RÉPUBLIQUE
FRANÇAISE

Liberté
Égalité
Fraternité

Post-Incident Remediation at ANSSI

A Full Scale Effort

Christophe Renard

ANSSI

January 15, 2025

Who am I?

ANSSI/CERT-FR

French national cyber-authority
Operations Directorate of ANSSI is also CERT-FR

Christophe Renard
Heading a team dedicated to post-incident remediation
Unrepentant ex-(sysadmin—integrator—developer).
`mailto:christophe.renard@ssi.gouv.fr`

CERT-FR

`https://cyber.gouv.fr`
`https://cert.ssi.gouv.fr`

Outline

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

1. Prelude

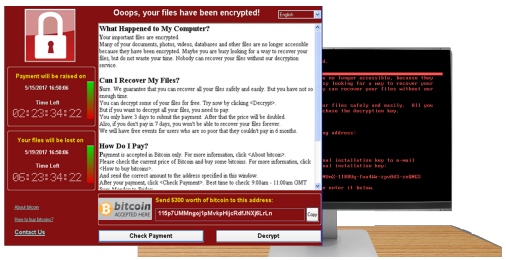
Why this talk?

We have things to share.

- We think there is a need of attention around post-incident recovery.
- We propose a new framework around “Remediation”.
- We designed, experimented with it.
- And now we want to share that work with you.
- And we expect to start a conversation.

An historical perspective 1/2

Evolution



- CERTA goes back to 1999
  - recovery → reinstall
- ANSSI was created in 2009
  - Espionnage
    - Bercy(2011) and many others. . .
    - Large systems and (very) persistent adversaries
    - **In depth infrastructure cleanup required**
  - Destructive events
    - Worms (Wanacry, NotPetya), or targeted destruction (TV5Monde)
    - **Priority to continuity and service recovery**
  - We considered remediation as
    - Something happening twice or thrice a year
    - **A tailored project for each victim**

A detailed retrospective on CERT-FR operations (in French) can be found here

`https://www.sstic.org/2023/presentation/cloture_2023/`

An historical perspective 2/2

Ransomware

- 2018, we see *Big game hunting* impacting our constituents
  - Hospitals, Municipalities, Infrastructures operators. . .
- Made worse during COVID
  - Extension of our perimeter to smaller health institutions
- CERT-FR activity in 2023
  - 3703 security events, 1112 new incidents, about 15 long term engagements(operations)
- Change of strategy:
  - Many shorter interventions $\rightarrow$ **1**/ rebuild a trusted core, **2**/ restore vital business services, **3**/ move to the next victim.

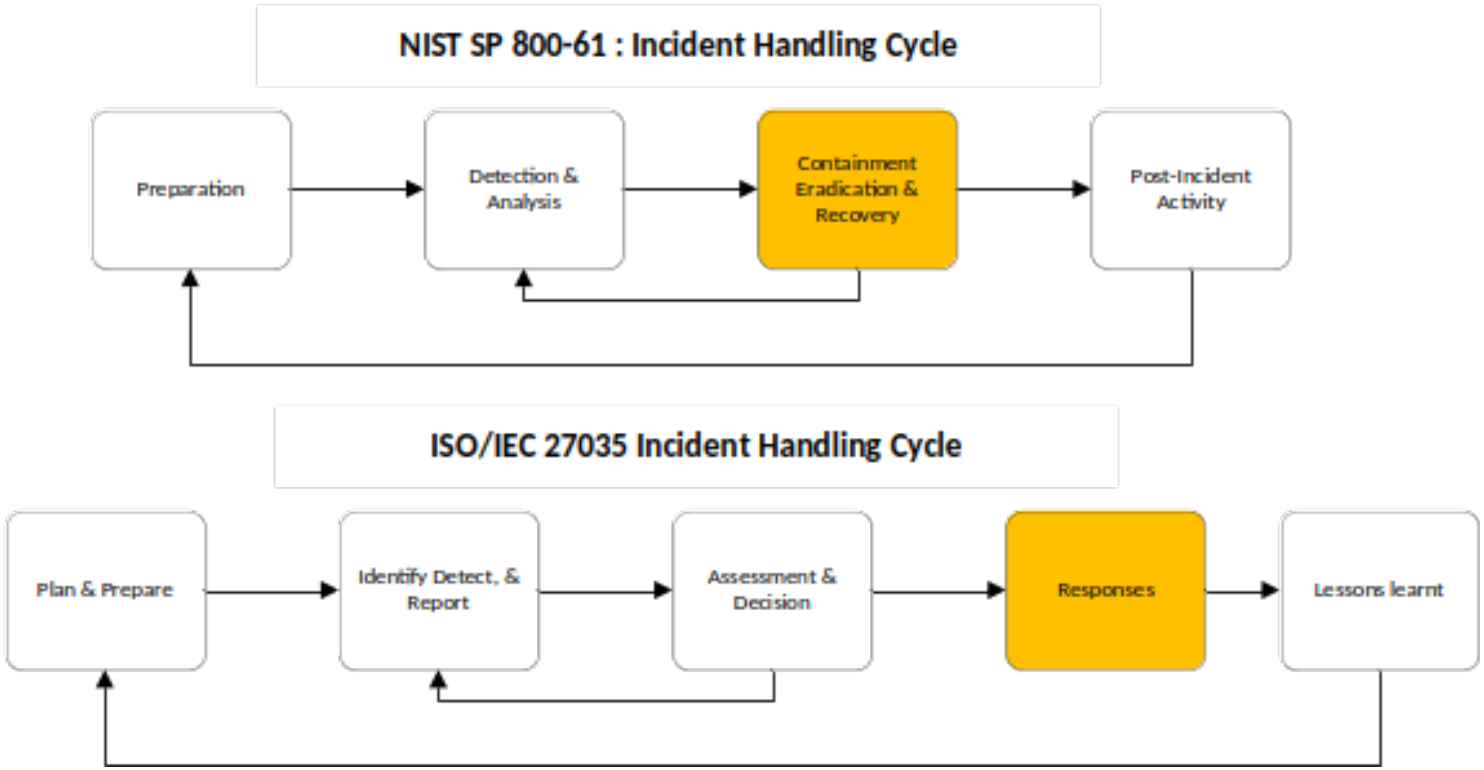
At this point, we realized we needed to take a step back and think about post-incident remediation

