RÉPUBLIQUE
FRANÇAISE

Liberté
Égalité
Fraternité

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

REMEDIATION COLLECTION

CYBER ATTACKS AND REMEDIATION

MANAGING THE REMEDIATION

IF YOU ARE CURRENTLY VICTIM OF AN INCIDENT

If you are reading this paragraph, you may be looking for information on how to handle an IT security breach or crisis.

This document provides guidelines intended to help you organise and manage the technical remediation actions.

If you currently urgently need to manage an incident, you will probably not have time to read the entire document. However, you should at least read the recap provided in the lines below.

Remediation is one of the response activities to a cyber attack, together with crisis management and investigation. It is a project designed to lay the foundations for defenders to recover a lasting control of the information system. The remediation project is usually implemented in 3 steps and a background activity, collectively identified in this document as CEER[1] for containment-eviction-eradication-rebuild:

1. **CONTAINMENT OF THE ATTACK:** to prevent the incident from worsening.
2. **EVICTION OF THE INTRUDER FROM THE IS CORE:** to recreate a trusted foundation from which to undertake reconstruction.
3. **ERADICATION OF THE OPPONENT'S HOLD:** to eliminate the attacker's ability to return through backdoors left open during the intrusion.

[1] See Part I - Remediation Plan Development, section 1. Definitions: remediation and the "CEER" sequence.

While these steps are carried out, the “rebuild” activity recreates the infrastructure that was compromised or destroyed by the attack.

To carry out these steps effectively, an organisation must:

1. Identify and prioritise the strategic objectives with senior management (I.2.)
2. Break down strategic objectives into operational objectives (I.3.)
3. Mobilise resources to serve the operational objectives (II.2.)
   (a) Internal teams
   (b) Hardware and software
   (c) External support
4. Identify the project owners, prioritise and initiate sub-projects to fulfil the operational objectives (II.3.)
5. Monitor and coordinate the implementation of sub-projects to fulfil the operational objectives (II.3.a. and c.)
6. Throughout the plan, regularly inform decision-makers and operators of the overall progress of the remediation project (II.3.b.)
7. Rely on service providers, if necessary, capable of supporting the remediation management and implementation (III.)

Part IV, “Standard Plans”, presents check-lists corresponding to three standard scenarios for the remediation activity:

Scenario 1: ” Restore mission-critical services as quickly as possible ”

Scenario 2: ” Take back control of the IS ”

Scenario 3: ” Seize the opportunity to pave the way for a controled and resilient Information System ”

These scenarios are templates for the most frequently encountered guidelines. They must be adapted to each situation. However, these standard plans offer the advantage of providing operational examples for managing and implementing remediation.

Spare yourself and your teams. Remediation is a marathon that can take up to several months. All the teams' efforts cannot condense months into days, and an exceptional pace cannot be sustained in the long term. Manage time from the start: the ability to sustain the action plan over time is more important than the speed with which it is implemented.

For additional information more specific to cyber crisis management, refer to the best practices and recommendations from the guide "*Crises of Cyber Origin, the keys to operational and strategic management*". It should be noted that any remediation project not based on an investigation of the incident might not be relevant[2].

[2] See Part II - Implementation of Remediation, Section 6. Considering your opponent.

CONTENTS

INTRODUCTION

1 GOALS

This document provides a conceptual framework for remediation operations following a major cyber incident[1] compromising the integrity of an Information System (IS). In this document, remediation is defined as the operations aiming at **taking back control** of a compromised information system after such an incident, and restoring it to a sufficient operational status for the organisation survival.

This document is part of an ANSSI collection of documents[2] relative to cyber incident remediation. It is an intermediate level document between the strategic booklet, addressing senior management, and the technical level documents, detailing the implementation of remediation actions. More specifically, this document is **intended to assist in the design and execution of the remediation project at operational level**.

⚠ **Caution:** This document does not encompass all aspects of incident handling. It focuses on the specificities of the remediation project in the larger context of incident response. This activity supplements crisis management[3]and investigation[4]. Please refer to ANSSI publications dedicated to these activities for details on their proper implementation[5].
This document aims to provide the insights to organisation and decision-makers in an unfolding situation, but it does not replace the technical guides of the ANSSI, which are the only ones that give an in-depth view of the subjects addressed.

[1] See the definition in the glossary provided in the appendix.

[2] See Appendix A "Structure of the corpus of documents".

[3] See the definition in the glossary provided in the appendix.

[4] *Ditto*

[5] For more information, see the ANSSI guide: Crisis of cyber origin: the keys to operational and strategic management.

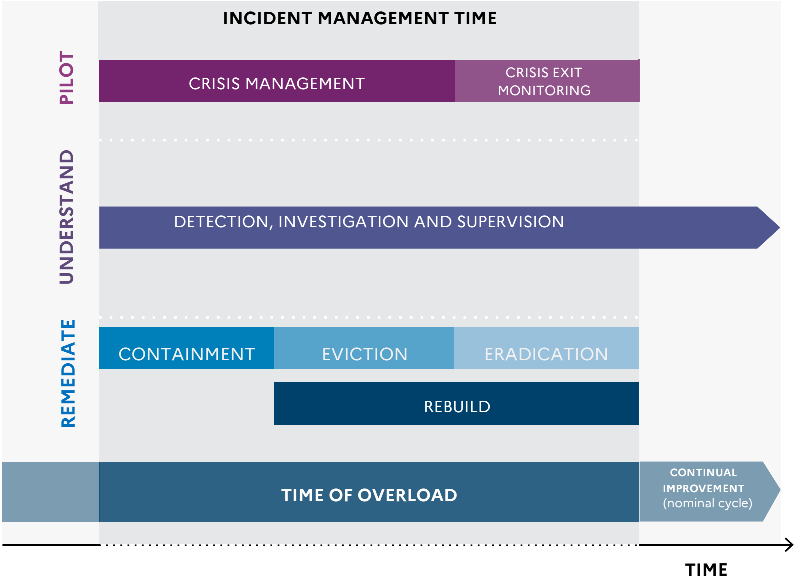


Figure 1.1 – Remediation within incident response

Remediation is an exceptional action. It takes place out of the normal cycle of an information system's continuous improvement of security, and assumes that the normal cycle will resume on exiting the incident. For the purposes of this document, remediation corresponds to the activities described in chapter 11 of the ISO 27035 standard "*Incident containment, eradication and recovery operations*"[6].

This document is not a reference document setting out a detailed process that must be followed. Neither is it the definition of categories of service providers capable of supporting remediation. Instead, it tries to present the options that each manager can implement depeding on the specificities of their situation.

2 AUDIENCE

This document is intended for managers in charge of handling the remediation operations following an information system security

[6] Standard ISO/IEC 27035: 2011, https://www.iso.org/standard/44379.html

incident. It is also addressed to their consultants and service providers carrying out the remediation operations. One of its aims is to enable operational managers to communicate the issues of remediation to their organisation's senior management and executive board.

3 STRUCTURE

This document has a four-part structure:

PART I - REMEDIATION PLAN DEVELOPMENT

This section is the core of the document. It presents a process for structuring the remediation plan around decision-making level objectives, and a breakdown of operational objectives.

PART II - IMPLEMENTATION OF REMEDIATION

This chapter provides an overview of the key points, in terms of IT security, to consider during remediation operations on the most commonly encountered elements of current information systems. This overview is intended as an introduction to the relevant technical guides, published separately.

PART III - REMEDIATION SERVICE PROVIDERS

This section provides support for the selection and management of services contributing to remediation operations, as well as for formulating calls for tenders and the key steps of implementation.

PART IV - STANDARD PLANS

This chapter describes the operational implementation of three typical scenarios of remediation based on their strategic goals. These plans propose a model of articulation between the decision-making, operational and technical levels.

PART I

DEVELOPING A REMEDIATION PLAN

Successful remediation requires designing and rolling out a plan. Because remediation starts in the heat of the incident and usually extends long after, it is critical to formalize this plan.A long-term security plan must extend the remediation actions and resume the continuous improvement process of IT security.

The remediation plan is therefore divided into one or more strategic objectives. Each of these objectives is broken down into operational objectives. To achieve each operational objective, a sub-project must be implemented.

In order to manage the plan implementation on the long run it is vital to order and rank all the objectives by priority.

The pace, participants and means of implementing this plan vary, not just with its progress, but also with the organisation's degree of preparation, and its control over the system before the incident.

Although remediation is a technical activity, it must be guided by the risks to the business line. An incident's severity is characterised by the extent of its impact on the business lines. If the disruption or threat to the business reaches a mission-critical level, the incident can be described as a crisis. For this reason, the remediation plan is carried out in cooperation with most of the affected organisation's stakeholders.

Major incidents and crises require setting up dedicated temporary management taskforces. Working in ' exceptional" mode is expensive. The organisation's resources are mobilised to the detriment of long-term activities, interrupting the cycles of continuous quality and security improvement. It is thus best to exit this mode as soon as possible, usually before the end of remediation activities[1], in order to ensure a transition to long-term security actions and a return to normal operation.

1 DEFINITIONS: REMEDIATION AND THE "CEER" SEQUENCE

Remediation is defined as the project to regain control of a compromised information system and restore a sufficient operating

[1] Upon destructive incidents, re-establishing essential services can take weeks or months. The long-term reconstruction of a controlled information system takes months, and often more than a year.

state. It begins when the incident is identified, and only ends when the strategic objectives have been met, which generally correspond to the restoration of services and the eviction of the opponent.

ANSSI summarises the remediation project as a sequence of three phases, accompanied by reconstruction actions, known collectively by the acronym "CEER".

1. CONTAINMENT Slows down the attacker in the information system by hindering its activity in order to give the defenders time and visibility.

2. EVICTION Permanently evict the opponent from a trusted core from which the less central parts of the information system are managed.

3. ERADICATION Clean the information system of any hold, even minor, that the attacker may have kept.

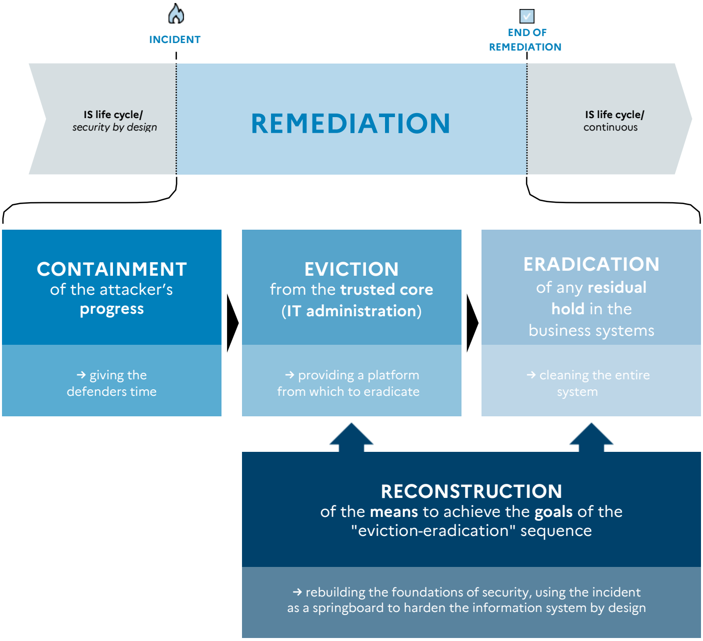
RECONSTRUCTION Reconstruction is a support activity for remediation intended to provide the IT resources necessary to restore the information system to acceptable operationnal and security state. It is run in parallel to the three previous steps. In response to a destructive attack (sabotage, ransomware), reconstruction is a key objective of remediation. In espionage incidents, reconstruction is more of a support of eviction and eradication. At the end of the "IT overload time", reconstruction will continue to gradually restore the information system and tighten its security.

