RÉPUBLIQUE
FRANÇAISE
*Liberté*
*Égalité*
*Fraternité*

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

**REMEDIATION**
COLLECTION

# CYBER ATTACKS AND REMEDIATION

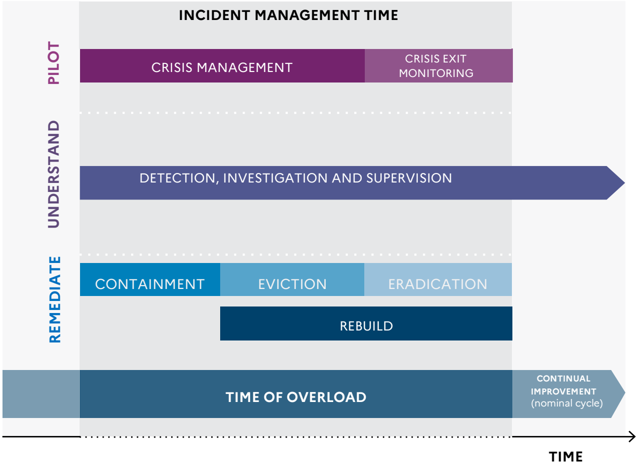
## THE KEYS TO DECISION-MAKING

ANSSI has published a set of remediation guides describing the principles for managing and implementing a remediation within an organization affected by a cybersecurity incident. The purpose of this strategic-level document is to define the main concepts necessary to understand the role of decision makers in the remediation process.

Remediation, along with investigation and crisis management, is one of the key aspects of the response to a cyberattack (business disruption or espionage). It is defined as the operations aiming at recovering the control of a compromised information system, and restoring it to a sufficient operational status.

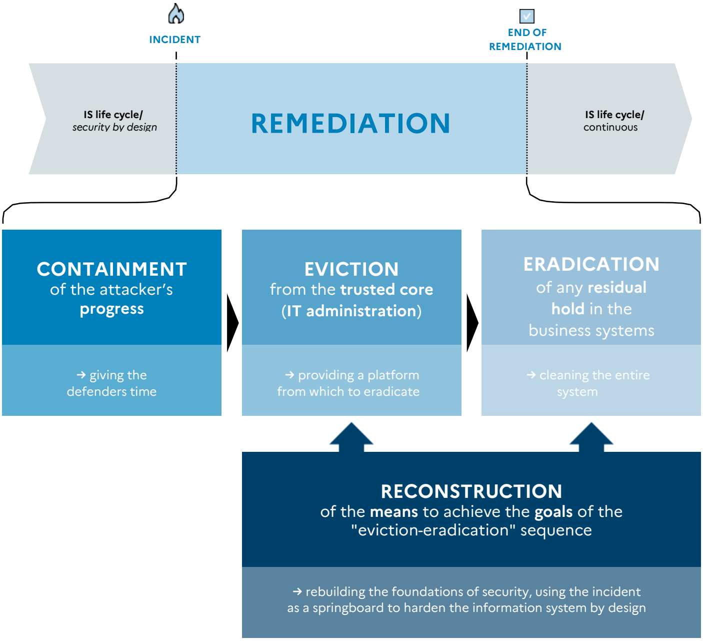
After a major incident, the remediation affects the life cycle of the information system for several weeks or even monthes, and impacts many business units during this period.

If the remediation is properly managed, the incident becomes an opportunity to significantly improve the resilience of the affected organisation. Decision-makers must set strategic objectives and quickly provide the necessary resources to reach them.



## DEFINITIONS: THE « CEER » SEQUENCE

Remediation can be sequenced according to the « CEER » diagram (*containment-eviction-eradication-reconstruction*):


INCIDENT
END OF REMEDIATION
IS life cycle/ *security by design*
REMEDIATION
IS life cycle/ continuous
CONTAINMENT of the attacker's **progress**
→ giving the defenders time
EVICTION from the **trusted core** (**IT administration**)
→ providing a platform from which to eradicate
ERADICATION of any **residual hold** in the business systems
→ cleaning the entire system
RECONSTRUCTION of the **means** to achieve the **goals** of the "eviction-eradication" sequence
→ rebuilding the foundations of security, using the incident as a springboard to harden the information system by design

The trusted core is the foundation of the information system from which the attacker has been completely expunged. It will be essential for carrying out remediation actions and its reconstruction is therefore a major step. Failing to rebuild it properly usually leads to a compromise/remediation cycle that can last for monthes or even years.

