techsmidt

Cybersecurity 2024

How to protect your assets, reputation, and operations.

Techsmidt is trusted by top tech brands & market leaders

Mojang Studios · Spotify · Nasdaq · King · Schibsted · EA · Klarna. · Hemnet · Zettle by PayPal · discovery+

We are all part of the **cyber threat landscape**

With COVID-19 came **an accelerated digitalization** and **new business opportunities**.

In our interconnected digital landscape, the same technology facilitating human and business connection also facilitates the sharing of innovations, skills, and tools among **global cyber threat actors**.

This escalating threat has raised concerns among governments and businesses alike, as **cyber attacks become both more frequent and complex**.

With **the rise of AI**, we need to anticipate intricate phishing schemes, a flood of deepfakes and social engineering, and hackers breaching target data while circumventing endpoint security defenses. We need to ready ourselves for the imminent surge of AI-fueled threats.

Cyber attacks should be viewed as a strategic tool, employed by malicious online actors to achieve their **political** or **financial objectives**.

We also have to recognize that **cyber risks are integral to the broader security landscape** and that hybrid warfare tactics are becoming increasingly prevalent, posing heightened cyber threats to governments and businesses worldwide.

It is **no longer a question of if** you will experience a cyber attack, but a question of when and how many.

And if so, **are you ready to manage cyber attacks?**

The most common **cyber attacks you have to manage**

The most common cyber attacks in 2023

Data breaches gain unauthorized access to, or disclose, your sensitive info.

Ransomware is a type of malware that encrypts your data and then demands ransom for access.

Phishing are fraudulent attempts to obtain sensitive info by targeting your staff.

Malware disrupts, damages, and gains unauthorized access to your IT systems and data.

Denial-of-Service (DoS) and **Distributed DoS** (DDoS) attacks overwhelm your IT systems with internet traffic.

Man in the middle (MitM) attacks intercepts your communication to steal or manipulate your data.

SQL injection injects malicious code into your databases to gain unauthorized access to your sensitive data and potentially manipulate or delete your database records.

Cross-site scripting (XSS) injects malicious code into your web pages.

Zero-day exploits exploit unknown vulnerabilities in your IT systems.

Insider threats are malicious actions by insiders, such as your own staff, core service personnel, etc.

Cryptojacking is unauthorized cryptocurrency mining on your IT systems.

Advanced persistent threats (APT) are long-term stealth attacks on your IT systems.

Ransomware is on the rise

Examples of ransomware

There are several different ways to get infected with ransomware, e.g through exploitable vulnerabilities, brute-force credential attacks, social engineering, previously compromised credentials, or abuse of trust.

→ **Akira Ransomware** and **LockBit Ransomware**
Akira and LockBit **encrypts the victim's files and demands a ransom to restore access**. Both Akira and LockBit are known for their ability to spread across networks and infect multiple computers. Akira has **possible links to the Russian FSB**, according to internal chat logs leaked online. Requested ransom sums of between $200k and $50M+.

→ **Qilin**
Qilin is part of a newer wave of cyber threats that **not only encrypts the victim's data but also steals information before encryption**. Qilin attacks are often tailored for each victim to maximize their impact and they use phishing emails containing malicious links to infiltrate the victim’s networks and steal and encrypt important data. Qilin threatens to publish the stolen information on the Internet if the ransom is not paid. This adds an additional level of extortion and **forces victims to pay to protect their confidential information**.

→ **BlackCat/ALPHV**
BlackCat, also known as ALPHV, is an advanced ransomware threat that has gained attention for its use of the Rust programming language, which increases its effectiveness and difficulty of detection. BlackCat **offers a Ransomware-as-a-Service (RaaS) model to its customers**, which means that it is distributed by several different criminal actors. Like Qilin, it is known to carry out **dual blackmail tactics**; both by encrypting the victim's files and by threatening to leak stolen data.

🚨 Ransomware accounted for 24 % of malicious cyber attacks and 72 % of businesses worldwide were affected by ransomware attacks in 2023.

Average cost per successful attack

$70k for SME

DDoS

DDoS attacks are frequently used as a diversionary tactic to divert the attention of website owners, allowing hackers to execute a more damaging secondary attack. Hackers can easily rent online resources for as little as $5 per hour to launch these assaults.

- → Use a DDoS mitigation service.
- → Use web application firewalls (WAF).
- → Establish a secure network infrastructure.
- → Continuously monitor website traffic.
- → Utilize intrusion prevention systems (IPS) to detect and block malicious traffic.