Completing the CEER sequence should provide defenders with a controlled information system, where the attacker's attempts to return are detected and neutralised.

The sequencing of actions is organised in such a way as to minimise the risks of backtracking (re-breach), and limit the attacker's ability to inflict damage.

Eviction is central to the remediation project. Recreating a trusted core of the information system, secure and free from enemy control, gives the defender a platform from which the eradication can be carried out.

Failing this step typically leads to a breach/remediation cycle that can last for months, even years. This type of "digital guerilla warfare" is never won by defenders: the teams become exhausted and disheartened, and IT services get enduringly blocked, all with minimal efforts from the attacker.


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

2 STRUCTURING THE PLAN AROUND STRATEGIC GOALS

a - Control and validation of the remediation plan

In the *IT overload time* of the incident, remediation is started under an exceptional management structure. This structure should involve members of the business departments, internal IT services and the department in charge of security. Subsequently, the entity's normal organisation must gradually resume management of remediation.

Remediation is therefore not just completing a series of isolated technical tasks. It is a complex process requiring a high degree of communication and coordination, and sensitivity to business issues.

In particular, **the success of restoring a service or function is determined by whether the business line can validate that it operates as expected**, not by just restoring the infrastructure.

b - Structuring the remediation plan

The remediation plan is a project that translates strategic objectives into operational objectives, and operational objectives into technical actions.

For example, the strategic objective "pay wages at the end of the month" can be broken down into several operational objectives: "restore backups of the HR application within one week", "reinstall the HR application", "set up workstations for employee timesheets input", etc. Then, if we take a closer look, the operational objective "restore the backups of the HR application within one week" can be broken down into technical actions such as "install a restoration server", "re-index backup tapes", "restore HR application data from tapes", etc.

LEVEL	DECISION-MAKER	IMPLEMENTATION	DESCRIPTION
Strategic objective	Organisation Senior Management	Technical and Business Departments	Objectives for the organisation
Operational objective	Technical and Business Departments	Technical Department	IT department objectives
Technical actions	Sub-project manager	Technical operators	Actions on the IS

The remediation plan's design can therefore be summarised as follows:

1. identify the strategic objectives;
2. break down each strategic objective into operational objectives;
3. break down each operational objective into technical actions.

c - Identification of strategic objectives

The strategic objectives define the situation to achieve at each key stage of remediation. These are choices made by senior management based on business priorities.

They are formulated in non-technical terms and must be **prioritised** and given **specific deadlines**.

Strategic objectives must be **few in number**. Too many different objectives spread the resources too thin and lead to failure.

It can sometimes be tempting to change strategic objectives during the projet. However, these changes have a catastrophic impact on the organisation of remediation. One must therefore only change course in exceptional circumstances.

The strategic objectives must be few in number, prioritised, set in a timeline, and consistent over time: they are the target towards which the teams work.

These elements are essential for technical decision-makers to orient their actions. The absence of such objectives is a major problem. Over the course of an incident, the internal IT services could find themselves at odds with the business lines and senior management. In addition, the organisation's operation could be affected by poorly defined priorities.

Strategic objectives are drawn up with the organisation's business process managers, and approved by the organisation's senior management. It may be useful to rely on pre-existing risk, continuity or business recovery analysis to identify them[1].

[1] Specifically primary assets identification in risk management process or Business Impact Analysis from continuity management are fruitful sources of assets identification and prioritisation

Examples of strategic objectives:

- “Pay wages at the end of the month”.
- “Reopen partner access securely within two month”.
- “Restart deliveries within fifteen days“.

In part IV, this document proposes three standard scenarios illustrating different strategic priorities. These should be broken down into objectives specific for each organisation:

Scenario 1: ” Restore mission-critical services as quickly as possible. ”

It refers to the restoration of services being prioritised, with security cut back to the minimum to restart the service core. In this case, the other parts of the information system are temporarily sacrificed. This scenario should only be used in cases of extreme urgency, such as those jeopardising the survival of the organisation, presenting an imminent threat to the vital interests of the nation, or endangering people.

Scenario 2: ” Take back control of the IS ”

It refers to a protected return to the previous state of the information system before the breach. This scenario is characterised by a medium time investment, but enduring risk reduction is pushed back entirely to the continuous improvement phase.

Scenario 3: ” Seize the opportunity to pave the way for enduring IS control ”

It refers to remediation serving as a springboard to long-term security of the information system. This approach relies on a higher investment during the incident to restructure the system’s architecture and practices before returning to normal operation and restarting with an enduringly controlled organisation.

Each of these scenarios illustrates distinct trade-off that each organisation must weigh and then embrace. These three approaches are only illustrative, and the objectives of the remediation plan must be adapted to the organisation’s priorities.

d - Remediation and business continuity

It would make sense for business continuity and recovery mechanisms to be implemented when a cyber attack occurs.

Continuity activities according to the ISO/IEC 22301 standard, and remediation as defined in this document, are aligned: management by strategic objectives consistent with the business priorities, sustaining and restoring degraded activity. Ideally, remediation would be the implementation of a business continuity and recovery plan in the face of a cyber attack.

Unfortunately, at the time of the publication of these guides, cyber-related crises have yet to be included in business continuity plans on a regular basis. They rarely consider the possibility of an active breach prior to and during their implementation.

Furthermore, these guides are intended to assist implementation of a remediation plan during the time of IT overload linked to and incident situation, whereas most standards focus on preparing for it. Ideally, remediation preparation should be part of business continuity and recovery preparation activities.

⚠ During destructive incidents, or during the containment phase, **actions for activity continuity will certainly be put in place in parallel to remediation**.
These actions may be **based on Business Continuity Plans** (**BCP**s) but also on Business Impact Analyses (BIA) or risk analyses, which usually have already done the work of prioritising the company's critical assets.
During the phases of eviction, eradication and reconstruction of the business services, the **Disaster Recovery Plan** (**DRP**) may be used to guide activity recovery.
However, **most of these plans do not take into account, in their procedures, that an active attacker might be present in the information system**. It is therefore important to consider carefully whether to use these plans on a compromised information system, and to amend them appropriately during an ongoing remediation.

3 BREAKING DOWN STRATEGIC GOALS INTO OPERATIONAL GOALS FOR REMEDIATION

a - Principles

The implementation of the operational objectives is aimed at attaining the strategic goals.

This principle makes it possible to select and prioritise operational objectives: the priority of a strategic objective will be extended to the operational objectives it entails.

In a remediation project, each operational objective can be considered as a sub-project, with its own deadlines and resources.

Table 3.2 – Exemples of goal implementations

STRATEGIC OBJECTIVE	OPERATIONAL OBJECTIVE
Being able to pay wages for the current month.	▪ Reinstall the payroll software within one week. ▪ Reinstall a restoration platform during the week. ▪ Re-index backup tapes within ten days. ▪ Restore the latest healthy data for the payroll application before the last week of the month.
Reopen partner access	▪ Switch to multi-factor authentication on all remote accesses within two weeks. ▪ Implementation of specific enhanced supervision. ▪ Open selective traffic flows in firewalls.

b - Nature of operational goals

Most operational goals focus on implementing security controls. In this case, the long-term effect of attaining these objectives is an important factor to consider when deciding on the operational objectives to be carried out. For example, the skills required to maintain new security equipment must be identified and sourced.

Nevertheless, some objectives are different in nature and do not directly relate to security. For example, actions such as updating a mapping of services or restoring a backup, are operational objectives but not actually security controls implementation.

⚠ **Initiatives not serving as strategic objectives** are not operational remediation objectives. In a remediation process, such actions are commonly pushed because they already existed, or because of a wish to do things "properly". In an ***IT overload situation***, when managing a major incident, all resources, but in particular human resources, are under pressure. Actions that do not serve the objectives of the remediation plan will therefore divert valuable resources from these objectives. It is recommended to review action lists regularly to remove any actions that do not serve the strategic plan.

c - Developing operational goals

CHOICE OF OPERATIONAL GOALS

Operational goals must be selected based on several criteria:

- effect on the progress towards one or more strategic objectives;
- complexity and cost of implementation;
- capability to be sustained over time.

Ideally, a good operational objective should bring a strategic objective significantly closer. It should also come at a sustainable cost. Finally, it should be as enduring as possible so that it can be taken up as part of the cycle of the post-incident continuous security improvement plan. However, in most cases, it will be necessary to choose between these criteria.

The operational objectives must meet S.M.A.R.T. criteria:

Specific the objective must be defined unambiguously and understood by all in the same way.

Measurable it must be possible to determine whether the objective has been met or not.

Accepted all stakeholders must adhere to the objective. In particular, the various parties involved in it must be in agreement.

Realistic the objective must be achievable at the time of the crisis and with the resources actually available.

Time-limited the objective must have a limited time frame.

In essence, defining operational remediation objectives is classical project management but within a framework that is particularly constrained by time and resources. All standard best practices in this area apply.

The circumstances of incident management are affected by many unknown variables, and operations are carried out in a context of high uncertainty. It is not uncommon to come up against an unexpected obstacle while trying to achieve an operational objective. In this case, the management system must pay attention to progress and potential roadblocks, and remain flexible so as to adapt, or even redefine the objectives. To ensure this flexibility, remediation activities must be monitored closely and continuously by the organisation's senior management.

PITFALLS TO AVOID WHEN DEFINING OPERATIONAL OBJECTIVES

In the heat of an incident, hastiness might be mistaken for speed. However, the definition of operational objectives is decisive for the success of strategic objectives. It therefore should not be skipped.

The list below is obviously not comprehensive, but it does include a number of significant pitfalls to avoid.

Table 3.3 – Examples of frequent operational objective issues

PITFALL	DESCRIPTION
Focus on implementing the "miracle" security solution.	This pitfall is particularly common. Although often necessary, implementing a security solution (e.g. EDR) cannot by itself be sufficient to close a major incident. It should not monopolize all resources and attention.
Set unrealistic objectives.	The decisions taken when dealing with an incident are often marked by a desire to ensure it can never happen again. It is therefore tempting to set excessively high objectives and to exhaust resources in trying to achieve them. It is recommended to rely on experts[1] experienced in this type of situation, and to favor conservative objectives.
Set goals based on what is familiar rather than what is necessary.	In the stress of a crisis, it is natural to rely on existing procedures and practices. However, remediation actions should be guided by goals, rather than by habit. Thus, internal IT services, which are supposed to harden access to the Active Directory or configure audit policies, may tend to continue performing their routine tasks, such as EDR and network management.
Have scattered objectives.	In the absence of a centralized and prioritized plan, each team may tend to carry out simultaneous actions without mutual coordination. This results in overlapping actions and gaps, scheduling and synchronization problems, as well as an inability to complete the actions because resources are spread too thin. This type of problem can be worsened by a lack of communication between teams in normal times, and the exceptional intervention of personnel external to the organization. Remediation management involves coordinating objectives and technical actions from the moment they are defined, in order to minimize this risk.

