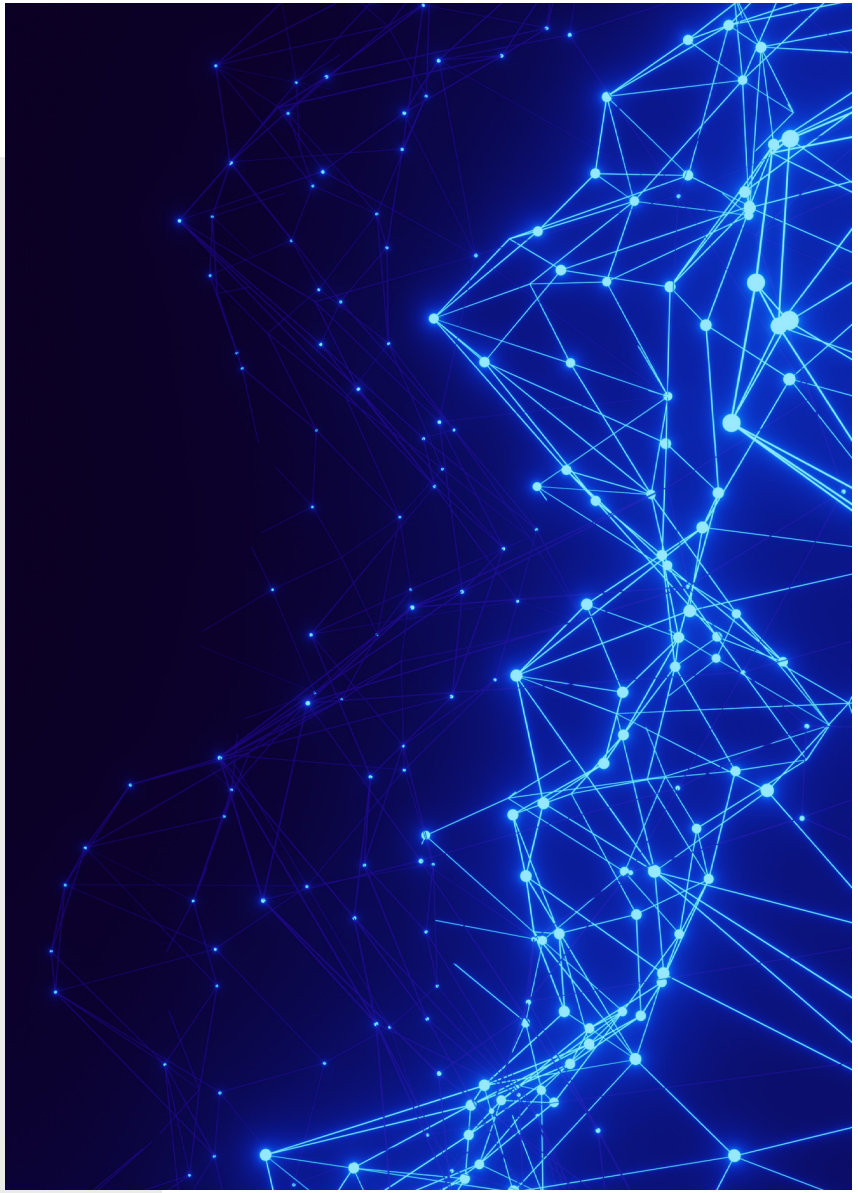
< WHITE PAPER: VULNERABILITY MANAGEMENT >

IDENTIFY AND ADDRESS VULNERABILITIES IMPACTING SOFTWARE, SOFTWARE PACKAGES, SOFTWARE COMPONENTS AND INFRASTRUCTURES



< ACKNOWLEDGEMENT >

This white paper is the result of discussions co-hosted by Julie GOMMES (AXA) and Anthony CHARREAU (Crédit Mutuel Euro-Information), and the work of:

- ALARDET Eric (Yogosha)
- BEAULIEU Benoit (Dattack)
- BREEDSTRAET Robert (Amadeus)
- CECILE Geoffroy (Sopra-Steria)
- CERDAN Vanessa (Cap Gemini)
- CHARREAU Anthony (Crédit Mutuel Euro Information)
- CORDIVAL Laurent (Headmind Partners)
- CORTES Sylvain (Hackuity)
- CREACH Jean-Baptiste (Sanofi)
- ERARD Patrick (Pôle d'Excellence Cyber)
- FIORUCCI Fabrice (Amadeus)
- GACHIGNARD Franck (Air France-KLM)
- GOMMES Julie (AXA)
- GUILLOT Yann (Amadeus)
- KHALIL Ayman (Red Alert Labs)
- KOLLA Vladimir (Patrowl)
- LESAGE Nadege (AntemetA)
- MASSONI Lauren (Wavestone)
- PARTOUCHE Johnathan (Accenture)
- PETERSEN Axel (Wavestone)
- PEYRON Lauranne (Headmind partners)
- POMMIER Christophe (Michelin)
- VALENTIN Yann (BPCE)

The working group would like to thank :

- SAS Campus Cyber, and in particular Angèle GUILBERT and Alice Aude BABOLACK NISSACK, for facilitating the organization of our working meetings and providing valuable suggestions and advice.
- Yann VALENTIN (BPCE) for initiating this working group before moving on to other functions.
- The Banking, Insurance and Financial Services group of the Cyber Campus for the prefiguration work on this white paper to be carried out in 2022.

< INDEX >

< INDEX >

< INDEX >

INTRODUCTION

This working group was set up within the Campus Cyber and drew on the preliminary work carried out by the Banking, Insurance and Financial Services group on the same topic.

It was triggered by the major problem encountered with the CVE-2021-44228 vulnerability dubbed «log4shell». Published on December 9, 2021[1], it affects the «log4j» component used in the development of Java/J2EE applications. This component is maintained by the Apache Software Foundation and widely used worldwide. The vulnerability allows remote code execution, with no special privileges and limited means of mitigating the ability to exploit it.

The ANSSI, via its «Panorama de la menace informatique 2022» published on January 24, 2023, reminds us that «the exploitation of vulnerabilities with patches is still too often observed, particularly in the context of incidents handled or reported to the ANSSI, and this despite the publication of notices and alerts on the CERT-FR website or reporting campaigns. ANSSI calls for the urgent deployment of patches on systems exposed on the Internet or, failing to do so, the implementation of workarounds».

In addition, ANSSI states that «The [Kinsing] group also stands out for automating the exploitation of vulnerabilities such as Log4J, which was exploited two days after it was disclosed».

The major challenge is to respond as fast as possible for the most critical vulnerabilities on the most sensitive assets.

Back in 2014, CLUSIF published a white paper on vulnerability management [2][3].

Exploiting a vulnerability can be the first step into a cyberattack (obtaining initial access to an information system) and/or ways of increasing the scope and impact of an attack already in progress (elevating the attacker's privileges or lateralizing the attack to other systems not previously impacted).

The area to be protected is huge, and all software publishers, including leading ones, are concerned by the existence of flaws in their code, with a trend towards increasing volumes. This is part of what CESIN describes as «a kind of fatality of digital mediocrity», where the publication of numerous and sometimes serious vulnerabilities is becoming a kind of normality for software publishers, and one with which IT managers must come to terms by regularly applying security patches.

This white paper is the working group's delivery. It aims specially to IT and security managers in public and private organizations of all sizes, whether they have their own IT or security teams, or use the services of integrators. The white paper can also be used by legal or communications teams working on crisis management.

It proposes a methodology for identifying, prioritizing and addressing vulnerabilities impacting:

- Software: developed by in-house teams;
- Software packages: commercially available or open source;
- Software components: libraries, frameworks;
- Software components: libraries, frameworks, dependencies integrated into software or packages used by the organization;
- Infrastructure elements: servers, workstations, network equipment, black-box appliances, industrial equipment.

This white paper details the steps involved in identifying and qualifying new vulnerabilities, preliminary analysis, internal and external communication, treatment and, where necessary, crisis management.

It also sets out the best practices recommended by the working group to limit or eliminate the impact of vulnerabilities.

Enjoy your reading.