$4.9M

Phishing

Today, Business Email Compromise attacks are the most common type of phishing attack. In this case, attackers compromise or impersonate official company email accounts to deceive and exploit individuals in your organization.

- → Use a password manager.
- → Use antivirus software.
- → Use multi-factor authentication (MFA).
- → Train your organization to identify unsafe emails.
- → Don’t open emails that look spam or click on links you don’t know.

$5.13M

Ransomware

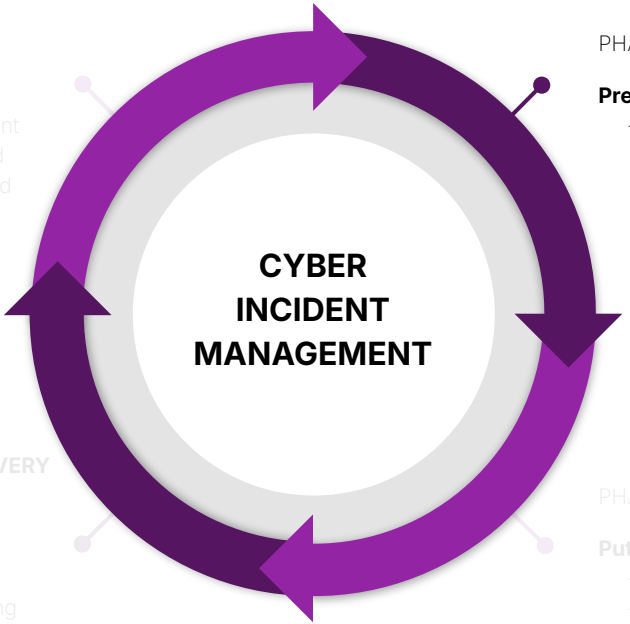
Ransomware-as-a-Service (RaaS) enables easy access to ransomware for a small fee or percentage of the ransom, democratizing its use. Cryptocurrency allows untraceable payments to cybercriminals, fueling the rise of large ransoms.

- → Conduct concise security training.
- → Implement visitor policies for physical security.
- → Perform regular risk assessments, including scans, patching, password enforcement, and centralized logging.

⚠️ An organization loses $1.3 million in the average data breach

techsmidt

How to **manage a cyber threat**



PHASE 1 - **PREPARATION**

Preparation is crucial for incident response.

→ Develop a strategy and processes, document it, build the incident response team, assign roles, ensure communication and training, and acquire necessary software and hardware.

PHASE 2 - **DETECTION AND ANALYSIS**

Put preparation into action.

→ Identify early signs of security incidents.
→ Analyze to distinguish real threats from false alarms.
→ Document incidents with relevant response procedures.
→ Prioritize based on impact analysis for efficient recovery.
→ Notify involved teams and explain the incident response plan for rapid recovery.

PHASE 3 - **CONTAINMENT, EXTINCTION AND RECOVERY**

Manage the situation.

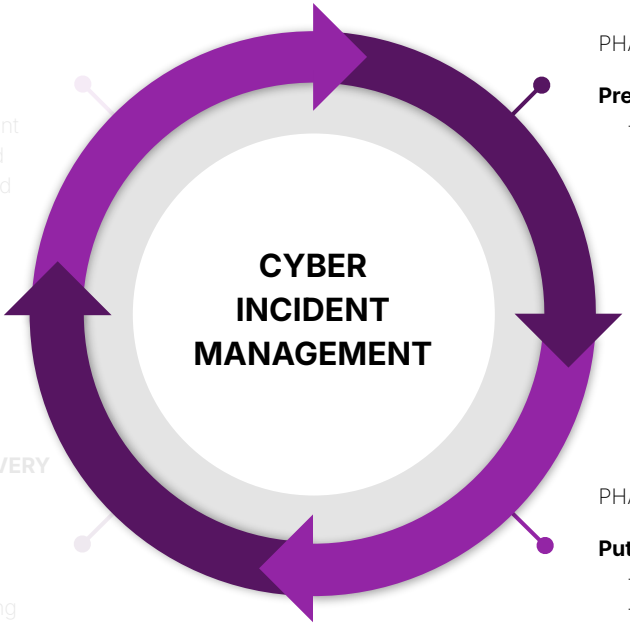
→ Containment aims to swiftly control events, minimizing further damage.
→ Identifying affected systems is crucial, applying incident response strategies for containment, eradication, and recovery.
→ Eradication involves using incident management tools and knowledge articles for swift resolution.
→ Recovery ensures systems are checked and reintegrated into the business environment, nullifying the threat.

PHASE 4 - **REVIEW** (post-incident analysis)

Learn and improve.