Aim for overly complex technical actions.	In normal times, it can be difficult to define deadlines for an ordinary IT project. In the heat of an incident, this is twice as hard. Teams tend to overestimate their ability to carry out complex actions in a degraded environment and are likely to find themselves blocked after doing so. It is necessary to prioritise the simplest, most precise actions possible, even when making them more complex seems possible.
Maintain inflexible objectives in the face of obstacles.	The achievement of objectives must be closely monitored in order to detect blocked actions. Obstacles may arise from a variety of sources: mutual lock between sub-projects, inadequate choices given actual conditions in the information system, implementation problems regarding a technology, lack of skills or availability of key personnel, actions of the attacker, discovery of new information concerning the information system or the attack. It is normal to abandon or redefine actions during remediation. Managers and operators must also be made aware of this, so that they can coordinate around these issues.
Have long-term goals pursued exclusively by temporary teams.	Some actions require specific expertise: Active Directory hardening, implementation of network segmentation, audit policy configuration, etc. These controls need to be sustained over time. If no handover is scheduled between response teams and those required to maintain them in the long term, the level of security tends to drop once remediation is complete, sometimes very rapidly.
Validate service reopenings in purely technical terms.	Technical action owners are rarely able to verify that a business process is possible from start to finish. The problem is exacerbated by the involvement, during an incident, of external IT specialists, who have little knowledge of the organization's business. Thus it may happen that the technical team considers that services have returned to normal, while the business lines still cannot work. Validation by the business departments that a function has resumed properly avoids such pitfalls. This step must be scheduled when the operational objectives are planned.

Have competing objectives relying on limited resources.	The successful achievement of several competing operational objectives may depend on a restricted group of people or IT components with limited capacity. In that case, it is useful to identify such bottlenecks early on so as to prioritize the achievement of these goals and identify possible alternatives. For example, data restoration involves significant amount of data transfer and is limited by network, or even disk speed. It may therefore be best to target only a subset of the data and transfer it to new systems, or to sometimes restart the activity with a blank database.
Limit your choices to only technical or long-term options.	Achieving strategic objectives in the very short term generally requires putting in place temporary solutions, such as an isolated business network bubble, an internal courier system or a hard copy communication plan. These options must not be forgotten, even if they are intended to disappear once the incident has been resolved. Also, their sun-setting has to be planned and organized.

BUSINESS CONSIDERATIONS

Beyond IT resources, implementing a remediation plan to manage a major IT security incident also affects the entity's business lines. If the incident directly disrupts service capacity (for instance, ransomware), remediation operations may even interrupt all or part of the business activities. These business teams are generally the only ones able of identifying the consequences of technical or organizational changes on their ability to work, as well as the degree of priority for their activity resumption. They must therefore be represented in the organization and management of remediation. If a crisis management structure is put in place, it generally takes charge of organizing internal communication. For the person in charge of remediation, there are a number of reasons why close exchanges with the business units are essential:

→ **Identify impacts and business priorities** Work with the activity managers to identify the assets to be protected in priority and to

[1] See Part III – Services providers in remediation.

determine the order in which to restart processes. These priorities are defined according to their importance for the business processes. This information drives the strategy.

→ **Share goals** The operational objectives of the remediation plan are traced in information and arbitration notes. Business line managers must be informed of these choices in order to best adapt to them, or even have errors rectified before the actions are carried out.

→ **Involve business lines in the pace of reconstruction** For the duration of a major incident, business activities can be severely disrupted. Remediation should help address the highest priority issues with ad hoc solutions to minimize the impact of this disruption.

→ **Validate and coordinate service resumption** At some point, the main business services will be able to resume in a secure environment. This resumption must take place after validation, by the business lines owners, that their tools are working properly. It must be planned so that the human, commercial and logistical aspects are managed in accordance with the remediation schedule.

PART II

REMEDIATION PLAN IMPLEMENTATION

1 REMEDIATION IN INCIDENT MANAGEMENT

Remediation does not take place in an isolated context. The remediation project is part of an incident response or crisis management framework, whose progress is guided by management instances in sometimes distinct time frames.

However, operating in exceptional mode is costly and difficult to sustain over time. The final stages of remediation are therefore generally carried out headed by internal IT services and the normal business departments.

Coordinating these components properly and including them in a complex sequence requires a clear vision of the progress of the different processes, as well as significant communication between the participants.

2 REMEDIATION PHASES

The remediation project sequence is made of three successive phases: containment, eviction and eradication. Each of these steps should be handled carefully: excessive haste at a point usually compromises the following step, and requires redoing all or part of the previous steps.

a - Containment phase

Very early in an incident, actions can be taken to limit the attacker's freedom. These actions are not intended to expel the intruder permanently, but to limit the impact of the incident, or at least prevent it from worsening, while giving defenders time to prepare and take back control.

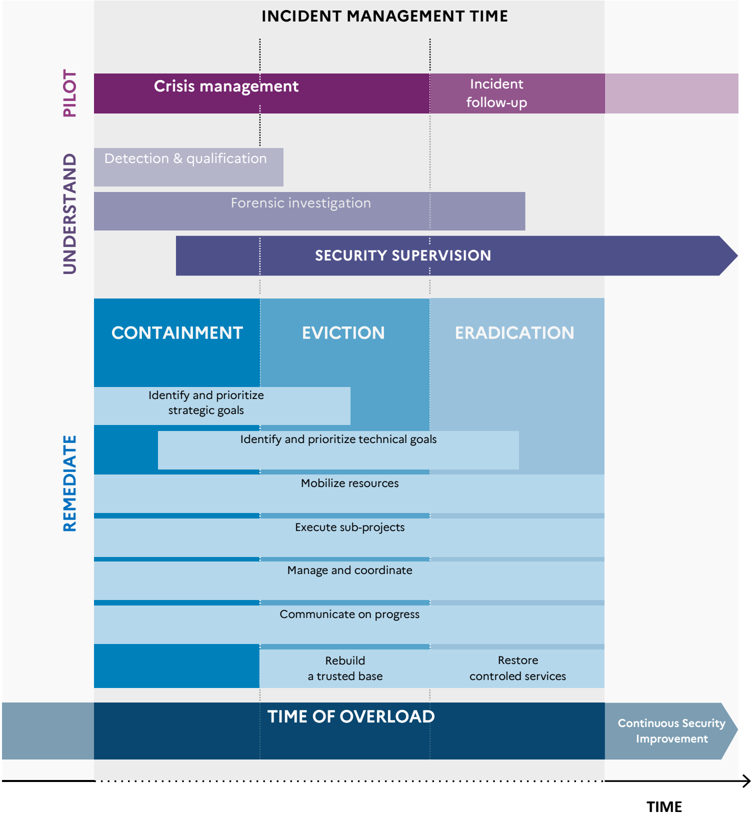


Figure 1.2 – Coordination of incident management and remediation

OBJECTIVES OF CONTAINMENT

→ **Preserve traces**

- preserving evidence that will be useful for understanding the incident.

→ **Limit the spread of damage**

- preventing the intruder from destroying traces;
- limiting the extension of malicious encryption or destruction of data;
- preventing the attack from spreading to other systems.

→ **Limit business impact**

- putting services or data of the compromised system out reach for the attacker;
- protecting information that is sensitive or necessary to rebuild the system.

⚠ **Preserving traces:**
Remediation activities destroy traces left by the attacker. These traces are essential for forensic investigation, which aims to establish the attacker's activities and serves as much for remediation itself, as for possible future legal proceedings. A balance must be found between the speed at which service is restored and the collection of information. In most information systems, a comprehensive collection of storage volumes is impossible. Analyses are therefore carried out on the basis of targeted forensic sampling, the selection of which is rarely possible beforehand.
Dialogue is therefore required on this subject with the teams carrying out the analyses and with any investigation department appointed by the courts of law.

→ **Limit the attacker's freedom**

- limiting possible communication channels;
- isolating the identified compromised resources.

→ **Gain knowledge about the attack**

- monitoring the identified or probable means of attack;
- forcing the attacker to use detectable means of communication.

POINTS OF INTEREST

Actions on a compromised information system are a form of communication with any attackers who may still be present. Any coercive action can be detected by the attacker and may trigger a reaction.

Consequently, containment actions must be selected with caution. This approach allows you to achieve your objectives, while keeping the attacker in the dark as much as possible on what the defenders may know of the attacker’s tactics, tools and procedures.

When serious actions are not imminently feared, it may be prudent to supervise the waypoints used by the attacker that have been identified, rather than hastily disabling them and forcing the attacker to use other means that have yet to be identified.

Containment actions are often one of the direct causes of information system failures. Strong traceability must be kept of any actions taken (typically by keeping a log). This will make it possible to trace the origin of an immediate or future failure. These notes also serve to remember that potentially disruptive controls have been deployed when returning to normal operation. Also, notes and logs are often useful when dealing with a court of law and insurance.

EXAMPLE OF CONTAINMENT ACTIONS

- Internet access blocked by filtering on the external firewall.
- Securing backups by disconnecting them from the network.
- Level 2 network segmentation on Ethernet switches.
- Switching off sensitive machines.
- Backup of virtual machine snapshots.
- Disassociation of selected services from the Active Directory Domain.

b - Eviction phase

Eviction aims to recreate a secure enclave controlled by the defenders, from which to carry out the actions for reconstruction and eradication of the attacker's hold. This trusted core[1] is the foundation on which the entire information system relies. If the eviction operation is not perfect, the attacker is likely to circumvent the controls put in place to compromise the system once again. Rebuilding a trusted core is essential to secure the system, but it is only the beginning of the process.

Although often relatively short, eviction operations require specific preparation and precise implementation. If these actions fail, remediation must be restarted from the containment.

OBJECTIVES OF EVICTION

- Create a system and network foundation beyond the attacker's reach.
- Implement reliable means of administration.
- Reconcile the need for guarantees regarding data imported from the compromised system (typically users and machines directories and part of the authentication data), and minimize reconstruction work.
- Build the authentication and trust system management services on which to base the return to production of the information system.

EXAMPLES OF EVICTIONS ACTIONS

- Recreate a virtualization infrastructure.
- Create a network segmentation isolating sensitive components.
- Switch from a compromised Active Directory to a healthy directory.
- Create dedicated and hardened administration workstations.