# CHOOSING YOUR REMEDIATION PLAN CORRECTLY: A MISSION-CRITICAL ISSUE

The damages from a cyberattack can amount to millions, even tens of millions of euros. Therefore, the orientations and resources provided to the remediation management are decisive for the future of the affected organisation.

This guide describes three scenarios, varying depending on the urgency to restart the business activities, and on the long-term costs incurred by the damages of the cyberattack. These scenarios are templates that must be adapted based on the actual situation during an incident. Nevertheless, they can serve as a basis for decision-makers to decide on the type of remediation that will be carried out.

### Scenario 1 - « Restore mission-critical services as quickly as possible »

Faced with an immediate threat to your organisation, a limited number of services must mandatorily be restarted. However, this approach will neither address the root causes of the incident, nor protect against a re-emergence of the attack in the medium term. Your organisation's survival remains in jeopardy.

### Scenario 2 - « Take back control of the IS »

You prefer to return the entire information system to its previous operating state as quickly as possible. It has not been restructured. Your organisation remains at risk, as long as substantial changes have not been made (administration protection, detection, etc.).

### Scenario 3 - « Seize this opportunity to establish a lasting control of your IS »

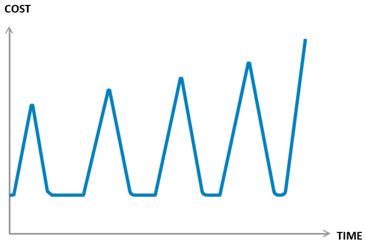
Since you must make major changes for remediation, you decide to seize this opportunity to change your security strategy. You choose to make a long-term investment to take back control and defend your information system. This approach enables you to adopt a proactive security model rather than a reactive one.

## REMEDIATION COSTS

The investments made in support of the remediation plan are decisive. They determine how the organization will resume its normal activity and how security will be managed. Depending on the chosen scenario, the remediation costs will be spread over the medium and long term.

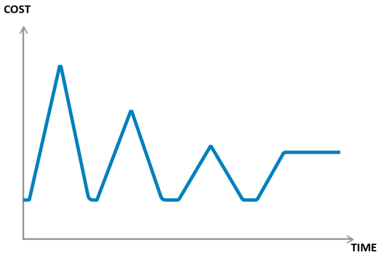
The cost graphs below are intended to illustrate and describe the major trends of the financial impact of a remediation. The goal of these diagrams is not to detail the costs of a remediation. They highlight the trend of these costs for an organisation affected by an attack, in the event of repeated resurgence of the incident.

### Scenario 1



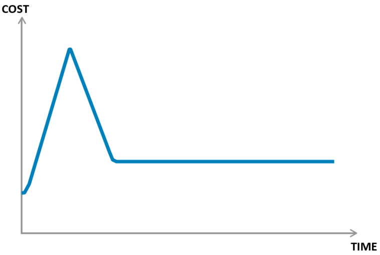
Urgently restarting mission-critical services has a low cost, but the risks of resurgence are high. This will require further remediation, resulting in a very high overall cost for the organisation.

## Scenario 2



The IS is back to its functional state prior to the compromise, as soon as the first remediation is carried out. However, the plan to secure the IS will spread over time and will once again impact the business activity.

## Scenario 3



The cost of the initial remediation is high, but it is a major opportunity to lay the foundations for state-of-the-art security. Ultimately, this investment will turn out to be very profitable. The organisation gains long-term control over its security.

## SEVEN RECOMMANDATIONS FOR A SUCCESSFUL REMEDIATION

### 1. Steer in the storm

Step back from immediacy: handling minute-to-minute activity is a never-ending task. Incidents are managed over weeks, sometimes monthes. Take the time to understand the situation and to have the available options explained to you, before making a choice.

### 2. Make structuring choices

Trying to deal with everything at the same time leads to the dispersion of resources and ultimately, failure. Only strong strategic decisions, confidence in the chosen strategy and significant financial commitments when handling the incident will have lasting effects.