[1] https://www.cert.ssi.gouv.fr/alerte/CERTFR-2021-ALE-022/
[2] vulnerability management 1 https://clusif.fr/wp-content/uploads/2015/09/clusif-2014-gestion-vulnerabilites-tome-1.pdf
[3] vulnerability management 2 https://clusif.fr/wp-content/uploads/2016/04/clusif-2015-gt-gestionvulnerabilites-tome2_vf.pdf

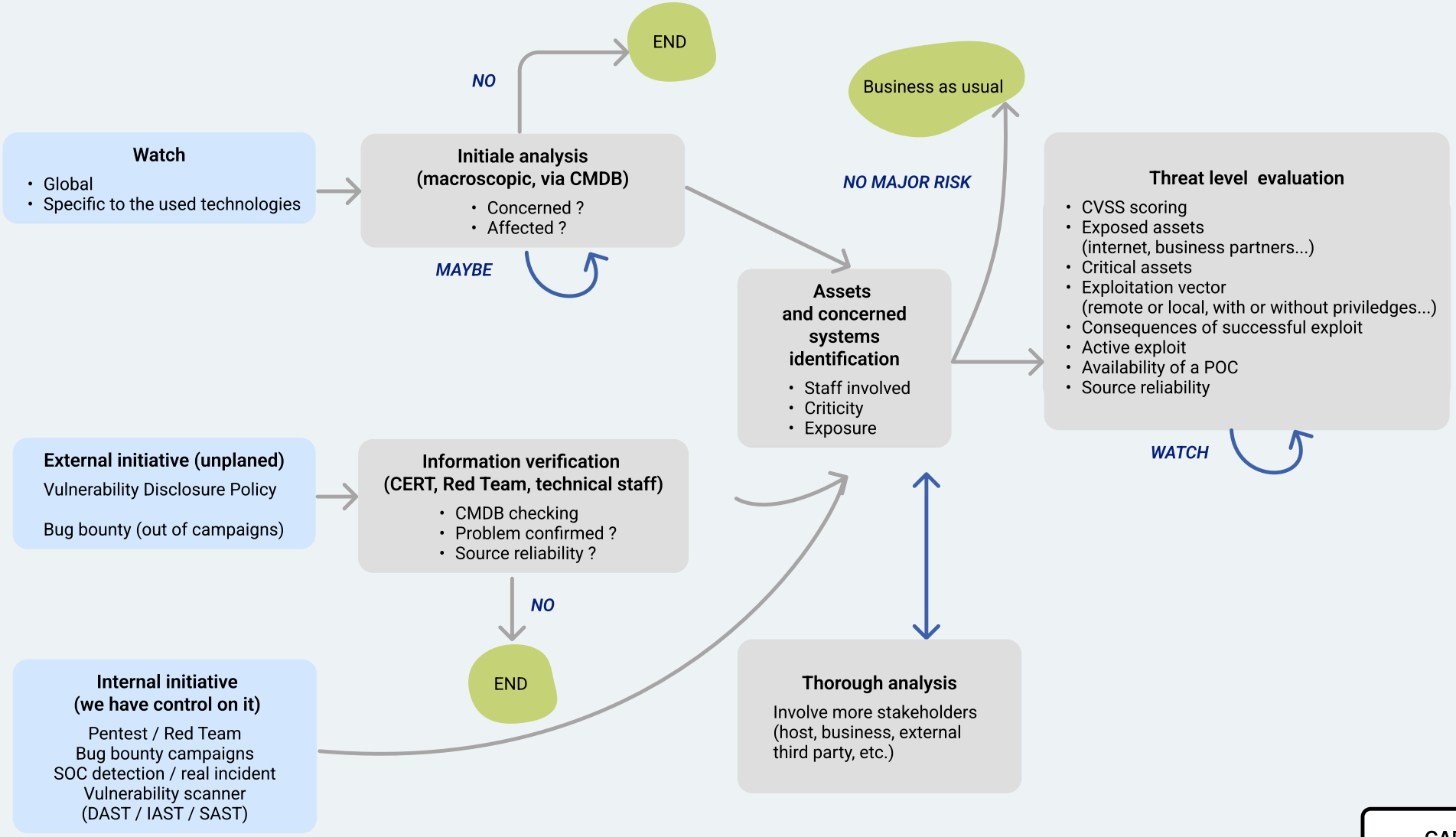
SUMMARY INFOGRAPHIC

To help you identify and deal with vulnerabilities impacting software, software components and infrastructures, the following flowchart proposes a 4-step methodology:

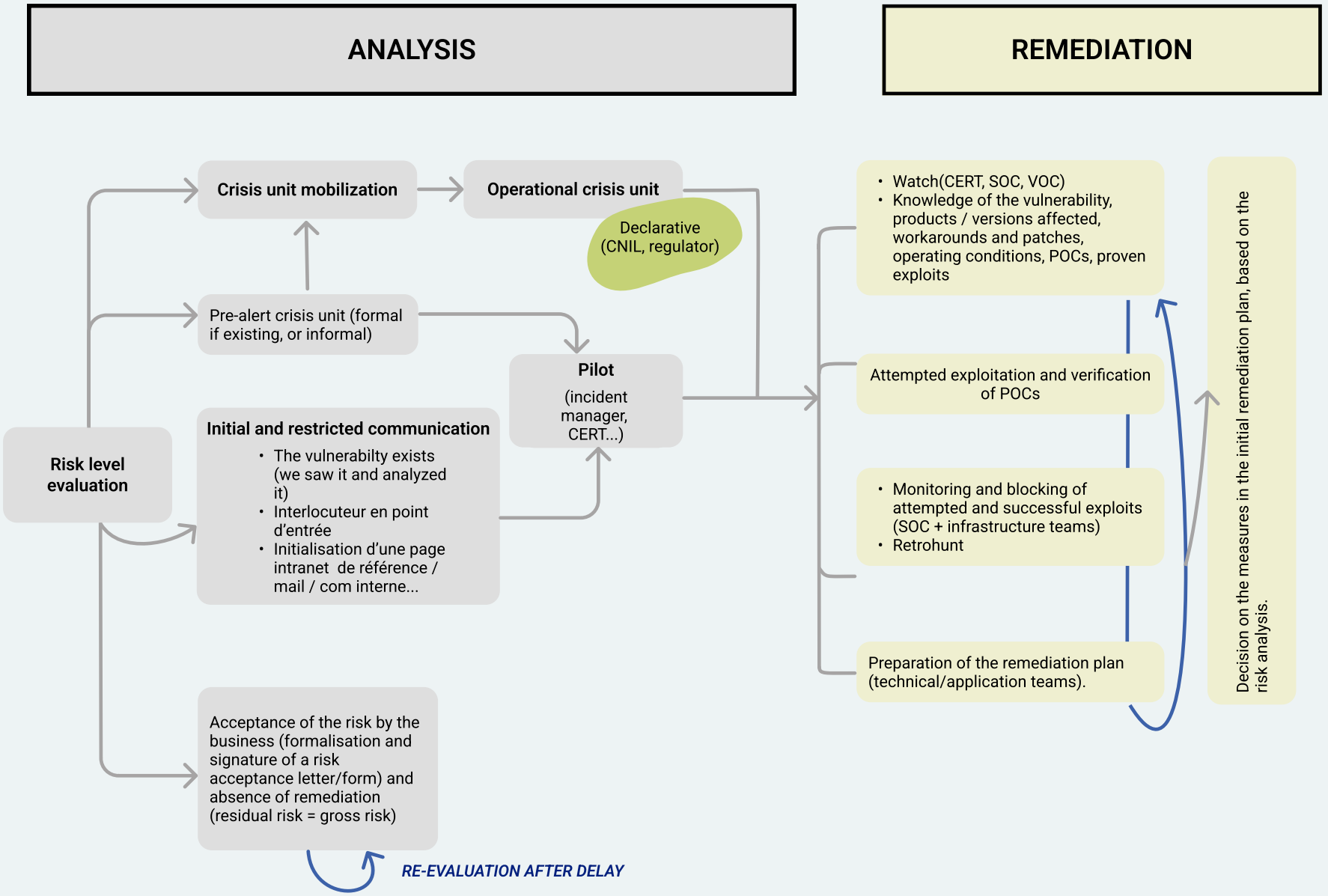
CAMPUS CYBER

IDENTIFICATION DETECTION

ANALYSIS



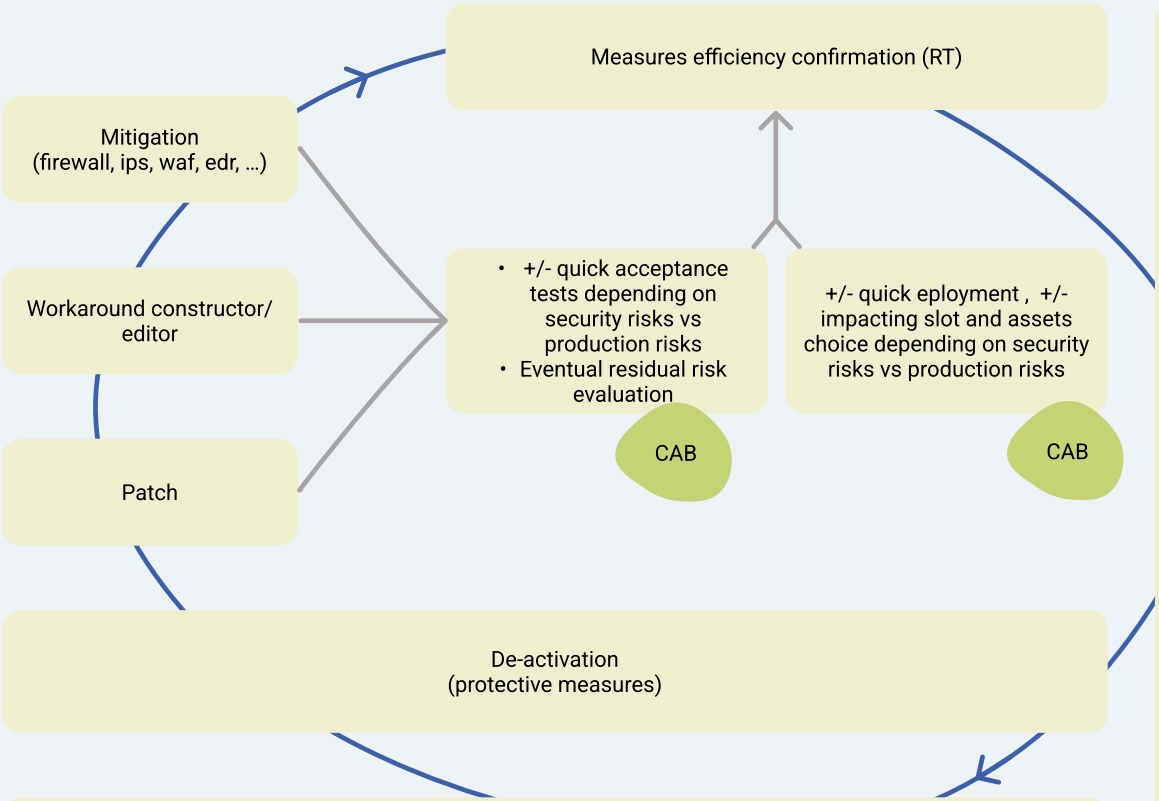
CAMPUS CYBER



CAMPUS CYBER

REMEDIATION

ROX



Remidation plan actualisation until:

- no residual risk
- long-term acceptable residual risk (risk acceptation)
- residual risk management in project mode

RETEX

Legal evaluation / SLA compliance

Communication actualisation

WATCH

GENERAL INFORMATION

In order to identify new vulnerabilities that could affect a company's information system, it is necessary to monitor the publication of new vulnerabilities and the associated threats (publication of exploit code, attack exploiting one of these vulnerabilities, etc.).

One of the **prerequisites** for effective monitoring is to have an inventory of the various technologies and products used in your company: operating systems, middleware, software, embedded software packages, firmware, industrial systems (SCADA), etc.

There are a number of complementary approaches to technology watch:

- Global watch, to keep abreast of major vulnerabilities and threats across all products;
- Vendor-specific monitoring;
- Technology-specific monitoring, via a free or commercial vulnerability monitoring service.

GLOBAL WATCH

Various sources of information on Internet keep you informed about major vulnerabilities and vulnerabilities impacting the main software publishers:

- **Governmental or institutional sources**

Many countries have their own CERTs, which publish security advisories and alerts on their websites:

  - CERT-FR (French governmental center for monitoring, alerting and responding to computer attacks) https://www.cert.ssi.gouv.fr/
  - CERT-EU (CERT of European Union institutions and agencies) https://cert.europa.eu/publications
  - CISA (US cyber defense agency) https://www.cisa.gov/news-events/cybersecurity-advisories https://www.cisa.gov/known-exploited-vulnerabilities-catalog

- **Security communities**

Non-profit organizations such as:

  - InterCERT France offers a discussion channel for sharing major vulnerabilities, restricted to association members;
  - OSSIR presents a review of security news, including vulnerabilities, every second Tuesday of the month, open to all.

- **Websites specializing in IT security**

Various computer security information websites and security product editors' blogs publish articles on major new vulnerabilities and the main threats linked to these vulnerabilities (exploit publication, current attacks). These different sources of information can offer different ways of being alerted: e-mail distribution lists, RSS feeds, X (formally known as Twitter)...

SPECIFIC MONITORING BY PUBLISHER

Based on an organization's inventory, it is possible to carry out a watch by publisher. Depending on the publisher, it may be more or less easy to track new vulnerabilities impacting their products:

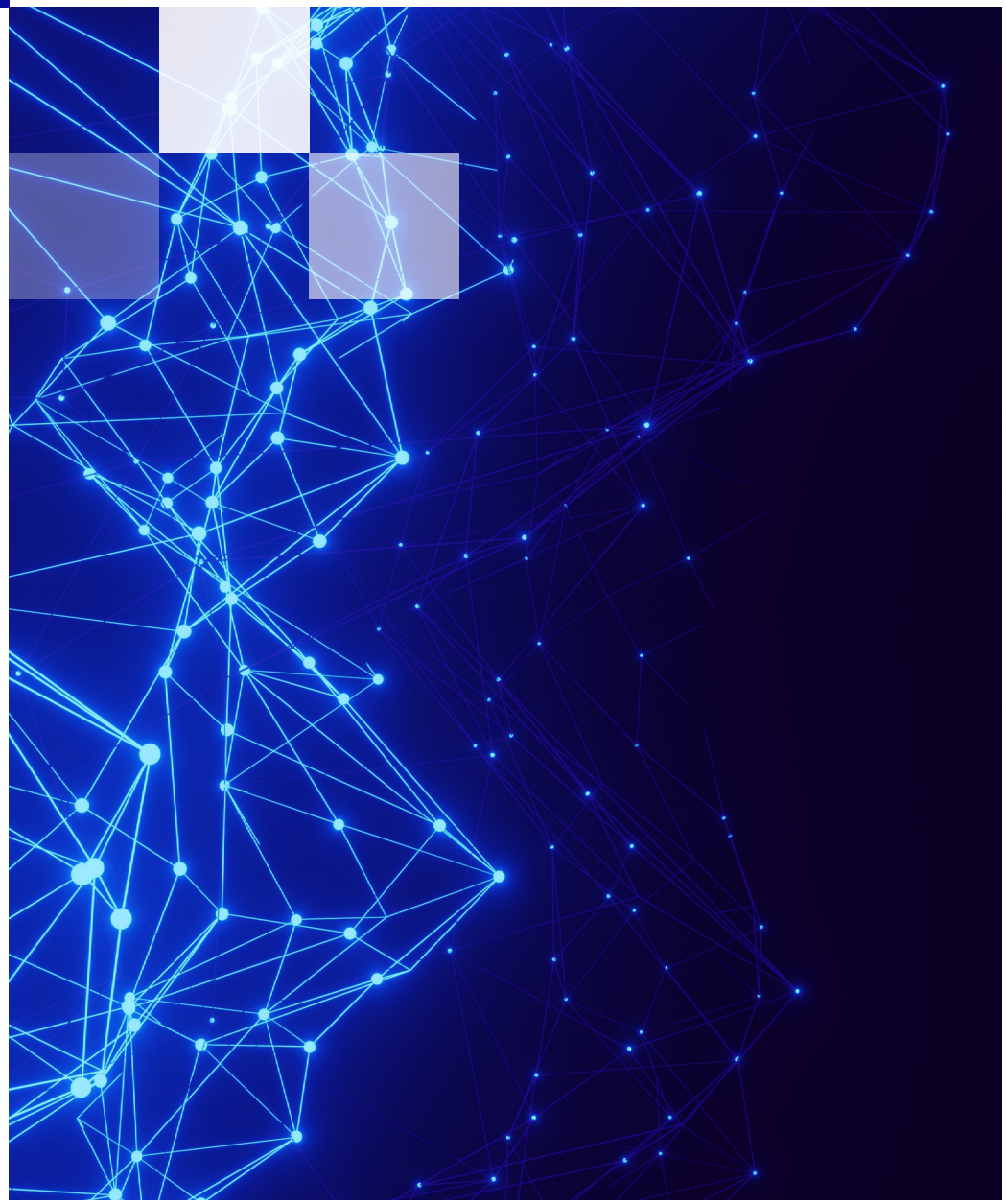
- In the best case scenario, the vendor publishes security advisories on a dedicated page of its website and sends out e-mail alerts. These advisories contain full details of new vulnerabilities, including affected product versions, severity, CVE reference, CVSS score and solution, which is usually the application of a security patch or workaround configuration;
- In an intermediate monitoring level, it is possible to:
  - Obtain information on vulnerabilities corrected in the ChangeLog of new product versions.
  - Search the NVD database (American public database of vulnerabilities based on CVE references) for new vulnerabilities published by a publisher (https://nvd.nist.gov/vuln/search).
- In the worst case, there may be no information available at all.

Some publishers issue periodic security patches to correct vulnerabilities for their products:

- Monthly (e.g. Microsoft, Adobe, SAP...);
- Quarterly (e.g. Oracle);
- No particular frequency (e.g. Linux distributions, Apple...).

