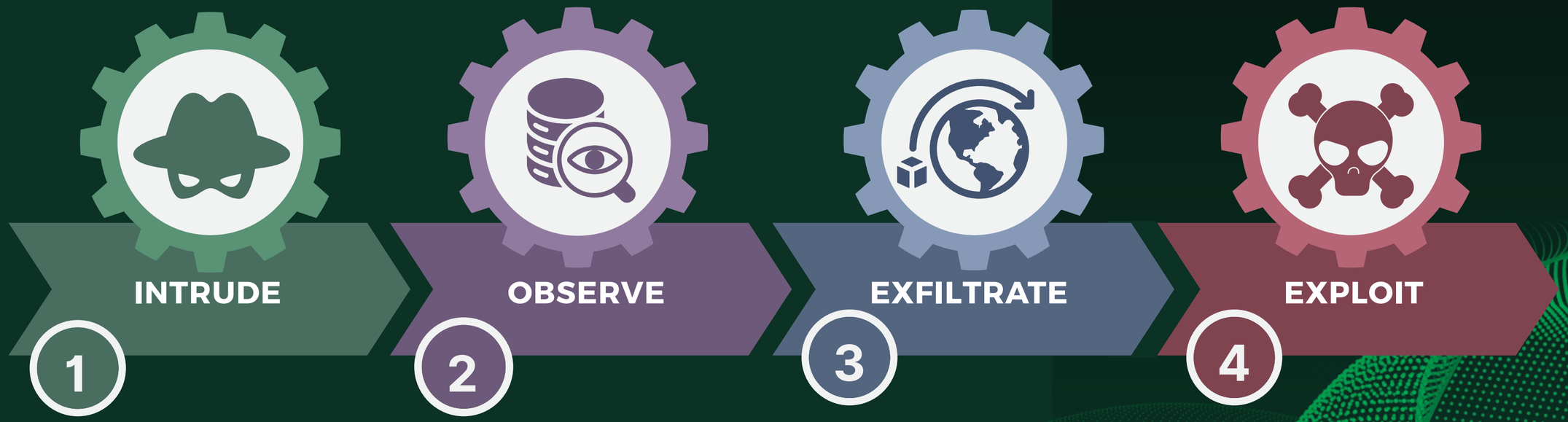
fortum
Powering a thriving world

GIS & SECURITY OF SUPPLY

	Industry	Planning	Management	Operations	Decision-making
Primary	**Energy distribution**	✔	✔	✔	✔
	Water supply	✔	✔	✔	✔
	Transportation & logistics	✔	✔	✔	✔
	Telecommunications	✔	✔	✔	✔
Secondary	Food supply	✔	✔	?	✔
	Healthcare	✔	✔	✔	✔
	Social and crisis services	✔	?	?	✔
	Public safety authorities	✔	✔	✔	✔
	Banking & Financial services	?	✘	✘	?
	Public administration	✔	✔	✘	✔
	Smart cities	✔	?	✔	✔