IMPLEMENTATION OF EVICTION

Eviction operations must be carefully prepared: identification of the minimum trusted core scope, architecture of the new infrastructure, acquisition and installation of servers and administration workstations, planning of changes to secrets and identifiers.

It is recommended to plan for an abrupt switch from the compromised system to a controlled system. The suddenness of the change should

[1] See the definition in the glossary provided in the appendix.

reduce opportunities for the attacker to adapt and compromise the new trusted core during its transition to production.

Depending on the pace of the incident, preparation for this switch-over can extend over several days or even weeks, while implementation takes place within a few hours.

Since eviction affects the core infrastructure of an information system, even if well prepared, its impacts extend to services beyond the scope of the trusted core. Operations to solve IS problems related to eviction must therefore be expected and may last several weeks [2].

It is essential to prepare the post-switch-over period with the IT administration teams, who will have to resolve the incidents induced by these changes, before the eviction starts.

POINTS OF INTEREST

It can be tempting to create a protected trusted core through an accumulation of security controls. However, each control imported into the trusted core must be managed from within it. Otherwise, such an action potentially constitutes a source of compromise for the trusted zone. For example, the deployment of an EDR in a trusted core requires that its console be included in this area. Similarly, the use of virtualization in the trusted core assumes that the administration of hypervisors is included. Moreover, the proliferation of imperfectly overlapping controls often provides only minimal security gains, but at a significant cost in terms of management complexity and performance. Experience shows that it is preferable to minimize the elements included in the trusted core and to manage the core's security specifically relative to the rest of the information system.

Moreover, it is risky to attempt partial evictions by trying to clean up compromised systems, without creating a trusted environment. In some rare cases, this approach is the only one possible. However, cleaning up an environment compromised by a skilled attacker is very difficult, and cases of re-compromise are not uncommon. Having high standards for the eviction aims to avoid "attempted eviction"/"re-compromise" cycles,

[2] This impacts are minimal if the information system has been partially or totally destroyed during the incident. But there are always user accounts in scripts, misconfigured computers or services shutdown and restarted in an improper time frame that have to be manually addressed.

which exhaust and demoralize teams due to often unsatisfactory results. The strategy of a simple cleanup of the trusted core is therefore only recommended when one has a very high degree of confidence of having identified all persistence points of the attacker.

Finally, it is sometimes tempting to recreate an entire information system, without reimporting any element of the compromised system. It has been observed that while most of the central functions of a system of moderate size can quite easily be reconstructed in this way, the return to normal operation soon hits many obstacles that can be difficult to overcome. This approach is particularly problematic in centralized identity systems[3]. In this configuration, the access rights applied to resources distributed throughout the system (files, email accounts, access to services) usually depend on unique centralized identifiers. Since these identifiers change when reconstructing from scratch, they must be corrected everywhere. This type of reconstruction should only be attempted on smaller or highly controlled systems.

c - Eradication phase

Eradication is the last step before returning to a normal service. During this phase, the defenders seek to eliminate any persistence of the attacker in the information system and to implement security controls to prevent the attacker's return. This is done by operating from the trusted core built at the time of eviction.

In practice, it is never possible to be certain that total eviction has been achieved. Security supervision must be set up to detect any return attempts that might not have been anticipated.

On most information systems, eradication cannot be carried out abruptly. The process is generally phased by IS sector and gradually returns all areas to a controlled state.

OBJECTIVES OF ERADICATION

- Remove the attacker's accesses.
- Eliminate all possible return channels for the attacker.
- Acquire visibility of any return attempts.

[3] Such as in, but not exclusively, Microsoft Active Directory environments

EXAMPLES OF ERADICATION ACTIONS

- Deploying EDR and supervision across workstations.
- Breaking down the IS into sub-systems[4] and migrating each of these into a controlled architecture, either inspecting or reinstalling the machines.
- Implementing a detailed collection of events (Windows events log, Syslog, traps) and a campaign to find evidence of the breach in the logs collected.
- Systematically using compromise detection tools with markers associated with the attacker.
- Migrating data to new service instances.

POINTS OF INTEREST

The eradication stage can be very long. There are multiple persistence possibilities for an attacker in an information system[5]. Most only activate a small number of them, but eradication can never guarantee that they have all been discovered. It has been observed that overly ambitious objectives are often abandoned during implementation, due to the depletion of resources. It is therefore preferable to aim for a lower degree of confidence on the completeness of eradication, while supplementing it with detection and response capabilities.

The goal of the remediation is to achieve a system on which any adverse activities can be detected and neutralized before becoming critical. Its aim is not to tend towards perfectly a watertight system.

It is generally impossible, on a large scale, to have the certainty that no backdoor, flaw or configuration change have gone unnoticed. It is preferable to prioritize eradication efforts on sensitive points, to segment the information system and to adapt the level of hunting effort to match the criticality of each considered zone.

Furthermore, during eradication, it is tempting to simply focus on technologically controlled systems: workstations and servers running on

[4] The breakdown of operations can follow geographical lines, be done by business unit, or prioritized by sensitivity of services...

[5] Persistences can be attained by implant installation, by modifying configuration or access rights, by creating or altering local or system-wide accounts...

Windows or even Linux. However, if the attacker compromised the information system, he may have compromised less-monitored components[6], such as:

- **Network equipment:** routers, switches, firewalls, VPN terminators.
- **Rarer systems:** mainframe, mini-computers, less common UNIX systems.
- **Equipment connected to the network:** printers, storage bays, cameras, telephones, industrial PLCs[7].

Although it is rarely possible to investigate all these equipments, the possibility that they might be compromised must be considered during eradication. Inspection, isolation, reinstallation or supervision of these devices should be considered.

RECONSTRUCTION STRATEGY

To facilitate containment and gradually rebuild the IS, two alternative approaches are preponderant:

→ **Isolation** the IS is divided into sub-networks isolated from each other, the services provided by each of them is then put through dedicated clean-up processes that can be carried out separately. The reopening of traffic flows between these networks is gradual and very focused. This type of approach requires detailed knowledge of application network flows and the ability to quickly identify them.

→ **Protection** a new healthy network is created, in which clean services are gradually reinstalled or reintegrated. This type of approach generally raises issues linked to hard coded addresses and network configuration.

These two approaches generate considerable work for technical teams, work that must not be neglected. They also require prior confirmation

[6] Quite often those are based on legacy systems, non updated software and with default passwords. The attacker may alter their configuration to compromise the system security, but they are often only used as unmonitored systems where nobody can see its actions.

[7] Notably, even in non industrial organizations, with building automation control systems.

that the network infrastructure can be trusted[8].

3 MANAGING REMEDIATION

Remediation management is an activity in its own right. This task is primarily akin to project management and action monitoring.

This is a specific project to manage, that requires numerous arbitrations and interactions with a wide range of people, under constrained circumstances.

In particular, a distinction must be made between[1]:

- crisis or incident management, which structures the organisation's strategy in the face of the attack;
- managing the investigation, which aims to establish the timeline of the attack;
- managing the remediation project, which consists in organising and monitoring the implementation of remediation actions.

Combining these roles in a single person is rarely effective for any major incident. Not only is the workload usually excessive for an individual, but different skills are required for each of these tasks.

a - Responsibilities

The remediation manager or managers are responsible for drawing up the remediation plan, monitoring the execution of the tasks, and qualifying their changes.

They are supported by experts when making complex technical choices.

They present the choices and changes in priorities, and request the crisis management or the business process owners to arbitrate them.

[8] Advanced threats will frequently implant network equipment such as routers or firewalls. A remediation strategy should only rely on such equipment if a good level of assurance can be reached regarding their non-compromise. If not, replacement or factory reset should be considered.

[1] The table describing the relationship between remediation and other activities in the incident can be found in Part II. — Remediation plan implementation, section 1. Remediation in incident management.

An important role in managing remediation consists in monitoring that the plans are followed properly, as well as ensuring that the problems encountered are correctly shared and, if necessary, arbitrated as early as possible. In particular, new information obtained through the investigation must be taken into account to steer the remediation, and may lead to actions, or even operational objectives, being postponed or abandoned.

b - Communication

Communication on remediation is part of the broader context of crisis communication[2].

Several key recipients can be identified for remediation communication:

- → **Decision-makers** must be informed of the progress, needs and problems encountered, without being overwhelmed by excessive detail. In order to avoid overly technical communications, and a “tunnel effect” where the project does not provide information on its progress, it can be prudent to define a communication dashboard or summary that is frequently updated. The crucial points to communicate are the remediation schedule and its possible delays, as well as the monitoring of the risks associated with each step.
- → **The remediation teams** must benefit from a frequently updated view of the project’s progress and critical stages. Since several groups are working in parallel, it is important to provide all the teams with information on the progress of each. Even when each task is broken down by team, it is essential to retain a view of the overall picture to ensure that all actions are consistent. Multidisciplinary teams should be given priority over specialists, in order to have in mind the context of any action when it is carried out. Progress summaries and multi-weekly reviews are generally the vectors for this communication.
- → **The business departments** are affected by remediation either in whole or in part. They will not be fully involved in all stages of technical reconstruction, but should be given a view of remediation throughout implementation. The key points are the timing of remediation and changes in business processes. This communication does not necessarily need to be very frequent. However, it must be kept up to date as the operation progresses. The involvement of the business departments, as well as feedback on the successes and

failures of remediation, contribute greatly to maintaining the cohesion of the organization during the incident. Complex arbitration on the reconstitution of the functions of the organization must also be made with the business lines. This communication generally takes the form of weekly updates.

→ **The rest of the organization** For operational security reasons, the details of remediation should usually not be shared with the entire organization. Nevertheless, it is necessary to ease the changes brought about by remediation. To do so, the key messages usually relate to communication on the existence of a security project, and especially to the preparation and support of security controls. This communication generally takes place by email, but also by sharing documents, FAQs and contact points.

→ **External partners** Public communication is not the responsibility of the remediation team. However, the changes made to the information system have an impact on customers and suppliers. In particular, the implementation of security controls, such as enabling multi-factor authentication, requires communication specifically addressed to them.

The messages linked to these changes must therefore be synchronized with the crisis communication, to make sure they are in line with the facts observable by third parties.

c - Teams

In the heat of a major incident, cross-functional cooperation is vital. The usual processes of the organization are often degraded, and the decision-making processes shortened. The advancement of remediation at the operational level can easily be blocked by cross-entity validation needs. Moreover, IT departments are rarely capable of validating recovery of an activity on their own, or identify its business priorities.

Lastly, there is a high risk of a disconnection between teams working intensively on the remediation and the rest of the organization, which is often paralyzed. Including the business lines in the remediation sub-projects is therefore essential. Ideally, the teams responsible for restoring a service should at least include:

- a manager;

[2] For more information see ANSSI guide: *Anticiper et gérer sa communication de crise cyber* referenced in appendices.

- one or more persons from the IT department with architectural and technical knowledge;
- one or more persons involved in the business line covered by the sub-project, and with knowledge of the processes;
- one or more technical experts required to implement the actions on the information system.