→ Perform post-incident analysis with the incident response team, organizational authorities, and involved individuals to capture lessons learned and assess the IR plan's effectiveness.

How to **manage a cyber threat**



PHASE 1 - **PREPARATION**

Preparation is crucial for incident response.

- → Develop a strategy and processes, document it, build the incident response team, assign roles, ensure communication and training, and acquire necessary software and hardware.

PHASE 2 - **DETECTION AND ANALYSIS**

Put preparation into action.

- → Identify early signs of security incidents.
- → Analyze to distinguish real threats from false alarms.
- → Document incidents with relevant response procedures.
- → Prioritize based on impact analysis for efficient recovery.
- → Notify involved teams and explain the incident response plan for rapid recovery.

PHASE 3 - **CONTAINMENT, EXTINCTION AND RECOVERY**

Manage the situation.

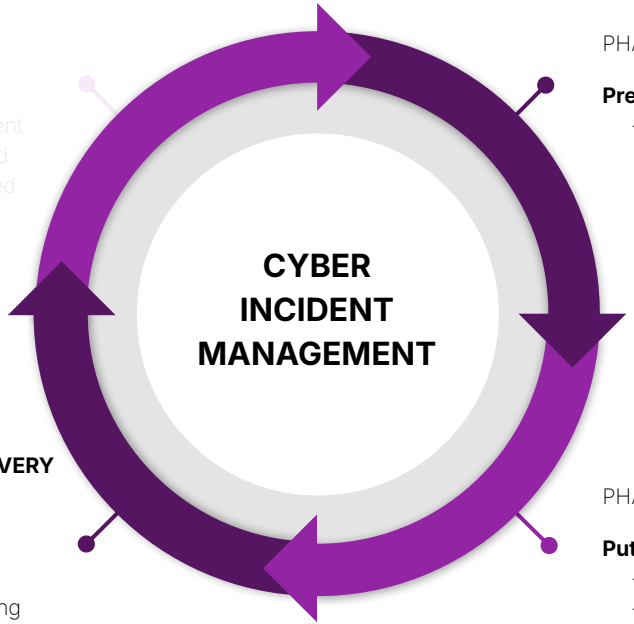
- → Containment aims to swiftly control events, minimizing further damage.
- → Identifying affected systems is crucial, applying incident response strategies for containment, eradication, and recovery.
- → Eradication involves using incident management tools and knowledge articles for swift resolution.
- → Recovery ensures systems are checked and reintegrated into the business environment, nullifying the threat.

PHASE 4 - **REVIEW** (post-incident analysis)

Learn and improve.

- → Perform post-incident analysis with the incident response team, organizational authorities, and involved individuals to capture lessons learned and assess the IR plan's effectiveness.

How to **manage a cyber threat**



PHASE 1 - **PREPARATION**

Preparation is crucial for incident response.

- → Develop a strategy and processes, document it, build the incident response team, assign roles, ensure communication and training, and acquire necessary software and hardware.

PHASE 2 - **DETECTION AND ANALYSIS**

Put preparation into action.

- → Identify early signs of security incidents.
- → Analyze to distinguish real threats from false alarms.
- → Document incidents with relevant response procedures.
- → Prioritize based on impact analysis for efficient recovery.
- → Notify involved teams and explain the incident response plan for rapid recovery.

PHASE 3 - **CONTAINMENT, EXTINCTION AND RECOVERY**

Manage the situation.

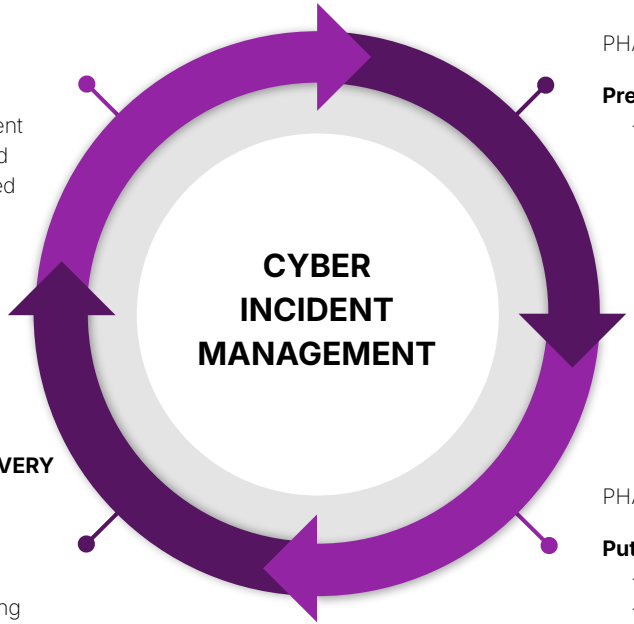
- → Containment aims to swiftly control events, minimizing further damage.
- → Identifying affected systems is crucial, applying incident response strategies for containment, eradication, and recovery.
- → Eradication involves using incident management tools and knowledge articles for swift resolution.
- → Recovery ensures systems are checked and reintegrated into the business environment, nullifying the threat.