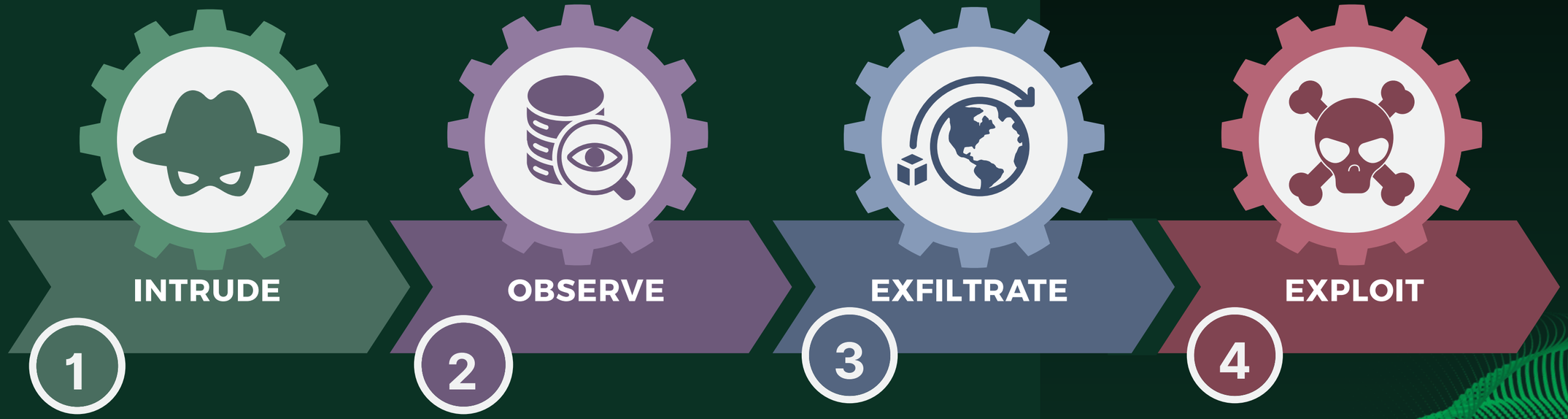
fortum
Powering a thriving world

KILLCHAIN



fortum
Powering a thriving world

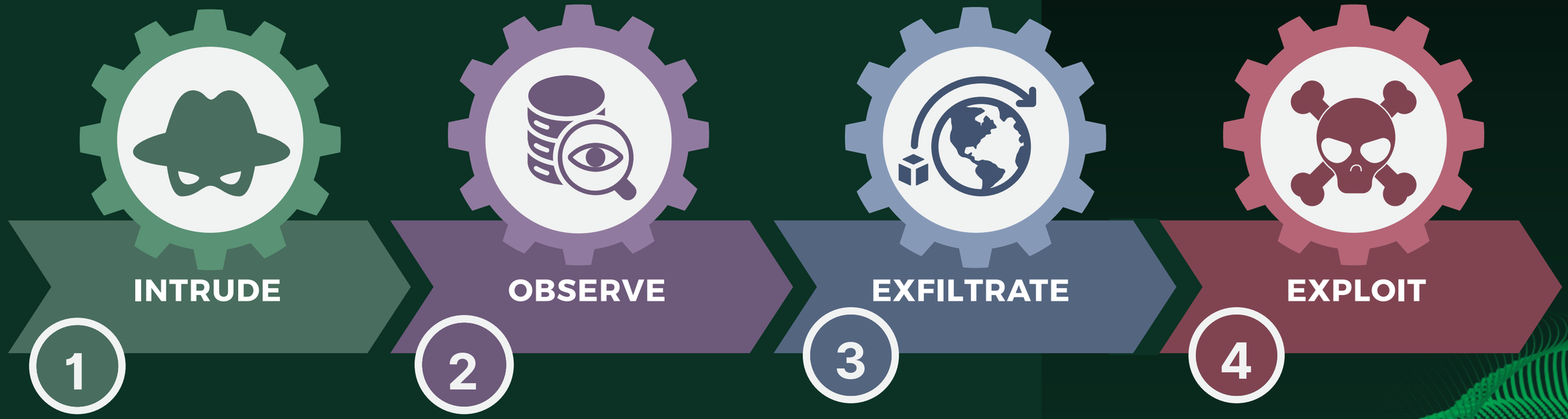
KILLCHAIN



1 Exploitation of a vulnerability in the target system (e.g. a known CVE), social engineering, or a deficiency in the process enables intrusion.