A sub-project may be focused on a segment of the information system subject to specific regulatory or operational safety constraints[3]. In this case, other experts shall be included in the arbitration to ensure compliance, safety and security in the remediation.

4 REMEDIATION EXIT

a - Definition of exit conditions

The end of the remediation project is reached when **all strategic objectives have been met**. The levels of expected services must be set realistically, otherwise they will fail.

Eradicating the attacker's hold on a large computer network is a tedious task. The system comes back to life as soon as services are restored, and re-contamination occurs frequently. The eradication goals should be designed according to the criticality of the systems or their exposure to a return intrusion. Except for the simplest cases, it is unrealistic to aim for total certainty of eradication. By contrast, it is possible to eliminate any presence from sensitive areas and to process any that remain when they are detected subsequently.

The same applies to the restoration of services after a destructive attack. The attack will have changed the practices, as well as the organization and its support systems. Some services may be permanently abandoned or reformed. In some cases, the attack might speed up implementation of a migration plan. In the most extreme cases, recovery of some services is simply impossible due to the data lost. It might also be considered simply too costly relative to its interest.

[3] Industrial control systems, or health related systems for example.

The definition of the expected service levels at the end of the remediation process is therefore crucial.

When assessing the achievement of objectives, a balance must be sought between the expected service levels and the duration of the remediation effort. The criteria are usually explained in the definition of the operational objectives. However, they are often reassessed during the remediation process. Indeed, the ability to achieve these objectives, the associated difficulties and the cost of remediation of some sub-systems all tend to be better understood over the course of the operation. When the objective completion levels are changed, they must be validated by the different management levels and quickly communicated to the stakeholders.

b - Exit time frame

If the remediation plan is effective, a first form of return to normal operation may be achieved before it is completed. This incident exit point is mainly characterized by an ability to return the business lines to most of their capabilities prior to the incident. But the IT overload time, might extend long after this moment.

At this stage, a trusted core for administrative actions makes it possible to ensure privileged accounts are protected. The main business applications are restored in a more secure environment. Although during this period business capacities are hardly ever fully recovered, the mission-critical activity of the organization is restored for the moment in a protected environment.

The actual end of remediation can take place a considerable time after this restart. Successful transitions are only achieved with support from senior management. Consequently, only coordination between the remediation team and the strategic decision-makers of the organization can make it possible to sustain the effort over time.

For this purpose, it is essential to:

- continue to communicate periodically the progress of remediation with the decision-making body;
- support privileged users (administrators, developers) in the transition of their practices;

- provide feedback to the entire organization on remediation and its objectives in order to minimize the after-effects of the crisis exit.

c - The risk of early demobilization

The crisis exit is also the time when most exceptional organizational and technical arrangements are dismantled.

However, this phase is psychologically complex:

- In the crisis, a substantial part of the organization, or even its entirety, is fully focused on the incident.
- At the crisis exit, the teams involved in remediation still have a lot of work to do, while the rest is demobilized.
- For privileged users of the information system, this is also a critical time, when the justification for exceptional care is dropping. Secure administration practices have generally not yet become a reflex and add to the workload of operators.
- Thus there is a risk of abandoning remediation halfway through and returning, for practicality's sake, to unsafe operating practices.

At this stage, the cost of the incident is still present in everyone's mind, and the impact of a relapse is generally well understood. But this awareness can quickly fade once the activity recovers.

d - After remediation is complete

Like all activities included in incident management, remediation must also involve the gathering of feedback.

Security incidents and reconstruction operations provide unique opportunities to highlight the strengths and weaknesses of an information system and an organization. This feedback can not only help prepare for potential future incidents, but also feed into the ongoing security improvement process. In particular, feedback from remediation must serve to draw up a post-incident security action plan.

A considerable proportion of the teams involved in remediation are specialists external to the organizations affected by the attacks. It is therefore advisable to carry out “on-the-spot” feedback collection phases in order to include people who may later be unavailable.

The other aspects of remediation feedback are based on the different practices implemented in the context of crisis management or a security incident.

e - Common problems with the business restart

An information system is almost never restarted in its entirety. When this occurs during an incident, many problems are likely to arise. The consequences of poorly managed recovery for the business lines can range from excessive recovery time to unrecoverable losses or data corruption.

In order to minimize the risks of this type of failure, it is necessary to carefully plan the order in which the services of the organization will be restarted, identify the tests to validate that each step has been completed correctly, and to plan “go/no-go” points for the progress of the restoration operations.

There are number of recurring problems when large-scale changes or restarts of the information system take place. They require careful consideration.

Table 4.4 – Common problems when restarting services

PROBLEM	DESCRIPTION
Circular dependencies.	Scheduling a system restart requires not only identifying technical dependencies (those between an application and its database), but also organizational dependencies (e.g., the need for an e-mail service to receive data processed in an application).

Return to service of previous data.	Restoring application data is often a delicate operation that plans do not provide for. First of all, there must be enough disk space to store them ,often more than twice the data size, since the copy returned to service often needs to be converted to another format. Sometimes it is even necessary to be able to store several times the size of the data, due to the temporary files generated during mass re-import. In addition, if the data is sensitive for the business or for the security of the information system, the choice of date to restore represents an important decision, often made at the highest level. Data that is too old loses value and frequently requires intensive updating work. Recent data may have been altered by the attacker in order to produce an adverse effect or to perpetuate their access. Knowing when the breach occurred will be decisive in making this choice.
Synchronization with external services.	Restorations or interruptions create a differential between two services. It is always possible for desynchronizations to occur. The most common are expiration of identification data or loss of cryptographic key rotation. It also happens that some services expect a continuity of chronological or counter sequence, and that a forward or backwards leap leads to failure. Preventing these problems requires identifying the external dependencies of the applications, if there is a need to recreate associations or synchronizations. It may be necessary to force some counters, or even create synthetic data to fill gaps.
Recovery of business data generated during the crisis.	Depending on the complexity of the applications, the reconciliation of data generated during the crisis with previous data can be very complex. An IT security incident usually lasts several weeks, sometimes several months. In general, instances of critical applications are restarted in temporary configurations to cover this period. These applications will generate data before they can be reintegrated into a reconstructed instance. Merging operations can force arbitration on information losses, or delicate export, filtering and re-import operations. Prior consideration of the subject is decisive in resolving this type of issue.

Corrupted states due to partial restarts.	Restarts in emergency situations, even if well prepared, frequently fail. Unknown elements are discovered, containment controls block communications or executions; buried scripts called indirectly have been lost, etc. These incidents can quickly become blocking points if they are not anticipated. A procedure to return to the previous state must therefore be planned for at this stage, in order to be able to correct the problem and clean up the remaining parts of the failed attempt. For each step, the business must set up a process for validation of the results.

5 REMEDIATION LOGISTICS

a - Limitations of internal capacities

Remediation of a compromised information system is a cumbersome project.

The teams in charge of day-to-day IT see their priorities change and their workload increase significantly over a short period of time. Even when abandoning routine tasks, internal teams are rarely able to sustain this increased workload without external help.

Furthermore, remediation work requires specific areas of expertise: Active Directory technology, hypervisor configuration, restoring complex applications. These skills are rarely all available within the organisation.

But, it is important to ensure that the knowledge acquired during the incident is preserved internally and not to rely exclusively on external service providers.

Finally, implementing exceptional resources requires the acquisition of equipment, accounts and licences not usually available in the organisation before the incident.

Mobilising resources at the start of remediation is essential in order to cope with the scale and complexity of the tasks. Remediation funding sets boundaries and must be determined as early as possible at strategic level.

b - IT hardware requirements during remediation

Restoring backup data, creating new secure services, or simply rotating them around, requires equipment.

If the organisation does not have sufficient stock of servers and storage resources, a few approaches are possible:

→ **Reusing pre-existing equipment through fast turn-around** cuts back equipment cost and delivery times. Nevertheless, this solution causes loss of information and evidence, or possibly even business data. In the case of advanced attacks, the risk of persistence in firmware makes reusing potentially compromised equipment in the trusted core risky.

→ **Acquiring new equipment through purchase, rental or loan** makes it possible to absorb peak needs during remediation. Costs can be spread out over time by redistributing equipment after remediation. This strategy can be very effective, but it requires a significant budget and strong ties with suppliers. Deliveries must be made within very short deadlines which is not always possible.

→ **Fully outsourcing some functions to external service providers** is also possible. Fully or partially switching the IS to the cloud is often considered during remediation. But this solution is usually a major restructuring for the organization and should be considered with care[1]. However, the pressure of the situation leaves little room for analyzing this change in policy in terms of risks and costs. If this change is being considered, its long-term impacts must therefore be analyzed.

Generally, a mix of several of these options is the solution retained, often moving up the timeline of any overhaul projects already being discussed.

[1] While migrating to cloud services can be fast, backtracking is rarely simple or quick.

c - Identification of requirements

The increased activity during a major incident requires mobilizing resources from outside the organization. Even when benefiting from a temporary influx of assistance, internal teams will be kept extremely busy by remediation operations.

The consequences of this temporary mobilization must also be taken into account: compensation of overtime, cancelling leave and bolstering hosting capabilities (offices, computer connections, electrical outlets, washrooms, food).

Managing the incident or crisis requires anticipating these needs and the associated expenses as accurately as possible.

A key role in managing remediation therefore lies in identifying the resources needed at each stage and procuring these resources. Unfortunately, ensuring the availability of human or technical resources on very short notice is often a problem. Remediation managers may need to switch between alternative plans to meet their objectives based on this availability.

d - Scheduling resources over time

From the start of a remediation operation, it is necessary to consider the long term. Even when this duration is taken into account, in practice it is almost always underestimated.

Considering the long term means putting in place the long term management of the human resources called upon, but also taking its duration into account in the budget allocated to external providers, even if this means limiting the initial scale.

Many remediation operations tend to end at an arbitrary point after exhausting the entire allocated budget, without having expelled the attacker.

Table 5.5 – Time scales for remediation steps

	PREPARATION	EXECUTION
CONTAINMENT	Hours	Days to weeks
EVICTION	Days to weeks	Hours to days
ERADICTION	Weeks	Weeks to months
RETURN TO NORMAL	Months to a year	Months to a year

e - Mobilizing external support

Removing an intruder from an information system is a different business from outsourcing data management in normal times. Remediation operations require calling on a diverse panel of post-incident reconstruction specialists, specific technology experts and generalists to carry out the numerous technical actions planned.

In addition to these participants[2], several entities may assist the organization in preparing for remediation. Some may directly assist in the process, but most will instead direct the organization towards service providers capable of assisting.

Among them:

- Sectorial, territorial, national or private CERTs[3] can provide direct assistance or indicate competent service providers.
- Supervisory authorities in many sectors increasingly have the capability to monitor IT security incidents and can refer organizations to appropriate service providers.
- Insurers, in addition to their role of providing financial coverage, often keep lists of service providers, sometimes even negotiating terms with them prior to any crisis.
- In business groups, it is not uncommon to have the required skills within the group.

[2] Regarding service providers, See Part III – Service providers in remediation.