### 3. Set strategic, business-focused objectives

The strategic objectives you must set determine the end of the remediation plan, and depend on one of the three scenarios presented above. These objectives are, notably, determined based on their impact on the business units' ability to work. Do not get caught up in fine-grained technical decisions, but take responsibility for their impact on your organization's business.

### 4. Stay aware

Remediation is a reaction to a hostile actor. Your opponent's actions may require adjustments. The game never ends.

### 5. Be flexible

Obstacles always emerge when implementing a remediation plan. You will need to adapt the resources, priorities and schedules, while maintaining clear and consistent objectives. Adapting actions while staying on course is one of the decision-maker's chief abilities.

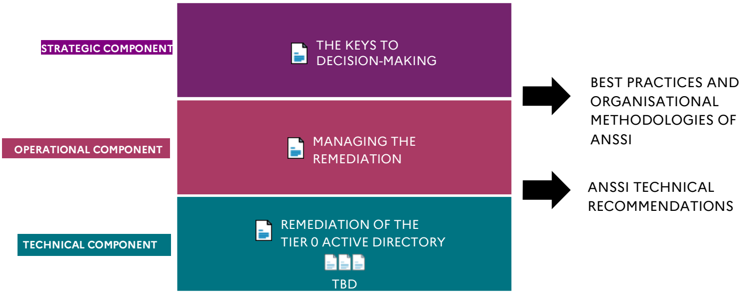
## 6. Keep your finger on the pulse

Once a remediation plan has been launched, your role is key to staying on course. Leadership, morale management and growing fatigue are crucial factors in the project's successful execution.

## 7. Keep your eye on long-term viability

Sound investments during remediation determine how normal business activity will resume and how security will be managed. A successful remediation project is not a substitute for a long-term security plan, but it can radically improve an organization's management of cyber risks.

# STRUCTURE OF THE CORPUS OF DOCUMENTS


STRATEGIC COMPONENT
THE KEYS TO DECISION-MAKING
OPERATIONAL COMPONENT
MANAGING THE REMEDIATION
TECHNICAL COMPONENT
REMEDIATION OF THE TIER 0 ACTIVE DIRECTORY
TBD
BEST PRACTICES AND ORGANISATIONAL METHODOLOGIES OF ANSSI
ANSSI TECHNICAL RECOMMENDATIONS

## FURTHER READING

Based on the information provided in this document, you have chosen a remediation option. You must now direct your teams to two types of documents:

- Operational documents (see the guide ***Cyber Attacks and Remediation: Managing the Remediation***) are intended for your CISOs, internal IT services and your remediation management teams. They will guide you through breaking down strategic objectives into technical objectives. These documents are intended to support the management of remediation operations during an IT security incident. They provide operational tools allowing technical team managers to manage the remediation project and its participants.

- Technical documents (see the guide ***Cyber Attacks and Remediation: Remediation of Active Directory Tier 0***) are intended for your operating teams. They detail the main areas of implementation to be considered during remediation. These documents guide your organisation through the technical actions to be carried out during remediation, for specific technologies (Active Directory Tier 0, etc.).

**REMEDIATION** COLLECTION

Remediation consists in recovering the control of a compromised information system, and restoring it to a sufficient operational status. Its strategic component, namely the guidelines and resources dedicated to managing the remediation, is decisive for the future of an impacted organisation. If it is properly managed, a cyber incident can become an opportunity for significant improvement.

Remediation, along with investigation and crisis management, is one of the key aspects of the response to a cyberattack (business disruption or espionage). It begins as soon as the intruder has been contained and can last several months.

Building on its extensive experience supporting organisations that suffered cyber security incidents, ANSSI has published a set of remediation guides describing the principles of remediation management and its proper implementation: the strategic component, the operational component and the technical component.

This strategic component will provide the necessary decision-making keys to set objectives and select a remediation plan.

Version 1.0 – December 2023
***Registered: December 2023***
Paper ISBN: 978-2-11-167195-9
Digital ISBN: 978-2-11-167194-2

**AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION**
ANSSI — 51, boulevard de la Tour-Maubourg — 75 700 PARIS 07 SP
*www.cyber.gouv.fr — communication@ssi.gouv.fr*