MARKET VULNERABILITY WATCH SERVICES

An individual watch of each editor or manufacturer, and an exhaustive human analysis, would not be effective on an information system of intermediate or significant size. In such cases, it may be appropriate to subscribe to a market watch service, which centralizes and qualifies security advisories from different vendors. By selecting the products in your inventory, you'll be kept fully informed of the vulnerabilities that could impact your company's products, as well as the threats associated with these vulnerabilities.



« Various sources of information on Internet provide information on major vulnerabilities and vulnerabilities impacting the main software vendors»

WATCH - PAGE 12

INITIAL VULNERABILITY ANALYSIS

When a vulnerability is identified during the watch, the first step is to carry out a rapid analysis to determine whether your company could be concerned. This macroscopic analysis is based on an inventory of the assets that make up the company's information system and the ecosystem that forms the company's business perimeter. It enables you to determine whether your company:

- **Is not affected** by this vulnerability: product not in use;
- **Is concerned,** but not affected by this vulnerability: use of a non-vulnerable version of the product, vulnerable functionality not activated...

In either of the above cases, the vulnerability analysis ends, with no further action required. It also determines whether the company:

- **Is possibly affected** by this vulnerability. There is no information on whether or not the product is used in the company. A more in-depth analysis is then required;
- **Is concerned and (possibly) affected** by this vulnerability. This is the case when the product is used in the company. Sometimes, an in-depth analysis is required to determine whether the configurations or versions deployed are vulnerable.

In both of the above cases, the initial analysis iterates and continues until a deterministic conclusion is reached.

EXTERNAL INITIATIVE (UNPLANNED)

The identification or disclosure of vulnerabilities may come from an external initiative. This concerns the ways of being alerted about one or more vulnerabilities impacting one's information system, without this coming from an action initiated by the company, as a result of which it would be expected to identify vulnerabilities.

INTERNAL FRAMING OR VDP

DEFINITION

The internal framework consists in defining a Vulnerability Disclosure Policy (VDP), or, for software publishers, a Coordinated Disclosure Policy.
This is an organization set up to enable the legal collection of vulnerabilities reported by sources outside the company, in complete security.
This is both an organizational process (named contact) and an operational framework for secure technical communication resources (communication channel, encryption resources), enabling the recovery of all information linked to the found vulnerabilities, outside the legal framework of penetration tests and vulnerability bounty programs . Responsible disclosure does not necessarily mean financial reward for the researcher, as the expectation of compensation for reporting a vulnerability can be considered extortion.

PROCESS / APPROACH

Setting up a VDP (mandatory in the case of NIS 2) can be summed up by defining the people who will be the points of contact and notifying the teams that may be involved in the process. This process must involve the following players:

- Safety team (mandatory) ;
- IT team or CIO (recommended) ;
- Legal (mandatory) ;
- Communication (recommended), in particular community managers;
- Business (recommended).

VDP is governed by the ISO 29147 standard, and in particular RFC 9116, which describes the «security.txt» file. As a minimum, it is recommended that you set up a «security.txt» file on your websites, containing the information needed for responsible disclosure of vulnerabilities:

- Named contacts (team, person) and contact methods (e-mail,telephone, web form, discord...);
- Encryption key for secure exchanges ;
- Web page pointing to the disclosure policy ;
- Web page pointing to a ranking page (listing people who havereported vulnerabilities) ;
- Explanation of expectations regarding vulnerability disclosure (e.g.eplay method, test dates, test IP addresses, etc.).

The following site allows you to generate this type of file, which you can then place in the «/.well-known/» directory of your site: **https://securitytxt.org/**
Once VDP has been set up, vulnerabilities can be introduced via this channel and will need to be confirmed.

EXAMPLES

The following examples provide recommendations for a VDP :

- ENISA: https://www.enisa.europa.eu/publications/vulnerability-disclosure
- CISA: https://www.cisa.gov/vulnerability-disclosure-policy-template
- NIST: https://csrc.nist.gov/Projects/vdg/related-guidance
- Standard « security.txt » https://securitytxt.org/

TRUSTED THIRD PARTY WITH OR WITHOUT FRAMING

DEFINITION

The disclosure of vulnerabilities by a trusted third party acting as intermediary, with or without framing, ensures the legality and security of the disclosure. In general, this type of channel is chosen by individuals when they cannot find a contact within the company or prefer to remain anonymous, as long as their actions remain in good faith and without fraudulent intent. The main French channel of this type is the Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).
Disclosure by a trusted third party does not necessarily leads to financial reward for the researcher, as the expectation of compensation for reporting a vulnerability can be considered as extortion.

PROCESS / APPROACH

It is recommended that a process be set up to deal with this type of vulnerability disclosure. At the very least, a single contact or entry point should be provided.

It is also advisable to make all the company's teams aware of the fact that they could be contacted (if the third party does not identify the right contact) regarding a vulnerability disclosure, so that they can pass on the information to the right contact. Vulnerabilities may arrive via this channel and will need to be confirmed.

EXAMPLES

The following third parties may contact the company in order to report a vulnerability :

- The French National Agency for Information Systems Security (ANSSI) https://www.ssi.gouv.fr/en-cas-dincident/vous-souhaitez-declarer-une-faille-de-securite-ou-une-vulnerabilite/
- Telecom operators https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000037196108;
- The Huntr initiative https://huntr.dev/ ;
- Specialized journalists;
- News and tabloid sites with their own alert process.

OUT OF FRAME

DEFINITION

The disclosure of vulnerabilities outside the scope of the company's activities corresponds to contact by an identified or unidentified individual, via any existing communication channel (e-mail, social networks, telephone calls, etc.), with a company contact not necessarily related to security.

PROCESS / APPROACH

Although there is no framework set up, it is recommended that a process be put in place to deal with this type of vulnerability disclosure. At the very least, a single contact or entry point should be provided. It is also advisable to make all the company's teams (in particular communications teams, social network managers, etc.) aware of the fact that they may be contacted regarding a vulnerability disclosure, so that they can pass on the information to the right contact, and in particular on how to behave (don't reject the contact, respond politely and acknowledge the request, etc.).
Vulnerabilities may arrive via these channels and will need to be confirmed.

EXAMPLES

There are many cases of out-of-frame vulnerabilities being disclosed, but the companies affected generally don't advertise on it. In 2023, a young developer published a critical vulnerability on X (formerly Twitter), making it very easy to obtain the personal information of users of a dating site. The only contact with the company was to quote it in the tweet: https://twitter.com/MathisHammel/ status/1685304981803483136 Corporate social network managers (community managers) need to be made aware of these issues.

INTERNAL INITIATIVE (UNDER COMPANY CONTROL)

The identification or disclosure of vulnerabilities may come from an internal initiative. This applies to all existing methods initiated by the company, for which it is normal and expected to obtain vulnerabilities.

DEVELOPMENT CHAIN TOOLS (CI/CD)

DEFINITION

Modern application development is accompanied by numerous tools for identifying known vulnerabilities (referenced CVE, CNNVD, CWE, OWASP...), bad development practices leading to vulnerabilities, or bad configuration practices. This process is carried out continuously at each stage of development and each new production release, to avoid upstream vulnerabilities and reduce the impact on the software publisher.

There are three main categories of tools:

- SAST (Static Application Security Testing) tools enable static analysis of source code to identify bad practices, deprecated or vulnerable library versions...
- DAST (Dynamic Application Security Testing) tools allow you to interact with an application to identify configuration problems, input/output management issues, etc.
- IAST tools (Interactive Application Security Testing) combining both static (SAST) and dynamic (DAST) testing.

PROCESS / APPROACH

Implementing security tools as part of the development chain requires the involvement of security teams, so that they can benefit from their expertise during the study of the solution, the choice of solution, its deployment and, above all, after it has gone into production, in order to qualify alerts. Vulnerabilities may arrive via these channels and will need to be confirmed.

INFRASTRUCTURS INFECTING VULNERABILITIES SCANNERS

Automated scanning tools are available on the market to scan infrastructure equipment (servers, networks, etc.) for vulnerabilities.

These tools can be:
- Authenticaded to allow wider acess to the scanned system and discover vulnerabilities that require prior authentication;
- Or unauthenticated to behave like a phased attacker of discovery.

They can also be positioned to penetrate the various security layers and components in a realistic way, or as close as possible to the assets to discover more exhaustively the vulnerabilities present (but potentially difficult to exploit as they are not widely exposed via the infrastructure measures in place: firewalls, IPS, WAF, etc.)

TOOLS LIMITS

With these tool we can identify three main difficulties:
- They reveal a large number of vulnerabilities that need to be qualified in order to rule out the many false positives;
- Vulnerabilities must be contextualized and prioritized, in general by manual processing;
- Correction recommendations are generally laconic and generic, making it difficult to act simply and requiring manual enrichment work.