fortum
Powering a thriving world

KILLCHAIN

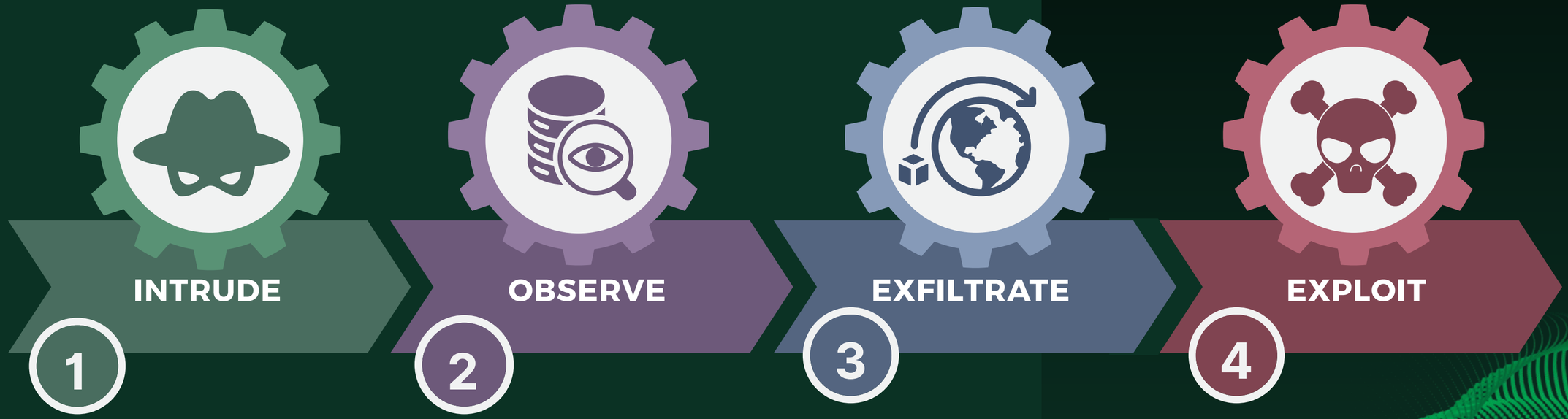


2

Espionage and observation within the target system in order to collect critical information and insight.

fortum
Powering a thriving world

KILLCHAIN

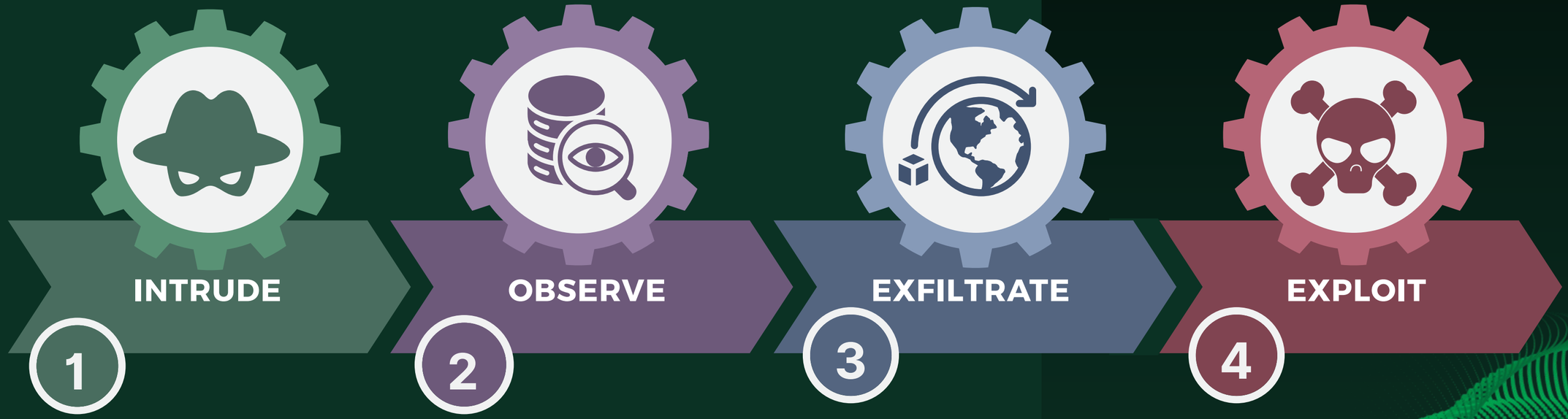


3

The aggregated data is exfiltrated from the target system, stored elswhere, and/or transmitted onward.

fortum
Powering a thriving world

KILLCHAIN



4 The information is, for example, sold or leveraged in the planning of cyber and hybrid operations.

fortum
Powering a thriving world

CVE EXAMPLES

CVE-2009-0839

MapServer 4.x & 5.x

"Stack-based buffer overflow, when the server has a map with a long IMAGEPATH or NAME attribute, allows remote attackers to execute arbitrary code via a crafted id parameter in a query action."