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

2. The problem

IR “by the book”

How we are told things should work



Lasting impacts

It is taking too long, costing too much

- We used to think remediation was mostly finished after we left
  - Then we checked
    - Most of the time, normal operations were not to entirely restored after a year (particularly after destructive events)
    - IT had been dedicated to post incident projects for months with huge human impacts
  - We asked around
    - Most of our international partners had similar experiences
    - No one had yet found a lasting solution
- The number of victims also changes the deal
  - There are only so many incident responders

Incident response

Who are you gonna call?

- Crisis management is a mature field
  - Lots of actors to prepare, train, assist
  - Focused on decision and communication
  - Lacking on connection with technical aspects
- Recovery is considered as mostly an IT issue
  - Little connection with business priorities
  - Integrators do not know how to operate with an attacker around
  - Internal IT is not prepared for the scale of the work
  - Means of coordination are gone, compromised or both

- Disaster recovery does not handle “cyber”
  - In many organizations BCR only plan for physical disaster
  - Cyber in continuity is an issue

Incident response

How do we deal with it?

- We have gotten pretty good at investigating. . .
  - Cyber-crime pressure has pushed a rapid ecosystem development
  - Tools, knowledge sharing, number of teams have progressed drastically
  - Detection tools are more common and better known

  But. . .
  - Connections between investigation and recovery are scarce
  - IR engagement are often too short for efficiently recovery
  - Victims do not know what to expect our even ask for

Who is in charge of coordinating the technical response?

3. The plan

Task force and consultation

The need for something practical ASAP

- We built a transversal team in 2019
  - Mixed skills
    - Audit, Incident Response, Industry and certification
  - Mission
    - Make technical remediation operations more efficient, and less reliant on us
    - **FAST !!!!**
- We identified we had to take a step back
  - Technical know how is not sufficient to improve the situation
  - Propose a framework
- Then we realized we did now know enough
  - Writing a "Universal how to remediate method" was beyond our reach
- Instead
  - Define the concepts and vocabulary
  - Support with technical documents
  - Improve $\Rightarrow$ frequent update

A cooperative ecosystem

- Our IR doctrine
  - We always work **with** the victim
    - With its IT
    - With its suppliers
    - With its priorities
    - With its Incident Responders (IR)
  - We do not handle all by ourselves
    - We can be a second level support to the IR
    - We can fully or partially delegate to private sector
    - In most cases we only supervise what is being done
- Consequently
  - Our doctrine has to be adaptable to most context, not only ours
  - We have to create a shared culture
    - Shared vocabulary
    - Shared project milestones
    - Shared actors roles
  - The result is
    - We have to make our content for all remediation actors (IR, IT, business, consultants. . .)
    - We have to actively promote it beyond our usual readers
    - We have to train people to select appropriate services