PENTEST AND EVOLUTION

DEFINITION

Penetration testing is the technical evaluation of the security of an IT environment. It consists in testing an application, an information system or hardware from the attacker's point of view, in order to identify vulnerabilities and defects likely to induce business risks, whether accidental or intentional.
Penetration tests can be more or less automated, existing in several variants:
- Audit-like services: penetration testing, regular penetration testing by subscription (Pentest-as-a-Service or PTaaS);
- Services for specific and complex attack scenarios: internal offensive safety exercises (Red Team) ;
- Bug Bounty campaigns ;

- Continuous Threat Exposure Management (CTEM) solutions for continuous asset mapping and penetration testing.

The advantages over SAST/DAST/IAST are, as a general rule :
- The finesse and depth of vulnerability research;
- Prequalifying vulnerabilities ;
- Contextualized, applicable recommendations.

PROCESS / APPROACH

The approach will depend on the solution adopted, but in general, the main phases are as follows:
- Definition of the scope to be assessed ;
- Contractualization ;
- Initialization, accompanied, depending on the case, by various deliverables (audit agreement, audit plan, audit authorization, etc.) and an initialization or launch meeting;
- One-off technical evaluation (penetration testing, PTaaS, Bug Bounty) or ongoing ;
- Punctual restitution during a meeting or continuously from a web portal;
- Closure in the case of service provision.

Vulnerabilities may arrive via these channels and will need to be confirmed.

SECURITY OPERATIONS CENTER (SOC)

DEFINITION

Mature in their cybersecurity managment companies have a Security Operation Center (SOC), an organization set up to detect potential security incidents.
Without going into the details of how an SOC works (some of its perimeters may be covered by a CERT / CSIRT, depending on the organization in place), these teams can step in to detect security incidents where one or more phases exploit one or more vulnerabilities in the information system.

PROCESS / APPROACH

The process of creating an SOC will not be detailed here, but although it is part of the security teams, it is necessary to define a process for reporting vulnerabilities to the SOC if they are identified as having been exploited during an attack.
Vulnerabilities may arrive via this channel and will need to be confirmed.

INFORMATION VERIFICATION

Once a vulnerability has been identified (or disclosed through an external or internal channel), it is necessary to determine whether the asset linked to the vulnerability actually belongs to the company, and whether the vulnerability has been confirmed, with regard to the reliability of the source.

CONFIRMATION

TEAM

An explicitly named team responsible for confirming vulnerabilities must be in place.

It may include :

- The CERT team, which is generally in charge of monitoring and has the knowledge required for this task;
- The SOC team, generally in charge of detecting attacks and incidents ;
- The Vulnerability Operation Center (VOC);
- Any other team or individual with technical prerequisites and a good knowledge of the company's environment.

ASSET OWNERSHIP

The team in charge of confirmation must check whether the information asset affected by the vulnerability belongs to the company. This involves checking whether the asset is actually present in the company's Configuration Management Database (CMDB), which is part of its vulnerability management obligations. If the asset is not present in the CMDB, it may be :

- Shadow IT;
- An error from the source of the vulnerability.

The trust placed in this source will depend on its reliability (see below). It is therefore advisable to manually check that the asset belongs to the information assets and/or to contact the source again to obtain more information.

VULNERABILITY AUTHENTICITY

Once the asset's ownership has been confirmed, the authenticity of the vulnerability needs to be verified: is it really true? This phase will require a technical understanding of the vulnerability and how to test it. If the means of testing it (exploit code) is provided, it must be read and analyzed to avoid any backdoor or side-effect problems, such as a denial of service.

If the testing protocol is not provided, it will be necessary to be able to make a decision without proof, the main cases being the following:

- Unknown vulnerability (unreffered CVE) :
  - With no known operating code: this is the trickiest situation to deal with. It may be worth contacting the publisher, the outsourcer, the developers... to obtain more information. This case occurred in 2023 with a simple tweet from an expert, on a Sunday, announcing a critical vulnerability in Fortinet VPNs (CVE-2023-27997). The editor then communicated about the vulnerability after 3 very long days;
  - With public operating code: this operating code must be found, analyzed, stabilized and tested, preferably on a non-production environment;

- Referenced vulnerability (CVE) :
  - No known exploit code: compare asset versions with those described as impacted by the source of the vulnerability and act accordingly.
  - With known exploit code: since the vulnerability is referenced, version comparison may be sufficient. In case of doubt, it may be worth testing the exploit code, with the necessary precautions.

SOURCE RELIABILITY

The reliability of the source is not in itself a confirmation criterion, but rather a weighting element in the confidence to be placed in a source. A vulnerability coming from from a fully automated tool (with a reputation for false positives) such as a SAST, will require more in-depth confirmation and more suspicion than an intrusion test. In the same way, an alert from the VDP will require more in-depth investigation and more suspicion than a report from the SOC team.
It will be up to the company to define its own confidence grid, but here is a first classification to help :

		Reliability concerning...	
		Belonging	**Authenticity**
EXTERNAL INITIATIVE	Internal framing orVDP	Low	Low
	Out of frame	Low	Low
	Trusted third party with or without frame	Low	Moderate
INTERNAL INITIATIVE	Development chain tools (CI/CD)	Strong	Low
	Pentest	Strong	Moderate
	Automated penetration testing with automated replay	Strong	Strong
	Threat Detection Team (SOC)	Strong	Strong

The criticality of the asset, the ease with which the vulnerability can be exploited and its exposition thus qualify the vulnerability. In the absence of an impacted asset, confirmation of the vulnerability's authenticity or a less reliable source, the process can be terminated.

If not, the process continues with the identification of the actives and systems concerned at company level.

ASSETS AND CONCERNED SYSTEMS IDENTIFICATION

Inventorying and identifying vulnerable assets is essential in order to better protect themselves. It is necessary to list the components of your environment with as much information as possible.
Here is a non-exhaustive list:

- Product name
- Manufacturer
- Product version
- Dependencies, if any
- Implementation date
- Product manager
- Criticality
- Number of components in the park
- Physical location
- Links with third parties (maintainers, outsourcers, developers, etc.)
- Other systems or applications that depend on this component (to assess the criticality of this asset)

It is also important to update this information regularly and to keep abreast of developments in:

- Versions
- Dependencies
- Contractual support levels
- End of support schedule (full, limited, limited paid, end of sup- port)
- Date of decommissioning (if no longer in the fleet)
- Manager
- Number of components

All these elements will bring added value and will enable us to better apprehend future vulnerabilities, and to spend as little time as possible wondering whether the company is vulnerable or not.

This database, if kept up to date, will make it easier to answer questions such as:

- Are we exposed to this vulnerability?
- Do we have the product in our environment?
- What is the exposure of this vulnerability in our park?
- What would be the impact of a successful exploitation of the vulnerability?

All this will make preliminary analysis quicker and easier. Numerous tools are available to produce scans, in order to maintain this database. With all the elements listed above, it's easier to identify whether the company is affected by the vulnerability, but it's important to first understand and analyze the vulnerability.
If the company is not affected by the vulnerability, there's no need to go into crisis mode.

OBSOLESCENCE MANAGEMENT

The explosion in vulnerabilities (current order of the day: several critical CVE vulnerabilities published every day) and the widespread use of open source dependencies in software have raised awareness of the need for dynamic infrastructure updates.

In the same way, product end-of-life drives obsolescence management. However, as patching frequencies and time to deploy new systems become shorter, it is recommended to adopt a posture based on principles such as:

- An obsolete base as a reason for refusal or unfavorable opinion in projects ;
- Consider as unacceptable the argument that assets using obsolete technology is not directly exposed (possible rebound);
- Invoice businesses for obsolescence-related operating costs (virtual patching, isolated «cul de sac» network zones, etc.);
- Agreed a «red button» notion: in the event of a major risk, the business is aware of a potentiel application shut down or maintenance.
- Having an obsolescence management strategy means you know your information system better, so you can manage any vulnerability more efficiently.

IN-DEPTH ANALYSIS

This stage consists of involving, if necessary, more players outside the internal IT teams (host, business collaborators, external third parties) and enriching the work of identifying the assets and systems concerned. This stage iterates with the previous one, and enables us to specify the criticality and exposure to the vulnerability based on the expert data collected.

THREAT LEVEL ASSESSMENT

A number of factors can be taken into account when qualifying a new vulnerability and take appropriate measures.

- Informations about the vulnerability itself:
  - CVSS base score;
  - Type of vulnerability: Remote Code Execution, Local Code Execution, Denial Of Service...
  - Whether or not authentication is required;
  - Whether or not an operating code exists, as well as knowledge of its operation publicly ;
  - The availability of a patch or workaround.
- Information about the affected asset(s):
  - Exposure: Internet, partners clients, internal only, behind equipment filtering the vulnerable service...
  - The impact of successfully exploiting the vulnerability ;
  - Criticality and availability of linked data ;
  - The extent of the operational, business and technical use of the affected component (in absolute terms, and more specifically in the context of the information system under consideration).

