# WHAT IS THREAT REMEDIATION? BEST PRACTICES FOR REMEDIATING THREATS

Cybercrime is predicted to inflict $6 trillion worth of damages globally by the end of 2021 and $10.5 trillion annually by the year 2025, growing at 15% annually. This already makes cybercrime the third largest economy after the U.S. and China and, perhaps, the greatest (illicit) wealth transfer.

The damages are larger than any natural or other man-made disasters. Cybercrime is seen as a real threat in the business world and in fact given rise to the popular adage: your cybersecurity strategy is your business strategy.

Considering that cybercrime is a real threat facing all business organizations and cyber-attacks are inevitable, what can you do to mitigate risks?

*(This article is part of our Security & Compliance Guide. Use the right-hand menu to navigate.)*

## What is threat remediation?

Threat remediation refers to the active cybersecurity activity of identifying and eradicating a threat vector.  It is a key component of the cybersecurity strategy that deals with the security posture of your organization, how well your organization is capable of:

1. Responding to cyberattacks
2. Containing the damages

3. Eliminating the threat altogether

This final step in the security defense kill chain is what differentiates threat remediation from threat mitigation—threat mitigation involves actions on *reducing* the risk of threats instead of eradicating and remediating the threat altogether.

For example, your corporate network may be compromised due to a zero-day exploit in your network identity and security control devices. The threat remediation exercise would involve ongoing monitoring for anomalous behavior.

Considering the fact that the security vulnerability in the security control devices has not been identified and cybercriminals are already able to gain unauthorized access to your network, security monitoring systems would flag the vulnerable devices and prompt the responsible authorities to apply the necessary remediation measures to eliminate the threat. In this case, replacing the vulnerable device or installing a security patch to the firmware will entirely eliminate the threat.


# Threat remediation best practices

So how do you remediate cybersecurity threats effectively? The following threat remediation best practices can help boost your cybersecurity posture and eradicate persistent threats facing your organizations.

## Build security from the ground up

Threat remediation requires certain provisions within the systems such as:

- Business continuity
- High availability
- Capacity to upgrade and patch without impacting operations

This is only possible when security is built into the systems from the ground up. Instead of treating security as layers of defense that can be installed at later stages, build resilient systems that can be modified and improved to remediate security risks.

*(See how DevSecOps bakes security into software development.)*

## Discover & categorize assets

Identify and track your IT workloads, systems, and information assets—IT discovery. Organize a database of records that updates in real-time and keeps track of system and configuration changes.

## Evaluate business value & risk

Once you understand where your IT assets are located and how they behave, you can isolate critical assets based on business value and associated risks.

*(Learn about the crucial practice of IT asset management.)*

## Monitor & scan

The next step is to identify potential vulnerabilities and exploits in the IT network. Scanning and monitoring the network is an ongoing process that looks into network traffic behavior and data logs using advanced AI-powered pattern recognition systems.

## Prioritize vulnerabilities

Monitoring data can be overwhelming and not all vulnerabilities pose the same risk levels. It is important to quantify the impact risk of vulnerabilities and focus remediation efforts only on the most urgent risks.

*(Try the impact, urgency, priority matrix.)*

## Create a remediation process & frameworks

The threat remediation approach can include a variety of countermeasures. Frameworks such as the Cyber Risk Remediation Analysis (CRRA) help adopt a range of Tactics, Techniques and Procedures (TTPs) associated with specific threats with the following approach:

- Select TTPs to mitigate
- Identify plausible counter measures
- Assess countermeasure merit
- Identify optimal countermeasure solution
- Prepare recommendations

## Automate the process

Enforcing a systematic threat remediation framework at scale without delays and human errors can be challenging. Automating the process not only speeds up the process, but also enables a data-driven approach to threat remediation.

Automation systems can be used to experiment with various TTPs and extract insights to help

optimize the remediation efforts on an ongoing basis.

### Improve continuously

The threat landscape is constantly evolving. No single threat remediation strategy can guarantee optimal results over the long haul. It's important to constantly monitor the systems, identify threats, and future-proof both the threat remediation systems as well as your overarching cybersecurity strategy.

### Set the culture & provide training

A majority of threat remediation can come simply by nurturing a culture of security awareness and best practices at the workplace. These activities, among many, can go a long way in maintaining an effective cybersecurity posture:

- Providing regular training programs
- Rewarding behavior of secure operations
- Preventing malpractices such as shadow IT

## The best threat remediation is proactive & automated

Threat remediation should be viewed as an active approach to cybersecurity measures. It refers to the process by which risk is assessed, indicators are identified, and warnings are flagged, prioritized, and resolved in a cyclical fashion. Effective threat remediation considers context, makes available actionable data and is part of an overall cybersecurity program that includes more traditional measures like preventive anti-virus software and raising employee cybersecurity awareness.

Threat remediation processes can be automated with a vulnerability management system—such as BMC Helix Operations Management. The most valuable threat remediation software must provide relevant information about threats in a way that relevant people can easily access and consume them. It should be able to resolve priorities without human interaction.

## Related reading

- BMC Security & Compliance Blog
- What Is Zero Trust Network Access? ZTNA Explained
- The MITRE ATT&CK Framework Explained
- AI Cyberattacks & How They Work
- Security Analytics: An Introduction
- Top IT Security, InfoSec & CyberSecurity Conferences