[3] Computer Emergency Response Team

- In French administration, FSSI[4] can also direct them to the departments able to assist in handling the incident.

6 CONSIDERING YOUR OPPONENT

An IT security incident is different from an ordinary production incident. This event involves the actions of an active and hostile attacker. Regardless of the reason for the intrusion, the attacker has reasons to oppose remediation.

Remediation actions must take into account their presence and ensure that intrusion cannot occur again.

In particular, this implies:

- blocking the attack paths used by the attacker;
- eradicating any access that the attacker may have retained on the information system;
- ensuring the integrity of new or reinstalled systems when they are acquired, configured and implemented;
- protecting exchanges between remediation participants from the actions of the attacker.

Depending on the attacker's targets, practices and technical means, the attacker may disappear from the information system as soon as the incident is detected, or on the contrary, remain there, actively adapting to the actions of the defenders. Throughout the remediation process, it is necessary to bear in mind that any action visible to the attacker potentially conveys implicit information that may trigger a reaction or adaptation.

a - The need to understand the attack for proper remediation

Following discovery of the intrusion, an investigation must be carried out into the attacker's actions. The results of these analyses will shape the remediation's management.

[4] *Fonctionnaires de Sécurité des Systèmes d'Information*, officers in charge of information security for a whole ministry in French administration.

The investigation can spread over several weeks, but from the very first days it can provide a number of crucial elements: accounts used by the attacker, vulnerabilities exploited, tools deployed. Deploying or strengthening security supervision means provides a clue to the hostile actions under way.

If the attacker is still active on the information system, it is often interesting to observe their actions, as long as the risk of aggravation can be controlled, in order to understand their objectives and means.

As the investigation progresses, the findings may lead to changing the operational objectives or reassessing their priority.

With the advancement of the remediation project, knowledge of the attack is less and less obtained from the investigation, and increasingly from the information system supervision controls. At the end of remediation, only the supervision controls remain.

KEY POINTS FOR THE REMEDIATION

For the remediation team, the main technical questions to ask the investigation team are as follows:

→ Question N°1 **What means did the attacker use to communicate during the attack?**

Most attacks are not carried out by autonomous code[1].

If the attacker remotely controls the attack, he uses some means of communication and often a complex infrastructure. The identification of command and control protocols and servers used by the attacker will enable the defenders to block the communication channels and monitor any attempts to return.

This knowledge makes it possible to harden these channels against the attacker, and to deploy appropriate supervision.

[1] Most autonomous malware will also report to their control using communications that are detectable.

Knowledge of the attacker's communications makes it possible to monitor their activity before eradication and to detect means of persistence that may have been missed.

When active communication channels are identified, the choice to leave them in place should be considered. Blocking known channels informs the attacker that they have been detected. This action may push them to use means that have not yet been detected by the defender. This may result in the defender going blind on the activities of the attacker.

Examples:

- IP addresses and server host names[2]
- domain names;
- specific protocols;
- protocol patterns[3].

→ Question N°2 What means did the attacker use to move around the information system?

An attacker's initial point of entry rarely provides direct access to their target with the privileges he needs.

To access the resources of interest, the attacker must move around the information system. This is commonly called lateral movement. The attacker will also look for ways to acquire the access rights necessary to attain their goals. These movements and this escalation of privileges are carried out by exploiting vulnerabilities or misconfigurations.

Identifying the means used by the adversary enable the defenders to neutralize those that are fully illegitimate and to secure those that are legitimate(by supervision, or by improved access control). Detecting vulnerability exploitation allows to define the priorities for patches deployment. This information enables security monitoring to detect where a returning attacker is going in the information system.

Examples:

- RDP or SSH connections;

[2] The common term for those being *Command and Control servers*, or C2.

[3] For example HTTP headers characteristic of tools of the attackers.

- remote execution by PSExec or WMI;
- exploiting application or system vulnerabilities;
- using remote administration tools deployed in the pool of computers;
- using legitimate accounts.

→ Question N°3 What means of persistence have been identified?

In most cases, the attacker seeks to maintain his access to the compromised information system. If the intruder's objective is espionage, persistence allows them to return later to obtain more data. However, if their purpose is criminal obstruction or sabotage, the attacker will often try to stay in order to observe how the incident response unfolds. There have been cases where attackers hampered remediation operation, or re-encrypted information system that had just already been encrypted by ransomware.

To retain access, the attackers modify the security configurations, or deploy more or less stealthy tools allowing them to regain their foothold after eviction.

Persistences must be systematically looked for and neutralized during the eradication phase. Knowing about them enables the security supervision to detect the attacker's attempts to return.

Examples:

- spoofing[4] existing accounts, created or modified by the attacker;
- software implants;
- re-configuring filtering equipment;
- cloud access;
- remote access services[5].

[4] Attacker can be seen performing account impersonation, creating or modifying accounts access rights on Single Sign On or locally on systems. These has been observed on servers, workstations, as well as on infrastructure equipment such as VPN, firewall, hypervisors, wireless relay.

[5] VPNs and bastion hosts are natural entry points, but services like ConnectWise Control, TeamViewer or LogMeIn often used for support services shall not be neglected

LIMITATIONS OF THE FORENSIC INVESTIGATION

The investigation into the incident has its own objectives. Its steps are independent of remediation. It is important to ensure that these two activities are properly synchronized: it is not recommended to block remediation pending information that is may not be very useful, nor to rush it before having acquired sufficient information.

The investigation should pay special attention to some trends, described below, that are not useful for remediation.

→ Obsessing over the initial entry point

In many cases, the initial entry point can be quickly identified: a workstation compromised by a malicious attachment, or a VPN access whose password was available on the Internet.

However, sometime the point of entry might not be so clear, especially when the intrusion is old. With some attackers, it is not uncommon to discover that there was an initial campaign that gave the attacker multiple points of entry.

It is therefore not recommended to focus all the remediation means on identifying the point of entry.

In most cases, it is possible to reduce the window of opportunity that the attacker can use, but not completely close it: the business lines need to exchange documents with the outside world, passwords are reused and there will always be at least one exposed vulnerable service in a sufficiently large perimeter.

It is therefore necessary to consider probable that there will always be at least one compromised device in the IS.

A more effective strategy is to:

- remediate identified vulnerabilities;
- reinstall compromised equipment;
- disable compromised accounts;
- define a procedure for the reintegration of equipment of unknown compromise status (update, integration into supervision) into the information system.

Limiting the possibilities of lateral movement or escalation of privileges are often the most effective security controls, and should be the focus of the most efforts.

→ Over-focusing on the incident attribution[6]

It is often possible to identify the ***modus operandi*** of the attacker, at least in part, through the investigation. By contrast, identifying the perpetrators of the attack is complex and should be reserved for the competent authorities. Many attackers use a very broad technical palette.

In practice, this information is rarely very useful in the context of remediation and is often given a disproportionate amount of attention relative to its practicality.

A remediation project should not wait for a possible attribution to choose how to define and implement its objectives.

→ Focusing on known attack vectors

When the investigation determines the steps of the attack, it is tempting to focus on the points exploited by the attacker. This information is often used to concentrate security controls based on what has been observed.

Knowledge of the attack does helps to eradicate the attacker's access and to detect any attempts to return.

However, the search is unfortunately never comprehensive. It is therefore necessary to avoid a false sense of security about the attacker's eviction. Careful attention must be paid to any abnormal activities that may indicate a forgotten blind spot.

To avoid falling into this trap, it is often useful to complete the study of the attack by looking for other vulnerabilities in the information system, to discover as many remaining flaws as possible and correct them.

[6] Identification of the attacker operating procedures through technical elements.

b - Sources of external knowledge

Knowing the means used by the attacker is important when choosing containment actions, but also vital to eradicating their access to the information system.

The results of the investigation often make it possible to use external information as a pivot to expand the search.

For example: the attacker's modus operandi consists in stealing data from file servers, creating RAR archives from the stolen data, and exfiltrating them via a public web server. An open source search indicates that these activities are often associated with the deployment of a particular type of remote control tool that remediation teams will be able to look for during eradication.

This type of information can be found in the publications of security solution vendors, CERTs and IT security authorities. This information may also be provided by threat intelligence services[7].

In the heat of a crisis, it is possible to forget to these mind-broadening sources of information, which are nevertheless important.

c - Selecting security and supervision controls

The investigation delivers information on the activities of the attacker, but also point the weaknesses of the information system. This information makes it possible to re-assess the system's security and adjust the security controls to be deployed.

The attacker's past actions do not determine those they will undertake in the future. Defender must therefore not restrict their action to preventing what has previously happened.

Murky areas in which the attacker initially escaped detection must be covered.

[7] These services are usually commercialized under the label of *Cyber Threat Intelligence* or CTI.

It is important to prevent and detect:

- local or global privilege escalations;
- explorations and lateral movement;
- their persistence and communication.

These controls are generally put in place during the incident to support remediation actions. It is recommended to consider their sustainability when they are deployed. In particular, it is important to adapt the controls appropriately to the level of team mobilization. The highest level of engagement usually cannot be sustained after the incident.

d - Operational security in remediation

Operational security refers to the protection of defensive actions against the attacker. These protective controls should be applied to all teams operating as part of incident response: strategic management, investigation and remediation. Remediation is not an ordinary integration project. This section provides a recap of the security controls that need to be considered. Operations carried out in the presence of an intelligent and hostile attacker, who observes and reacts, require special precautions. Most non-specialist participants are unfamiliar with this.

BACKGROUND

Many attackers do not leave the compromised IS once their goals have been reached or even once they have been detected. In particular, they often monitor incident response and remediation actions in order to counter them. For that purpose, they monitor the defenders' communications, retrieve the documents generated by the teams working on the incident, and try to collect the new passwords as they are changed.

Remediation teams cannot rely on infrastructure that has been compromised to work securely. Such a situation requires setting up specific resources until confidence has been restored in the information system.

Furthermore, the IT incident may be the direct cause of a degradation in working resources. Thus, a ransomware attack usually renders the messaging, file-sharing and often even the intranet unavailable, or usable only in degraded mode.

In those circumstances, improvised means are generally set up: temporary workstations, disk bays, cloud infrastructure. These systems will host sensitive information. However, these means are often deprived of adequate security controls and thus highly exposed to the risk of a breach.

Perfect security in remediation is impossible to achieve and maintain over time at an acceptable cost. The protective controls of the remediation project must be chosen while remaining aware of compromise, accepting some risks, but avoiding paralysis due to excessive caution.

COMMUNICATIONS WITHIN THE REMEDIATION TEAM

Knowing the actions taken against the attackers is the attackers' priority. Their access rights are often extensive when a breach is discovered. It is therefore not uncommon to find that the email accounts of administrators, CISOs, internal IT services or incident response teams are spied upon. Sometimes attackers are able to follow on-line crisis meetings[8].

Intruders also try to retrieve documents relating to the defense of the information system: action plans, new configurations, lists of markers. They also try to spy on internal discussion forums and Wikis. In some cases, attackers used mobile data management (MDM) tools to track response activities on the phones of the organization.