The organization must prioritize the typology of vulnerabilities according to its business priorities. For example:

- Remote Code Execution (RCE) without authentication.
- Remote control injection (RCI) for partial or total control.
- Read and write access to files on the vulnerable system.
- Read access to files on the vulnerable system
- Local privilege escalation
- Denial of service (DOS)

This is in line with the context of alerts generally issued by CERT-FR or other actors such as CERT-US, for example, concerning very often:

- Popular products: Microsoft, security equipment, VMWare, Confluence and Acrobat, well-known and widely used libraries;
- Remote code execution and authentication bypasses.

This preliminary analysis calls on technical skills and a good knowledge of the field, which can be found in teams such as: SOC, CERT, operational administration, security or risk experts and analysts. The result of the preliminary analysis work is a risk analysis, contextualized to the vulnerability studied and in the precise context of the information system or solution considered, using the criteria presented above, plus the effort required for mitigation.

A useful complement could be the production of a net CVSS score (e.g. by varying the CVSS Environmental Score), system by system, to translate this analysis work into a standard vulnerability assessment mode. It may also be useful to take into account the EPSS score.

BUSINESS IMPACT ASSESSMENT

Business impact assessment, sometimes called «Business Impact Analysis» (BIA), assesses how a breach of confidentiality, integrity, availability or traceability will block or reduce business activity, by looking at how all products and services may be affected. The ISO 22301 standard provides guidelines for a successful impact assessment. The results of this analysis must include :

- Defining the scope of operational activities;
- Mapping the dependencies between products/services, processes, activities and resources;
- The order of priority for the recovery of products/services/processes following an incident: what should be restarted/resumed first because it is more important for the business?
- Determining the resources required for priority activities/products/services: office space, people, equipment, data, communications, technological assets, third parties, budget...
- Identification of legal, regulatory and contractual requirements, and their impact on disaster recovery. For example, an application may not be critical to the business, but must be on the list of priority applications to be restarted due to legal or technical constraints (such as DNS);
- Mapping dependencies on other activities, suppliers, etc.
- Assessing the impact of an incident over time.

Impacts must be measured in the following terms, for example of each company:

- Financial: how much the company stands to lose (and/or not gain) because of the incident, market stability, fraud and financial gains...
- Reputational: estimate of brand image deterioration following the incident;
- Legal/regulatory: assessment of sanctions and disputes that may result from the incident;
- Operational: Impacts on sales, operations, productivity, projects, competitive disadvantage;
- Safety: social.

Once these impacts have been assessed, business resumption must be scheduled in order of priority.

COMMUNICATION

Communication must be adapted to the situation, and its scope must be kept to a minimum, bearing in mind that the problem is still being dealt with and remedied at this stage (it is therefore inappropriate to widely circulate a recipe that could damage the company's interests).

Three types of communication may be required, depending on the need and legal obligations:

1. **Internal communications:** exchange of information within the company between employees and departments
    a. Restricted internal communication to the relevant technical and cybersecurity teams, as well as to security management
    b. Internal communication for the Information Systems Department / Corporate Management
2. **External communications:** exchanges of information between the company and external parties, such as customers, partners, the media, etc. Examples: business partners, third-party suppliers, insurers and legal advisors, customers, end-users, etc.
3. **Communications with regulators:** exchanges of information between the company and government regulatory bodies. Examples: ANSSI, ENISA, CNIL...

The following is a typical example of how to communicate when external communication is required for a confirmed vulnerability:

1. **Identification of affected customers** using the solution in question that could be affected by the vulnerability ;
2. **Prepare clear and precise key messages** to inform customers about the vulnerability, its potential impact on their systems and data, and the remediation measures underway;
3. **Send cybersecurity notifications** to each concerned concerned, giving the level of information relevant to the vulnerability and the remediation measures taken or recommended;
4. **Set up a customer support team** if necessary to answer customers' questions and concerns about vulnerability and remediation measures;
5. **Track all communications** with cutomers and document interactions for better traceability.

RESTRICTED INTERNAL COMMUNICATION

This communication is generally issued by the SOC or CERT. It is intended for IT and security contacts who need to know about it, as they have a role in dealing with the vulnerability, implementing mitigation mechanisms, deploying the update detection of attempted exploits or compromised systems, monitoring (evolution of vulnerability analysis, availability of kits/exploit code, known compromises, etc.) or assessment of induced risks, for example.

It is technical in scope, providing details of the problem, the analysis and the action plan followed.
It can take the form of a «vulnerability sheet» distributed by e-mail and in a newsletter including, for example :

- References (CVE...)
- Description of the vulnerability (impact, systems affected, links to the editor's security advisory)
- CVSS score
- Possible solutions (patches, mitigations...)
- Threat status (public exploit, ongoing attacks...)
- Company risk assessment
- Recommendations / action plan / deadlines

For complex vulnerabilities and/or those requiring extensive remediation work (e.g. log4shell), it may be appropriate to publish an internal vulnerability log, centralizing the latest reviewed and validated information and aligning all remediation players on the same level of information, analysis and action plan. This avoids each player doing his or her own research and analysis on the basis of information found on the Internet of potentially variable relevance, leading to divergent assessments of the course of action to be taken.

This approach saves the team in charge of qualifying a vulnerability from having to re-explain remediation actions to each team in charge of correction. This approach is similar to that of CERT-FR, which regularly updates its bulletins and alerts, highlighting any changes made.

INTERNAL MANAGEMENT COMMUNICATION

This communication is generally issued by a security contact (CISO, SOC, etc.) or the team in charge of incident management. It aims to :

- Inform the IT department, or even senior management or the board of directors, of the problem and the risks involved,
- Confirm that the subject is identified and under control,
- Avoid solicitations from the other direction, following media coverage of the vulnerability on the Internet, in the specialized or general press, in circles and communities of exchange to which executives belong...

This is usually a single communication, sent early in the processing-chronology, but it presents several complexities, with the need to :

- Explain the problem and how to solve it;
- Be written early (before or at the very beginning of its popularization, if it is that this vulnerability will be publicized);
- Be written when sufficient elements are available: preliminary analysis, sufficient understanding of the problem, its stakes and how the company can respond.

In rare cases, this communication may be updated during the course of a project treatment, if the situation so requires. The working group recommends thinking through and documenting the communication model and process to be used, in advance of a real problem: trigger criteria, graphic layout, topics covered, validation circuit before distribution, distribution method, recipients. This anticipation ensures efficient, rapid handling, with minimal improvisation on the day of the event. If the vulnerability is covered by the media, internal communication can be **extended to all employees**, in order to reassure and limit anxiety, rumors...

EXTERNAL AND TOWARD REGULATORS COMMUNICATIONS

The working group notes that it is generally not the responsibility, or authorized, of technical or safety teams to communicate externally on a problem encountered within the company.
In the context of a highly publicized vulnerability, solicitations can come from :

- Customers, to reassure themselves about their data and know the degree of exposure to this vulnerability (which may be zero);
- Of partners, to find out if they are at risk (malfunction of activity, propagation through exploitation of vulnerability...);
- From colleagues (ahead or behind in understanding vulnerability and associated threats) ;
- Insurers ;
- Regulators (national, European, specific to certain countries where the company ...).

Communication is essential to reassure the various players that the problem is being properly taken into account, and to confirm that the situation is under control and does not require them to implement protective or audit measures.

More and more often, the working group realizes that external requests are now accompanied with a questionnaire specific to each issuing establishment. This leads to complexity in processing, and presupposes a personalized response each time.

The working group recommends that companies take control of their communications and issue a standard press release, planned and prepared in advance, in the event of a request, without spending time and energy on a personalized response, unless the issue at stake requires it (key customer, regulator, insurer, etc.)

External communication is generally the task of the communication teams (external, social networks, institutional...) and/or the risk management department for exchanges with regulators or supervisory authorities. These teams are not IT specialists, and must be supplied by the technical and security teams with elements of language that have already been popularized, and which can be used to create the press release.

In the same spirit as for internal communication, the working group recommends that the communication model and process to be used should be thought through and documented before a real problem arises:

- trigger criteria;
- stakeholders and roles;
- graphic layout, sections covered;
- validation circuit before use;
- distribution mode (solicitation only or proactive to selected recipients);
- ...

...to enable efficient, fast and non-improvised treatment on D-day.