PHASE 4 - **REVIEW** (post-incident analysis)

Learn and improve.

- → Perform post-incident analysis with the incident response team, organizational authorities, and involved individuals to capture lessons learned and assess the IR plan's effectiveness.

How to **manage a cyber threat**



PHASE 1 - **PREPARATION**

Preparation is crucial for incident response.

→ Develop a strategy and processes, document it, build the incident response team, assign roles, ensure communication and training, and acquire necessary software and hardware.

PHASE 2 - **DETECTION AND ANALYSIS**

Put preparation into action.

→ Identify early signs of security incidents.
→ Analyze to distinguish real threats from false alarms.
→ Document incidents with relevant response procedures.
→ Prioritize based on impact analysis for efficient recovery.
→ Notify involved teams and explain the incident response plan for rapid recovery.

PHASE 3 - **CONTAINMENT, EXTINCTION AND RECOVERY**

Manage the situation.

→ Containment aims to swiftly control events, minimizing further damage.
→ Identifying affected systems is crucial, applying incident response strategies for containment, eradication, and recovery.
→ Eradication involves using incident management tools and knowledge articles for swift resolution.
→ Recovery ensures systems are checked and reintegrated into the business environment, nullifying the threat.

PHASE 4 - **REVIEW** (post-incident analysis)

Learn and improve.

→ Perform post-incident analysis with the incident response team, organizational authorities, and involved individuals to capture lessons learned and assess the IR plan's effectiveness.

Cybersecurity is hard.

But **it’s not rocket science**.

Cybersecurity in a brief

Cybersecurity is the practice of **protecting your organization's digital systems**, **networks**, and **data** from malicious attacks, while **meeting regulatory demands**, and **supporting your business objectives**.

In today's interconnected world, where businesses and individuals rely heavily on digital technologies, cybersecurity is paramount.

It **encompasses a range of strategies**, including network security, endpoint protection, immutable backup repositories, encryption, IT security policies and processes, and user awareness training.

There are **well-established standards, processes, methods, knowledge and tools** that should be adopted and implemented in your organization.

By **implementing robust cybersecurity measures and staying creative**, organizations can safeguard their sensitive information, maintain operational resilience, and protect against cyber threats such as malware, phishing, and ransomware.

It’s all about **continuous improvement**

in **these five areas**

→ Governance
→ Organization
→ Processes
→ Information
→ Technology

How **we can help** you

1. **Cybersecurity Assessment and Improvement**
   We offer comprehensive cybersecurity assessments to identify your vulnerabilities, and then develop and execute tailored strategies to mitigate risks and strengthen your cyber defenses.

2. **Security Awareness Training**
   Recognizing the importance of human factors in cybersecurity, we offer engaging and interactive security awareness training programs to educate your employees and foster a culture of security within your organization.

3. **Incident Response and Threat Management**
   Our team provides rapid incident response services to minimize the impact of cyber attacks and proactively manages threats to prevent future attacks.

4. **Compliance and Regulatory Support**
   We assist you in navigating complex regulatory requirements and achieving compliance with laws, regulations and industry standards such as GDPR, Network and Information Security Directive 2 (NIS2), Digital Operational Resilience Act (DORA), Cyber Resilience Act (CRA), EU Cybersecurity Act (CSA), ISO 27001, and NIST.

About us

Founded in 2017, **TechSmidt specializes in cybersecurity**, **product development**, and **IT infrastructure**. With 225% growth over the past five years, we deliver cutting-edge solutions and expert consultants to clients in Sweden, Europe, and the US.

Our high-performing teams take ownership to the next level and execute with passion, driving innovation through value-driven and experimental projects. TechSmidt has **built products and provided protection for over 1B end-users worldwide**, securing their digital future.

Join us as we continue to lead in tech excellence and innovation.

Trusted by top tech brands & market leaders

Mojang Studios · Spotify · Nasdaq · King · Schibsted · EA · Klarna. · Hemnet · Zettle by PayPal · discovery+

Need our help?

Book a free strategy call

Book your call ↗