In the case of advanced attacks, the use of intelligence techniques may include broader counter-surveillance: for example, monitoring whether a specific malware has been submitted to a service such as VirusTotal, listening to the communications of the organization with incident response specialists or law enforcement agencies.

It is therefore imperative to keep the remediation work completely dissociated from the compromised system. This includes using storage and communication means separate from the compromised system[9]. The workstations used by the defenders must also be protected. Ideally, new or reinstalled workstations not linked to the information system should be used. If this is not possible, special protection must be set up: specific EDR, configuration hardening, communications restriction.

[8] In the past multiple ransomware groups have published screenshots of Teams and Slack discussions inside incident response teams.

[9] It is important to consider access transitivity. Notably, relying on a cloud service connected to the compromised Active Directory is unsafe.

Data exchanged outside protected stations must be encrypted in transit and preferably also in storage, to avoid interception.

In most organizations, telephony has now migrated to IP. Thus voice-over-IP infrastructure is also a computer system commonly targeted by attackers. It will generally be necessary to prioritize exchanges over cellular telephony, or via applications using end-to-end encryption for voice communications, preferably certified by ANSSI[10].

If cloud applications and services are used for remediation, multi-factor authentication must be used.

A balance must be struck between reasonable operational security controls and the ability to work. This adaptation always results from a compromise between practicality and security. Nevertheless, these compromises must be made consciously and with guidance. In addition, they may require to implement compensatory controls.

COMMUNICATIONS WITH THE REST OF THE ORGANIZATION

Remediation necessarily affects the rest of the organization. It is therefore necessary to communicate about it. Saying nothing always generates detrimental anxiety. However, it should be remembered that any internal communication is potentialy read by the attacker, and often communicated externally[11].

It is generally prudent to avoid including details too specific about ongoing actions, at least before their completion, in internal communications. The balance between providing information and preserving trust is difficult to achieve. These decisions must be coordinated at the highest level.

COORDINATING WITH THOSE OUTSIDE THE ORGANIZATION

Often, while the incident is being handled, exchanges with the outside world are affected: link disconnection, closure of remote access,

[10] The list can be found on ANSSI site: `https://cyber.gouv.fr/trouver-un-produitservice-de-securite-evalue`

[11] For more details, please refer to ANSSI guide "Anticiper et gérer sa communication de crise cyber"

activation of security options. The partners of the organization will inevitably discover these changes. Moreover, these contacts may be secondary targets or entry points for the attacker.

Communications with partners must therefore take into account the fact that the attacker has a view of the usual means of communication. Generally speaking, this means setting up temporary dedicated means of communication, with informed partners for the duration of the incident.

Exchanges with service providers or with external entities involved in the remediation must be protected to the same degree as internal exchanges within the remediation team. A dedicated information system, encryption solutions and the use of multi-factor authentication are strongly recommended. Particular attention should be paid to the enrollment of participants in the remediation systems. In the absence of sufficient precautions, attackers may recover credentials and log on in place of the legitimate user.

In an advanced attack, even when communications are encrypted, knowledge of the recipients of the exchanges can be sensitive. For example, if a CISO suddenly starts exchanging emails with addresses from an incident response services provider, or calls a phone number associated with ANSSI, this probably indicates that an incident management is in progress.

DECOMMISSIONING EXCEPTIONAL RESOURCES

When dealing with the incident, a lot of sensitive information is exchanged on uncommon systems. Exceptional access is also provided.

It is necessary to make sure that these elements do not create a risk of information leak or uncontrolled access once the remediation is over. In particular, it is necessary to ensure that all data outside a secure information system (e.g., on a cloud workspace instance) is properly destroyed, and access removed from workstations that were kept out of the information system.

If workstations dedicated to remediation have been used, the most prudent thing is to wipe and then reinstall them. This is facilitated by using disk encryption during the incident. Similarly, portable media must be decommissioned, including USB flash drives and disks that may contain sensitive data.

To be able to carry out this task, a log of all these items must be kept during the remediation.

PART III

SERVICE PROVIDERS

A remediation project following a major IT security breach requires significant mobilisation on the part of the technical teams and the use of various types of expertise. Few organisations have sufficient staff and the diversity of skills required to cover these needs. Most remediation services therefore include a significant proportion of subcontracting.

1 FORMULATING THE NEEDS

Requirements must be specified as precisely as possible.

Unfortunately, terms refering to remediation matters can be interpreted very differently. Do not hesitate to draw up an explicit list of the actions expected of the service provider.

In particular, a clear distinction needs to be made between remediation and non-remediation services provided during response to an incident.

→ Remediation services

- Remediation management services, which assist the organisation's senior management in taking back control of its information system.
- Expert technical services for remediation, which can range from cleaning and remediation of an Active Directory to network reorganisation or recovery of damaged data. These interventions are carried out by experts familiar with how to work on a compromised information system.
- Hardware, software and application administration services are often necessary for restoration, reinstallation or reconfiguration of information system components, or even to run centrally planned eradication tasks. However, these operations are not carried out by people specialising in working on compromised systems. They must receive support to limit the risk of bad practices.

→ Other incident response activities

- Digital investigation services, which aim to trace the attacker, establish how they entered the information system and how they moved within it, as well as identify the accesses still present.

- Crisis management services that assist the organisation's senior management in handling the incident, in particular in coordinating actions, managing impacts and communication.

2 SELECTING SERVICE PROVIDERS

Ideally, relationships with service providers required to intervene in an emergency are contracted as part of the preparation for IT security incidents.

If there is no pre-existing contractual framework for the incident, it is preferable to rely on already established relationships, via insurers or industry specific organisations.

ANSSI issues the Security Visa[1] to a number of service providers. Among them are Digital Forensic and Incident Response providers or ***Prestataires de Reponse aux Incidents de Sécurité*** (PRIS) in French[2]. It is therefore possible to seek assistance from trusted service providers whose level of competence has been verified. Nevertheless, it is important to note that this PRIS qualification does not currently include management and implementation of remediation services, nor is there yet a qualification scheme encompassing all types of remediation services.

This guide can thus serve as a basis for formulating the requirements of the beneficiaries and for identifying the services to be provided.

When selecting service providers, it is important to identify the service milestones that will be used to monitor their progress. These milestones should be determined as soon as the contract is signed.

3 STEERING THE SERVICE

A specificity of services in the context of a remediation is that they are provided in quick succession.

[1] Security visa on the ANSSI website: https://cyber.gouv.fr/les-visas-de-securite

[2] The list of PRIS is available on the ANSSI website: https://cyber.gouv.fr/prestataires-de-reponse-aux-incidents-de-securite-pris

Indeed, several contributors with specific and specialised expertise (file restoration, Active Directory configuration, firewall or virtualisation configuration, etc.) work for brief periods only. Their actions must be integrated into longer information system restructuring activities.

In order to limit the loss of information and capacity, particular attention should be paid to:

- interventions that block each other, to be scheduled prudently and leaving a margin for delays;
- the proper collection of deliverables from each contributor and their provision to the other contributors who will need them, whether internal or external;
- the format of the deliverables, which must allow those using them to do so as directly as possible (avoiding data re-entry, or conversions that frequently introduce errors);
- the proper definition of the end-of-intervention conditions and their validation, to avoid receiving partial deliverables or incomplete configurations.

Coordination between contributors is complex and essential. Organising workshops between these participants may be particularly useful to ensure a proper understanding between specialists and continuity between the different stages of remediation. Working with internal IT service members paired up with external providers throughout the remediation process is an effective way of limiting information loss.

Finally, any blocking points likely to be encountered by a contributor should be detected as quickly as possible, in order to avoid freezing the entire remediation process. To achieve this, frequent progress reviews are a good solution.

4 THE END OF THE SERVICE

The service is completed once all the milestones have been reached.

It is important to ensure that all deliverables are recovered, even if they have already been sent to another participant.

In addition, it is often necessary to contact a participant again in order to clarify certain settings. These post-intervention updates must be scheduled upstream, in order to avoid unavailability or unforeseen costs.

PART IV

STANDARD PLANS

This section examines three typical scenarios. Their purpose is to describe how the organisation's decision-making priorities are linked to its operational objectives and the resources to be deployed. These scenarios are templates and should not be carried out as they stand, but rather must be adapted to the organisation who will use them.

While these scenarios could cover a simple remediation project, they are often used as successive phases in more complex remediation plans.

1 "RESTORE MISSION CRITICAL SERVICES AS QUICKLY AS POSSIBLE"

a - Description

This scenario applies in a situation where the disruption of the organisation's activity has a major impact on its survival or on an essential or mission-critical service.

In these circumstances, it may be necessary to carry out a remediation focused on the relevant service(s), before being able to deal with structural problems. This scenario assumes that mission-critical services can be unbundled from the rest of the information system.

The remediation described below outlines the phases necessary to reopen services after a major breach.

b - Strategic objective

Ensure the continuity or restart of a mission-critical service for the organisation within a short period of time.

c - Operational objectives

- Create a restricted trusted foundation for the mission-critical service (network, virtualisation, identification).
- Secure restoration of the mission-critical service (reinstallation or cleaning).

- Remove the attacker’s residual access in the critical services bubble.
- Prepare for securing the mission-critical IS over time.
- Minimally remediate the vulnerabilities exploited by the attacker on the rest of the IS.

d - Progress

A minimum trusted core is restored around which a recovery bubble is built. This trusted core is not necessarily a complete authentication infrastructure, but rather a strictly necessary system, network and identity foundation.

Critical service dependencies are inspected, cleaned and imported into the recovery bubble.

Servers supporting the service can be reinstalled or imported, and cleaned. Although reinstallation offers better guarantees, it is not always possible (lack of the time required to rebuild configurations, or simply unavailability of installation media).

The bubble is placed under tight security supervision and the service is restarted as soon as possible.

For the rest of the information system, outside the bubble, a minimal campaign to eradicate exploited vulnerabilities and backdoors placed by the attacker is carried out after the service restarts.

The risk is accepted, these actions may be part of the continuous improvement of the information system.

Moreover, a strong separation of a mission-critical service from the rest of the organisation is rarely sustainable. Ultimately, this service will have to be reintegrated into the secure information system. The purpose of the scenario is to give defenders the time to deal with this reintegration outside of the emergency.

e - Residual risks

The priority given to the speed at which the service is restored makes it impossible to create or recreate a resilient IS security organisation.

If a project to increase the security maturity of the system in question is not carried out at a later stage, the risk of new significant incidents arising is high. In practice, it has been observed that although the mission-critical activity has been secured, the recurrence of incidents in the rest of the IS has a lasting impact on the organisation. The IS security long-term plan must take into account any actions postponed beyond the emergent situation.

When an in-depth project to tighten security is not carried out after an incident, the ANSSI notes that the cost of recurring incidents affecting businesses can quickly exceed that of a more comprehensive remediation.

2 "TAKE BACK CONTROL OF THE IS"

a - Description

In this scenario, the organisation aims to recreate an information system in a state close to its initial state, without aiming for profound transformations.