Communication sample to B2B partners to pass on information regarding support within your organization:

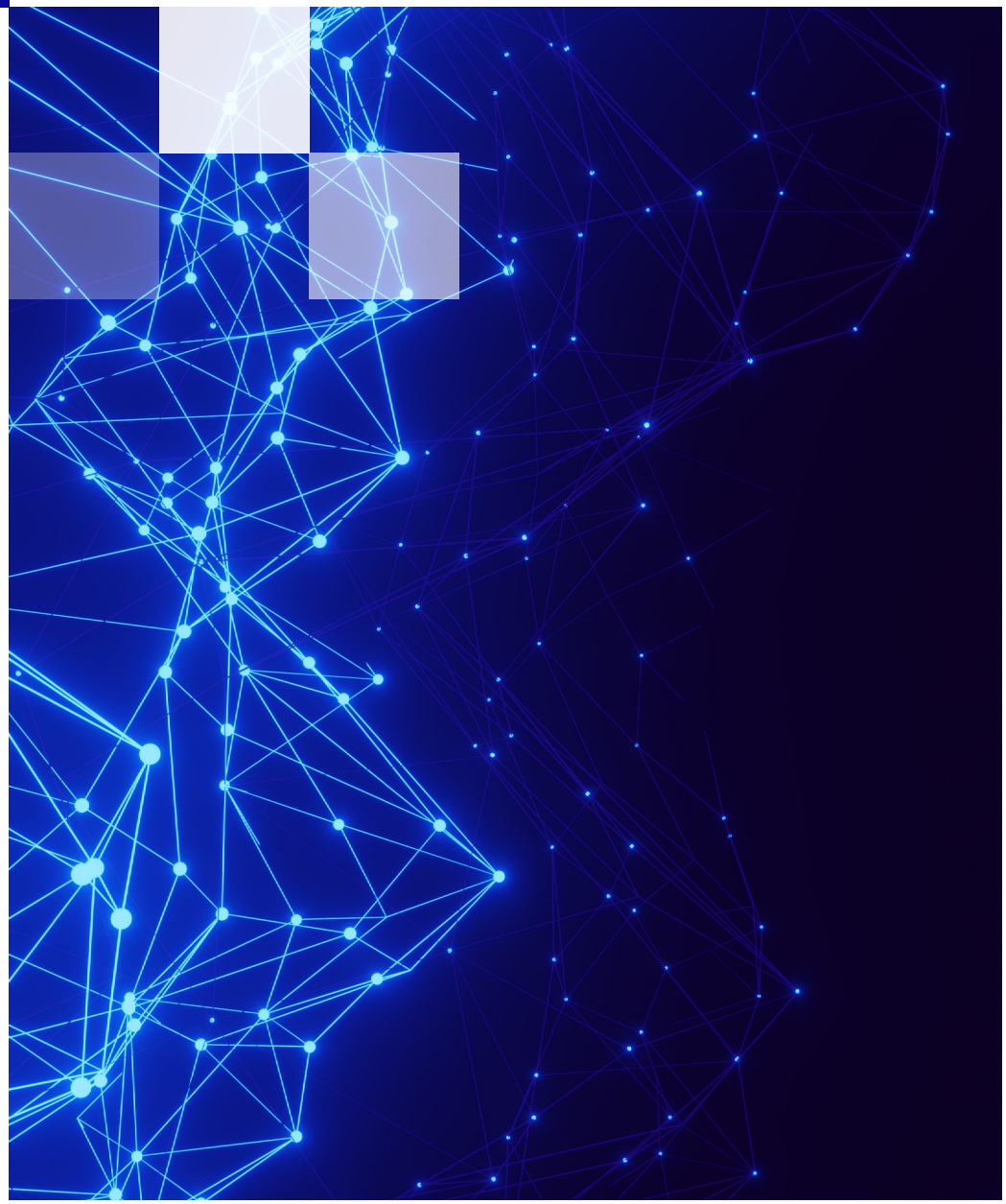
<OBJECT: [COMPANY SECURITY] - Log4Shell security alert information - Log4j>

Hello [To be personalized],

**On Friday December 10, we were informed of a critical security alert on the Apache Log4j software. Our teams were immediately mobilized over the weekend and in the days that followed to identify the potentially affected servers and implement the countermeasures recommended by our CERT and ANSSI as quickly as possible.
Since this alert, no incidents linked to this vulnerability have been reported.
In particular, the scope of this analysis in the context of our relationship is as follows:**

[Services to be customized according to B2B partner].
- Application A
- Extranet B
- Website C
- Product D

**All these services remain under surveillance.
We remain at your disposal for any further information,
[Signature to be personalized].**



«Publish an internal vulnerability log, making it possible to centralize the latest news and to align all remediation players on the same level of information, analysis and action plan to follow.»

COMMUNICATION - PAGE 32

CRISIS MANAGEMENT

The working group recommends referring to the crisis management guide published by ANSSI: https://www.ssi.gouv.fr/guide/crise-dorigine-cyber-les-cles-dune-gestion-operationnelle-et-strategique/

PREALERT

Early warning is based on the ability to identify the precursor signals of a crisis, assess the risks and anticipate an unfavorable development for the company. It plays a critical role in the successful implementation of a crisis unit.

It's a continuous, iterative process that requires constant attention to weak signals and careful risk assessment.
The following paragraphs describe a detailed process suitable for medium-sized and large companies. The various phases can be streamlined, and meetings or milestones less frequent.

This stage enables you to react proactively rather than reactively, thanks to :

- Continuous monitoring, whether technical (CERT, SOC...), societal (media, social networks, financial data) or sectoral trends;
- Continuous risk reassessment;
- Identification of internal and external stakeholders who could be affected by the crisis: employees, customers, investors, regulatory authorities, etc.
- Issuing an initial alert to these stakeholders, informing them of the event in progress and ensuring their potential availability in the event of activation of the crisis management system within minutes / following hours ;
- Rapid activation: As soon as warning signals are confirmed and risks assessed, the organization is ready to rapidly activate the crisis unit, with clearly defined roles and responsibilities, and an effective communications infrastructure.

MOBILIZATION

Setting up a crisis unit is an essential step in dealing with critical situations quickly, efficiently and in a coordinated way. The mobilization of this small but highly competent team is based on several fundamental principles that guide the organization's response to the impending crisis.

STAKEHOLDERS

When mobilizing, it is imperative to designate a clearly identified crisis leader/manager. This person must have the necessary authority to take decisions quickly, make himself understood by COMEX members, and coordinate actions efficiently in stressful situations.

The right people need to be mobilized during a crisis. The greater their number, the more difficult it can be to make decisions. So it's essential to mobilize the right people at the right time, with the right skills. Crisis units are generally made up of:

- the company's COMEX;
- the crisis managment responsible;
- the risk manager
- technical expert(s)
- direction of the communication department;
- HR and/or legal representatives (as required) ;
- business continuity planners.

CRISIS ROOM

A crisis management room must be requisitioned for this purpose throughout the duration of the event, for example, every hour. It will be used for meetings between the various stakeholders. The requisition can only be terminated once the crisis is over.
This room should be located on the company's premises, away from prying and secured so that no one can enter when a crisis meeting is not being held there.
It must be equipped with Internet access, a conference call system, telephone lines (if necessary, non-IP), whiteboard, markers, projector/video sharing system and screen.

OPERATIONAL CRISIS UNIT

An operational crisis unit meets a predefined objective: taking decisions, technical actions, ...
Each member of the crisis unit must have clearly defined roles and responsibilities, ideally at the same hierarchical level. This avoids overlaps and gaps in action. Everyone needs to understand their specific role and how they contribute to the overall crisis management effort prior to the event.

It is possible to create a sub-set of the operational crisis unit, for a given time and with a given objective, to enable a few key people (technical, compliance, legal experts, etc.) to focus on one mission, without disrupting the operational crisis unit, and to reintegrate it once the deliverable has been produced.

OBJECTIVES

The work of the crisis unit must be guided by clear objectives, defined at its first meeting. These objectives must be aligned with the organization's mission and values, while aiming to mitigate the effects of the crisis on stakeholders.

These objectives will be reiterated throughout the crisis, but crisis situations are rarely linear, and the ability to adapt quickly to change and constantly reassess is essential.

Companies with a business continuity plan have already defined an action plan to help them keep track of the various stages of the crisis (evacuation protocols, communication procedures, lists of important contacts, etc.).

CHAIN OF COMMAND

At the first meeting, it's also important to define a clear hierarchy within the crisis unit, and in particular to decide who has the right to vote on decisions. The chain of command must be understood by all members.

COMMUNICATION WITHIN THE CRISIS UNIT

The communication system must be efficient and resilient. In addition to regular, hourly meetings, for example, members need to use fast, secure communication channels to share information, updates and decisions.
It is essential to keep detailed records of all actions taken, decisions made and communications made.

During each crisis cell meeting, each participant will provide an update on the information concerning his or her scope. At the end of each crisis unit meeting, it is essential to:

- Summarize the list of actions to be taken, by whom and the fixed deadlines ;
- Inform all participants of the time of the next meeting;
- Update and distribute the status report to those who have a right to know.