Doctrinal corpus

We wrote three guides

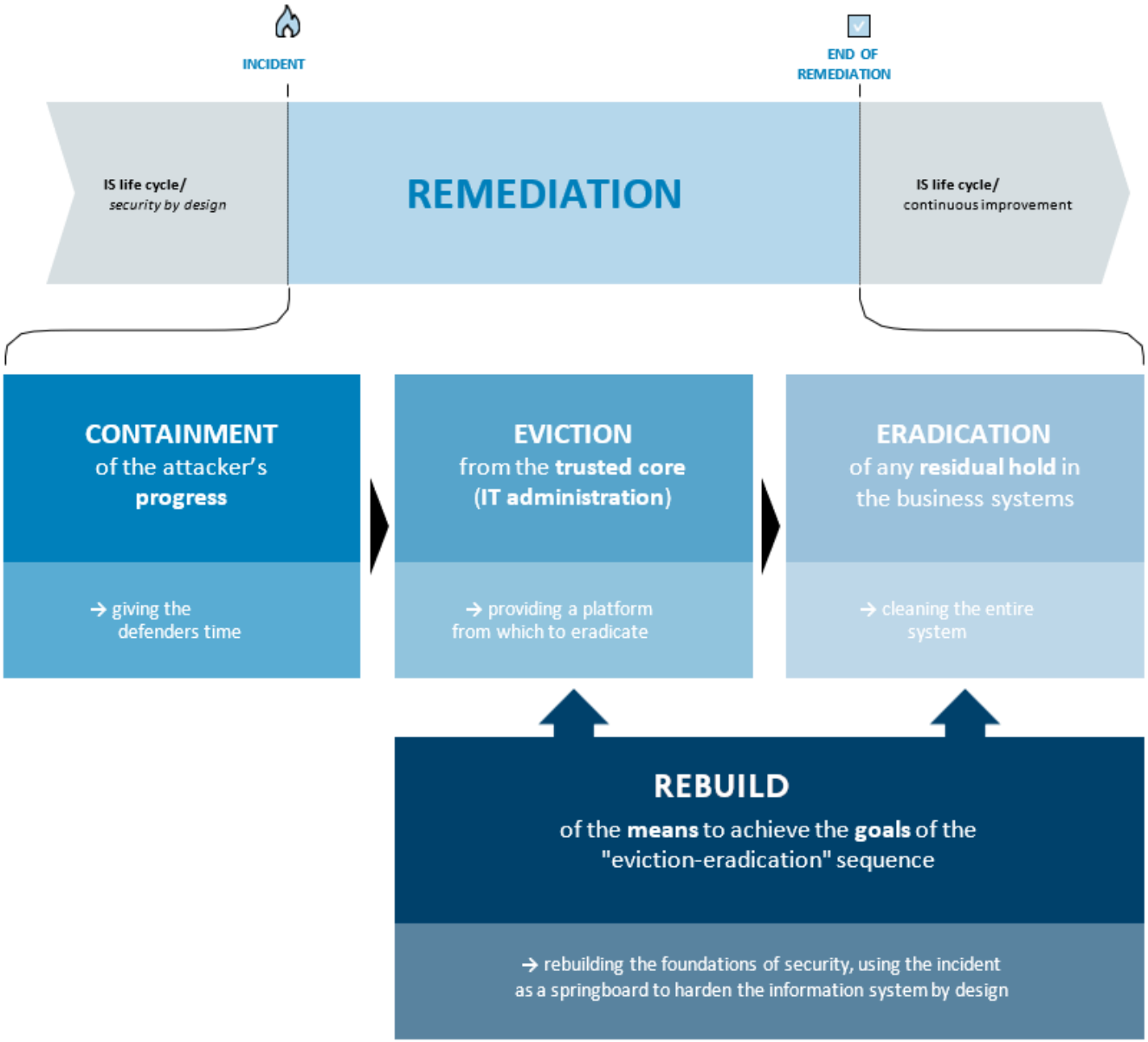
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