Source: MITRE

CVE-2025-57870

ArcGIS Server 11.3 - 11.5

"This vulnerability allows a remote, unauthenticated attacker to execute arbitrary SQL commands via a specific ArcGIS Feature Service operation. Exploitation can result in unauthorized access, modification, or deletion of data from the underlying Geodatabase."

Source: ESRI Inc

fortum
Powering a thriving world

The Register®

Chinese gang used ArcGIS as a backdoor for a year – and no one noticed

Crims turned trusted mapping software into a hideout - no traditional malware required

Carly Page

Tue 14 Oct 2025 // 16:48 UTC

A Chinese state-backed cybergang known as Flax Typhoon spent more than a year burrowing inside an ArcGIS server, quietly turning the trusted mapping software into a covert backdoor.

Researchers at ReliaQuest say that the espionage outfit, which Microsoft tracks as a China-based state-sponsored actor, modified a legitimate ArcGIS server object extension (SOE) to act as a web shell, giving them long-term, near-invisible access. By exploiting ArcGIS' extensibility features while avoiding traditional, signature-based malware, Flax Typhoon embedded itself so deeply that even restoring systems from backups simply reinstalled the implant.

EXPLOIT EXAMPLE

fortum
Powering a thriving world

HOW TO STAY SAFE?

IDENTIFY THREATS 1

ASSESS & PRIORITIZE 2

MITIGATE (SYSTEMATICALLY) 3