The objectives of this scenario aim to strengthen the existing system while minimising the changes.

b - Strategic objectives

- Within a reasonable time, return the business to a nominal operation and production activity.
- Take back control of the information system.

c - Operational objectives

- Create a hardened trusted core that can be controlled over time.
- Restore the previous IS security level outside the trusted core.
- Remediate the specific vulnerabilities exploited by the attacker outside the trusted core.
- Eliminate the attacker's accesses throughout the information system.

d - Progress

A trusted core is rebuilt containing a complete and secure management infrastructure. The architecture of this bubble is completely rebuilt to the state of the art.

Strong security supervision is put in place on the trusted core before it is put into service, and maintained long term.

A campaign to remediate identified vulnerabilities and eradicate the attacker's backdoors is run on servers and terminals. No change to architecture or management processes is made outside the trusted core.

Strong but temporary security supervision is put in place outside the trusted core to ensure the eradication is effective. This level of supervision outside the trusted core is gradually reduced to a lower state that is sustainable in the long term.

e - Residual risks

In this scenario, priority is given to the speed to exit the crisis and return to normal operation. As a result, in-depth security work cannot be carried out outside the trusted core and the risks of future compromise and escalation of privileges remain high.

3 "SEIZE THE OPPORTUNITY TO PAVE THE WAY FOR ENDURING IS CONTROL"

a - Description

In this scenario, the incident is used as the starting point for restructuring the information system security.

The strategic objectives aim to reduce enduringly the risk of major IT security disruptions, at the cost of a longer recovery time and a higher initial investment.

The operational objectives are actions that can be sustained in the long run and integrated security.

b - Strategic objectives

- Return the business to a nominal operation and production activity.
- Implement sustainable protection to avoid repeating a comparable situation.

c - Operational objectives

- Create a hardened trusted core that can be controlled over time.
- Create a controlled and sustainable level of security for server and application administration practices.
- Remediate the vulnerabilities exploited by the attacker on the rest of the IS.
- Implement a sustainable detection/response/correction capacity over the entire IS.
- Eliminate the attacker's accesses throughout the information system.

d - Progress

A trusted core is rebuilt, containing a very comprehensive service foundation. For this purpose, the architecture of the trusted core is completely rebuilt. Strong security supervision is put in place on the trusted core before restarting it, and is maintained in the long term.

The architecture of services outside the trusted core is broken down into sectors to be processed successively. By default, all sectors are considered compromised.

Each sector is reviewed in turn:

- identified vulnerabilities are corrected;
- the attacker's backdoors are removed;
- its architecture and management organisation are reviewed and modified if necessary;
- its security supervision is integrated with that of the trusted core.

The remediated sectors constitute the healthy IS, with the aim of eventually including the entire IS. Areas not yet addressed are considered compromised and the focus of tight isolation and security supervision controls.

A campaign to remediate identified vulnerabilities and eradicate backdoors is run on terminal workstations. They receive a lower degree of security supervision than servers and the trusted core.

e - Residual risks

No modern information system can provide strong protection for all segments of the information system. In particular, among terminals, it is accepted that some remain compromised. Efforts are focused on limiting escalations and impacts so that low severity incidents do not escalate.

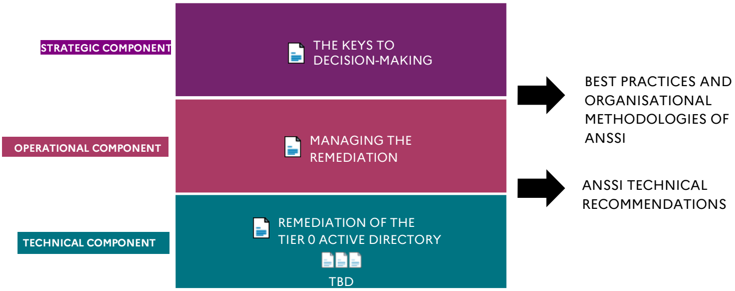
Building the trusted core ensures that, even in the event of a severe incident, it is possible to regain control of the information system without large-scale operations.

PART IV

APPENDICES

A STRUCTURE OF THE CORPUS OF DOCUMENTS

This corpus is divided into three documents, each of them detailing a different component of the remediation: the strategic component, the operational component and the technical component.


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

B GLOSSARY

CONTAINMENT

Containment refers to all the actions taken at the start of an IT security incident designed to contain its extent. Most containment actions disrupt the information system's usual operation, or consume resources abnormally. As such they are generally not sustained for prolonged periods. The implementation of the remediation plan must make it possible to lift containment measures in order to reach a sustainable balance.

CRISIS MANAGEMENT

Crisis management[1] is a management process that identifies potential impacts that jeopardise an organisation and provides a framework for enhancing resilience, with the capacity for effective response preserving the interests of the organisation's key stakeholders, reputation, brand and value-creating activities, and effectively restores operational capabilities.

CYBER CRISIS

A "cyber" crisis is defined by the immediate and major destabilisation of the day-to-day or future operation of an organisation (lost contracts, halted activities, inability to deliver services, heavy financial losses, major loss of integrity, etc.) due to one or more malicious actions on its digital services and tools (cyber attacks such as the use of ransomware, denial of service, etc.). Such events therefore have a considerable impact, which cannot be dealt with through usual processes and within the framework of the normal operation of the organisation.

Accidental events, in other words those which are not the result of malicious activity on the IS, and malicious actions not resulting in immediate and major interruption to the organisation's essential services, are therefore excluded from the scope of the definition.

ERADICATION

Eradication refers to both the search for and neutralisation of the attacker's residual or potential hold on the information system around the trusted core and is accompanied by controls to prevent them from returning.

Eradication on a large system can be a massive amount of work. For this reason, eradication operations are often phased by department, business units or sectors of the information system.

[1] As defined in the requirements for ANSSI certified cyber-consulting professionnals: "Prestataires d'Accompagnement et de Conseil en Sécurité des systèmes d'information" (PACS) certification scheme `https://cyber.gouv.fr/sites/default/files/document/PACS_referentiel-exigences_v1.0.pdf`

EVICTION

Regaining control of an information system requires creating or recreating a trusted core. This sub-system, kept out of the attacker's reach using strong controls, is the foundation for recovery actions. From this trusted core, defenders will be able to work on the rest of the information system beyond the attacker's reach.

Eviction therefore consists in recreating a trusted core based on data from the system that has been compromised. In some cases, eviction is recreation without reusing old elements of the information system. In most cases, eviction is more a combination of filtering and cleaning the data from the compromised system before using it on reinstalled systems.

INVESTIGATION

Investigation[2] is the process aimed at collecting and analysing any technical, functional or organisational element of the information system used to qualify a suspicious situation as a security incident, and to understand the modus operandi and the extent of a security incident on an information system.

MAJOR SECURITY BREACH

A major cyber security incident is a sequence of technical events that are severely impacting, or risk severely impacting, one or more business lines identified as essential to the organisation's activity.

It is a cyber attack's impact that determines its severity, not its nature. The impact must always be considered with regard to the business lines supported by the information system. The major incident is characterised by the potential to degenerate into a crisis if not properly circumscribed and handled.

[2] As defined in the requirements for ANSSI certified incident response professionals: "Prestataires de Réponse aux Incidents de Sécurité" (PRIS), https://cyber.gouv.fr/sites/default/files/2022-10/pris_referentiel_v2.0%5B1%5D.pdf

MANAGEMENT LEVELS FOR A MAJOR IT SECURITY INCIDENT

A security incident and its management can be considered from three distinct levels:

- The **decision-making level** is responsible for taking account of the incident and its impacts on activities in the organisation's management. At this level, the senior executives shall determine the main orientations for crisis management and exit conditions, according to the priorities of the organisation and its stakeholders.
- The **operational level** is handled by the managers in charge of the information system and its security. Decisions at this level are generally made by technical managers, information system directors and information system security managers. During an incident, it is at this level that decisions are made on how to implement as broad technical actions the guidelines approved at decision-making level.
- The **technical level** is the level at which precise technical actions are organised, implemented and applied.

OPERATIONAL REMEDIATION GOALS

An operational remediation objective is a measurable state of security level or functional level of the information system. These objectives are the technical implementation of the strategic remediation objectives. These objectives are detailed in the remediation plan as concrete actions.

RECONSTRUCTION

Reconstruction is a support activity for remediation, designed to provide it with the IT resources necessary to restore the information system to operational and secure conditions.

At the same time as remediation, reconstruction can help to maintain the organisation's mission-critical activities.

At the end of the "emergency situation", reconstruction will continue to gradually restore the information system to normal operation and improve its security.

REMEDIATION

Remediation is defined as the project to regain control of a compromised information system and restore a sufficient operating state. It consists in a sequence of actions leading from an existing impaired state to a desired state. In the context of an IT security incident, this work begins as soon as the adverse action is being contained, and can extend over several months.

When crisis management is put in place, it often ends in the early stages of remediation.

Remediation only ends when the functional and security levels of the information system meet the strategic objectives. The end of remediation also signals the return to the continuous security improvement cycle.

REMEDIATION PLAN

The remediation plan is the list of actions to be taken to bring the information system into compliance with the operational remediation objectives.

This plan can be broken down into sub-projects by operational remediation objective.

STRATEGIC REMEDIATION GOALS

The strategic goals define the situation to be obtained at each key stage of remediation. These are choices made by senior management in the light of business priorities.

They are formulated in non-technical terms and must be prioritised and associated with specific deadlines.

The organisation's senior management determines and prioritises strategic remediation objectives.

TIME OF IT OVERLOAD

The term "Time of IT overload" is used in this document to refer to the period between detection of a major incident and lifting of exceptional (or crisis) management controls.

During this time, normal IT activities are de-prioritized, or suspended to concentrate on incident and post-incident work.

"Time of IT overload" is the opposite of "normal situation", during which the organisation's management processes are not mobilised to deal specifically with the incident.

In most cases, remediation begins in the emergent situation but ends during a normal situation.

TRUSTED CORE

The trusted core is the part of an information system underpinning the security of the entire information system. In most information systems, the trusted core includes: identity management, administration, security supervision components, and hypervisors.

Compromising a component of the trusted core would lead to compromising the entire information system.

Secure architectures aim to minimise the size and complexity of the trusted core, in order to keep its security as simple as possible. This minimalistic nature of the trusted core is particularly important in an incident where any part of the information system may have been compromised.

Although the trusted core of most office systems is frequently centred around the Active Directory, this is not the only possible case.

REMEDIATION COLLECTION

Remediation is defined as the project to regain control of a compromised information system and restore a sufficient operating state. Its operational component is vital to its success : structuring, implementing, handling the logictics or even phasing out of the remediation are key steps that must be well handled. An incident can become an opportunity of significant improvement if properly managed.

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 operational component will provide some assistance to design and implement a remediation project, as well as advices for each step of the remediation and classic scenarios.

Version 1.0 – December 2023
Registered: December 2023
Paper ISBN: 978-2-11-167191-1
Digital ISBN: 978-2-11-167190-4

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