4. Our vision

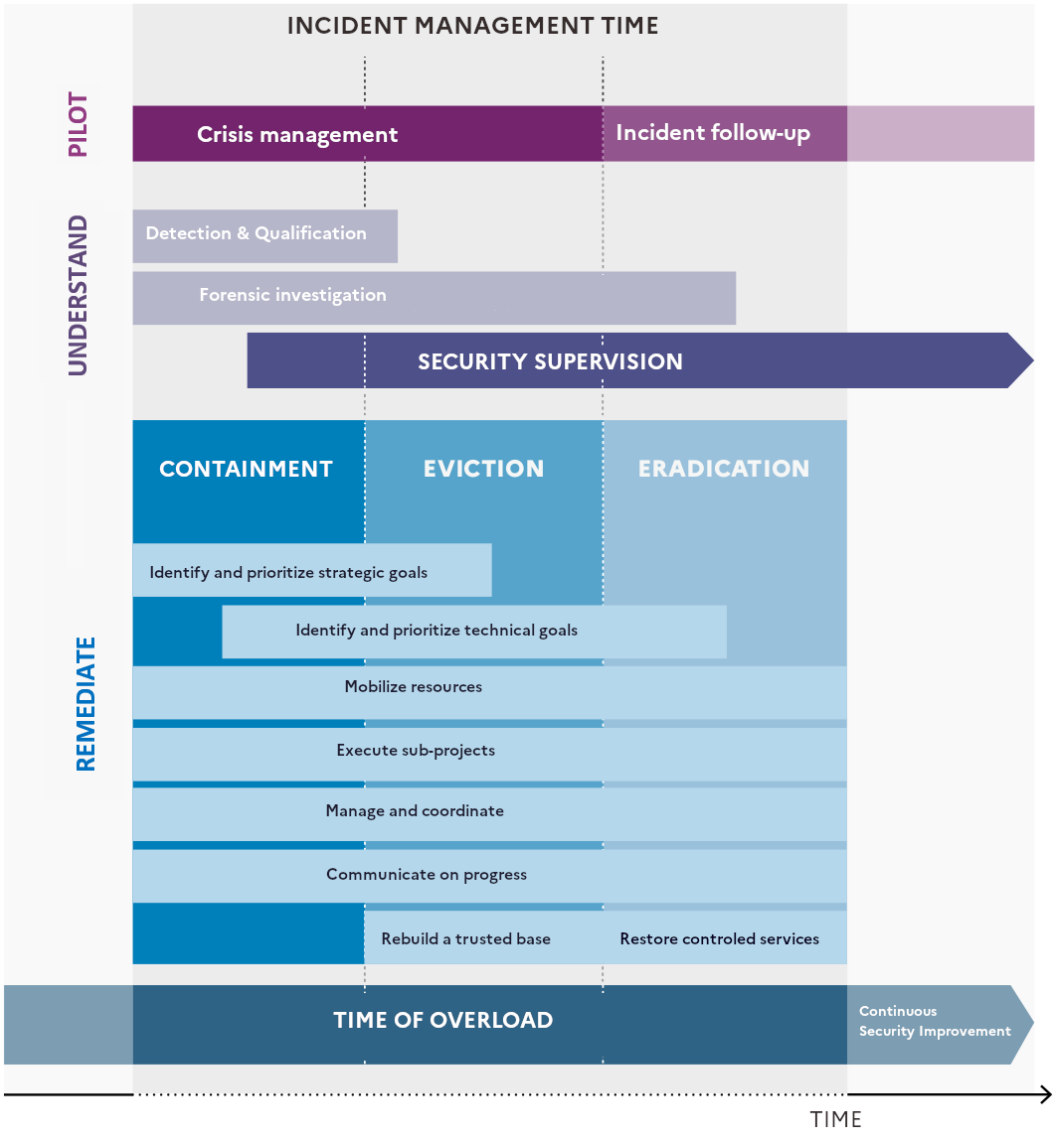
Foundational principles

- **Remediation is a project**
  - Aiming at **regaining control and restoring functions**
  - Executed by IT and its suppliers
  - But ultimately **lead by business needs**
- **Remediation takes place during a specific time**
  - Starting with the incident (during containment)
  - Extending after beyond the end of the crisis
  - There is a long **overload time** for IT
  - After most of the organization as left the incident in the past
- **Remediation is not normal integration**
  - Starts in a degraded situation (destruction, compromise)
  - Adversarial situation $\Rightarrow$ OPSEC required
- **Remediation needs a dedicated management**
  - Coordination of multiple threads of actions
  - Adapting to problems in the shortest possible loops
  - Able to bridge business and IT

CEER Sequence



Remediation as a project within IR



Projects templates for remediation

- 3 templates
  - Illustrative of common strategies
  - But only an help to think strategic to operational priorities

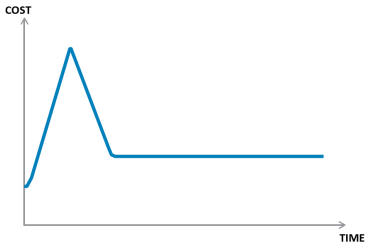
Scenario 1: Maintaining a service

Priority to a critical service running in a protected bubble. The other parts of information system might be compromised repetitively.

Scenario 2: Regain control

The whole information system is remediated but not improved Cost is significant, and incidents might diminish with time with proper continuous improvement.

Scenario 3: Restructuring



Strong investment in restructuring the information system and administration practices during remediation. The goal is to ultimately reduce the future incidents cost to very little.

5. Conclusions

The end

Contact <mailto:christophe.renard@ssi.gouv.fr>

See more at <https://cyber.gouv.fr/piloter-la-remediation-dun-incident-cyber>