MONITOR 4

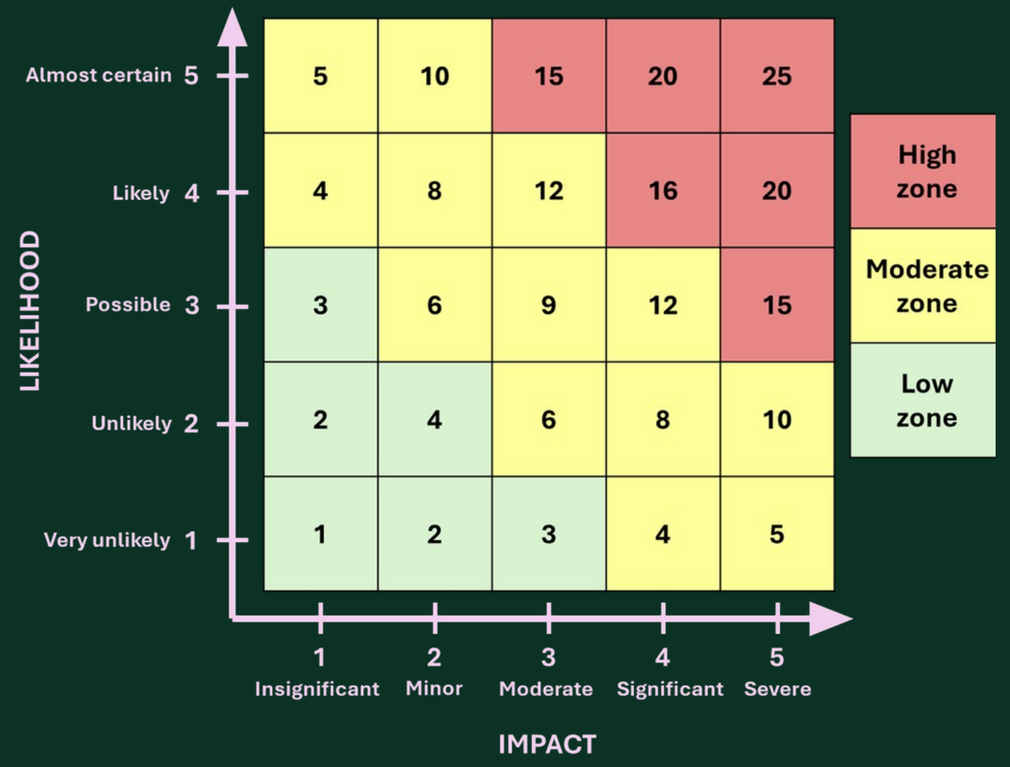
fortum
Powering a thriving world

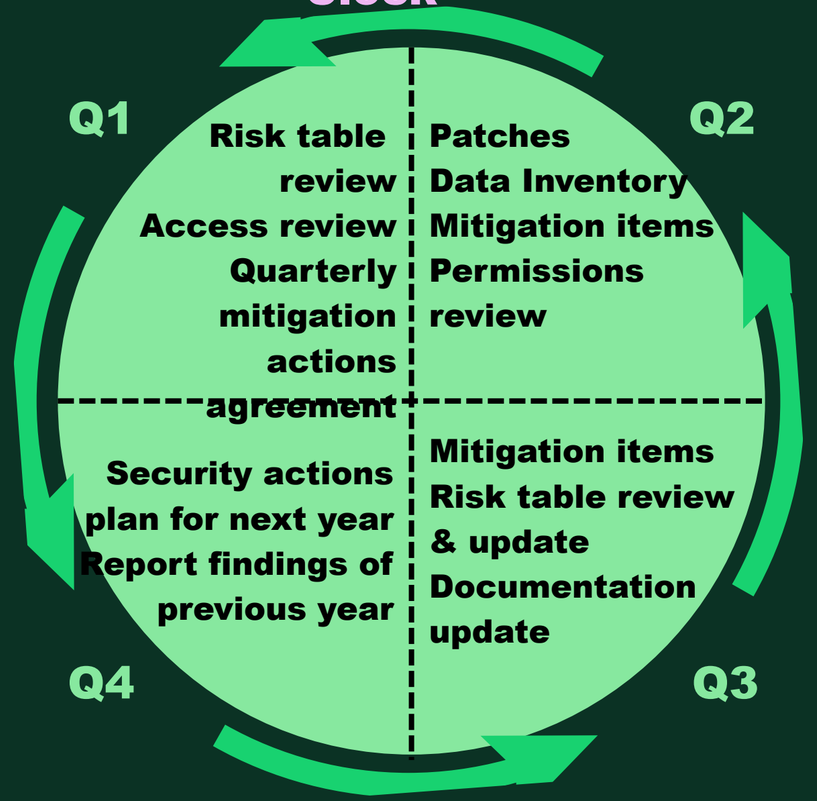
USEFUL TOOLS FOR GISSEC

Threat Modelling | Risk Assessment | Year Clock

Threat modelling in critical GIS environments

URN:
https://urn.fi/URN:NBN:fi:amk-2025111828483





fortum
Powering a thriving world

TAKE ACTION!

THREAT MODELLING
Identify critical systems, functions, and their vulnerabilities.

MONITORING
Actively monitor usage, traffic, logs, and anomalies.

EXERCISES AND SIMULATIONS
Regular exercises and simulations that cover potential scenarios.

CYBER HYGIENE
Updates, MFA, strong passwords, closing unnecessary services...

INCIDENT RESPONSE
Enhance response by automating actions to known threats (SOAR).

CONTAINMENT
Isolate affected systems or accounts.

PATCHING
Apply updates to fix vulnerabilities and exposure to known exploits.

RECOVERY
Restore systems and services to normal operative state.

fortum
Powering a thriving world

Functional plan of what WE do in an incident.

fortum
Powering a thriving world

So....

GRID RESILIENCE STARTS WITH GIS

https://www.linkedin.com/in/suvi-tuulia-haakana/

suvi.haakana@fortum.com

fortum
Powering a thriving world

THANK YOU

for your time and attention

https://www.linkedin.com/in/suvi-tuulia-haakana/

suvi.haakana@fortum.com

fortum
Powering a thriving world