RE EVALUATION

It is essential to carry out regular assessments to analyze the relevance of actions taken, and identify where improvements are needed. This feedback loop helps strengthen the organization's resilience in the face of future crises.

CRISIS EXIST CRITERIA

It's often easier to set up a crisis unit than to shut it down. By default, reaching the risk acceptance threshold is the crisis exit criterion. However, the criteria remain at the discretion of the company: it may be worthwhile to define the elements that will determine the exit point right from the start of the crisis. Deciding on a gradual exit from the crisis helps to keep the players on track and maintain their level of involvement.

Once the threshold has been reached, the solution may be to switch to the operational cell only, or to the classic vulnerability monitoring instance, where one exists.

INITIALE REMEDIATION

At this stage, the incident remediation phase begins. This involves several processes that must run in parallel.

DEFENSIVE TEAM (BLUE TEAM)

WATCH

A watch is kept by the CERT, SOC, VOC or all other infrastructure/application team concerned, depending on the organization, in liaison with the manufacturer or publisher of the vulnerable product. It consists in continuously updating our knowledge of vulnerabilities:

- Products and versions affected: after an initial assessment by the editor / builder, this list may evolve in the light of a more detailed analysis, excluding certain products where a doubt existed, or including new products not initially taken into account.
- Exploitation conditions: the payload of the attack exploit code or the modus operandi for exploiting the attack may evolve, leading to the emergence of new methods.
- Publication of a Proof Of Concept (POC): this is code demonstrating the possibility of attack by exploiting the vulnerability described. This POC may or may not be integrated into an offensive framework such as metasploit.
- Existence of proven cases of exploitation: victims who report themselves, cases of successful cyberattacks claimed by attackers, information disseminated by a national or sector CERT, etc;
- Publication of a workaround: this is generally a configuration or infrastructure measure (blocking a network port, blocking a specific operating mode, etc.), preventing or limiting exploitation of the vulnerability;
- Publication of a patch: this is the development and release of a nonvulnerable software version by the editor. A patch must be systematically checked to confirm that there is no impact on production and that the security problem described has been corrected.

Significant events must be communicated by the monitoring team to the operational crisis unit or incident manager. Evolving conditions can also lead to a reassessment of the risk level, and more immediate or drastic remediation decisions.

DETECTION AND/OR BLOCKING

In addition to its monitoring activities, the SOC needs to identify the following characteristics outstanding attack techniques, in conjunction with the Red Team, in order to :

- Implement a detection/alerting rule for attack attempts, and thus characterize the origin of malicious flows or the intensity of attempts;
- Set up a blocking rule to prevent successful exploitation of the attack, until the editor / manufacturer publishes a workaround or patch.

These detections/blocks are based on pre-existing infrastructure components: SIEM, firewall, IPS, EDR, NDR, WAF, proxy, ... Key metrics should be communicated to the operational crisis unit or incident manager. Evolving conditions can also lead to a reassessment of the risk level, and more immediate or radical remediation decisions.

RETROHUNT ANALYSIS

Once the remarkable technical characteristics of an attack are known, it is advisable to carry out a search for its markers in the information system (retrohunt), in order to check whether there have been any attack attempts prior to knowledge of the vulnerability. This task is generally carried out by the SOC (sometimes by the CERT or the IT Department, depending on the organization).

This requires the availability of event logs or flow histories (NetFlow), produced by pre-existing infrastructure components, to investigate, and sufficient retention depth to go back far enough into the past.
The detection of one or more successful attacks must be communicated to the operational crisis unit or incident manager. This changes the geometry of the incident in progress, moving from preventive actions to the investigation of a proven security incident.

OFFENSIVE TEAM (RED TEAM)

If the organization has a Red Team or a security team on the offensive, it can be involved in :

- Verify the relevance of published PoCs, and confirm that the actually enable the feared attack to succeed. This step requires operational precautions, in particular to ensure that the PoC source code does not contain a backdoor, will not allow the dissemination of sensitive information or will not compromise the information system;

- Determine the remarkable technical characteristics of the attack: payload, signature, use of an atypical port, network or system kinematics, etc., and communicate these elements for potential detection/blocking of attack attempts by the SOC or technical teams. Once the detection / blocking is in place, the SOC can confirm that it is working correctly with a new exploitation attempt by the Red Team;
- Check the effectiveness of a countermeasure (bypass, patch): confirm that a previously successful attack no longer works after implementation.

A Red Team exercise, by an internal or external team, simulating a real attack, can be organized to check that corrective measures have been applied. Typically, these exercises are conducted as follows:

- Planning phase: definition of target and objectives, including specific vulnerabilities to be tested and attack scenarios to be simulated;
- Information gathering: The Red Team gathers information, often supplied by the crisis unit;
- The attack: The Red Team simulates the attack using various techniques to exploit the vulnerability as a real attacker would;
- Evaluation of results: If the Red Team successfully exploits the vulnerability, this indicates that the patch has not been sufficiently effective, so we'll have to continue iterating in the crisis unit. If the attack fails, this indicates that the vulnerability has been correctly corrected.

TECHNICAL TEAMS

Technical teams (infrastructures, applications) are involved in implementing countermeasures proposed by the SOC or CERT (e.g. firewall rules, WAF rules, etc.) and testing the correct operation of workarounds or patches proposed by the vendor, both in terms of the absence of impact on production and the ability to deploy the patch on the infrastructure (packaging, deployment strategy, etc.).

Ideally, tests should be carried out on a qualification environment representative of production, failing which on a unitary production element or excluded from the processing of real production flows for the duration of the test.

CONCLUSION

Based on the analyses and risk assessments communicated by some or all of these three teams (red team, blue team, technical teams, depending on the size and organization of the company), the incident manager or the operational crisis team reassesses the level of risk and draws up an initial remediation plan, which may be updated on an ongoing basis as the data communicated by the 3 teams evolves.

In many operational cases, it is not possible to wait for complete knowledge of the vulnerability and certainty about the suitability of the remediation plan before taking action. Operations are frequently iterative, and some initial countermeasures may be deactivated once other measures or a patch have been applied. The remediation plan must therefore remain open-ended. The aim is to assess the risk to production and business continuity in relation to the security risk, and to maintain a controlled and acceptable level of risk with the actions decided upon.

DETAILED REMEDIATION

The preliminary vulnerability analysis enabled us to rapidly launch internal and external communication initiatives, as well as providing the means to continue addressing vulnerability if necessary.

The next stage in the vulnerability management process mobilizes a wider range of players and expertise, in order to identify vulnerable systems and applications, mitigate potential impacts, apply patches, monitor and respond to incidents. So security teams, application production teams, infrastructure teams, Dev leaders, CERT/CSIRT, SOC, Red Team, application managers, business continuity, and more if need be - depending on the organization - are mobilized.

The inventory and discovery of vulnerable assets will be based on the organization's cartography when it exists and is up to date, and can be combined with vulnerability scans. Vulnerability scans offer the identification of published vulnerabilities to facilitate the search.

In-depth analysis and qualification of the threat, using reverse engineering, will enable us to understand and block the threat, and test workarounds and exploits.

Strengthen vulnerability monitoring, through external monitoring services and exchanges within the community, and through internal cybersecurity monitoring (SOC, CERT/CSIRT) will provide information about its exploitation (frequency, targeting, actors), but also potentially indicators of compromise (IOCs) that will enrich detection tools and rules.

Dealing with a critical vulnerability is similar to dealing with an incident, even if there is no proven impact. In fact, the resources mobilized, the actions taken to measure the risk and potential impact, and the communication tools used, justify formalizing and tracking events in the same way as for a security incident. This will facilitate follow-up over time.

INITIAL PLAN AND WEIGHTING OF VARIOUS REMEDIAL SOLUTIONS

Once the analysis phase has been completed, the output will be a coherent set of applicable measures known as the «Initial Remediation Plan». For the purposes of this document, a good definition of remediation would be: «The process of improving or correcting a risk situation induced by a vulnerability.»

This initial plan broadly documents the various methods available for correcting the vulnerability. Broadly speaking, there are three types of remediation:

1. Patch: in this situation, the vendor or manufacturer associated with the vulnerability proposes a software patch to correct it. This patch may not fully correct the vulnerability, and the vendor may announce more comprehensive releases in the future. In all cases, this can have a knock-on effect on production, in which case you need to assess the risk induced by the vulnerability and the impact of the patch.
2. Workaround: in this situation, the editor or constructor does not propose a patch, but a workaround that renders the vulnerability unusable. This may involve, for example, the application of a particular configuration.
3. Mitigation: In this situation, it is not possible to fully correct the vulnerability, either through a patch or a workaround: the tactic will be to indirectly mitigate the risks associated with the vulnerability.

This may involve:

- «Virtual patching», which consists in blocking exploitation of the vulnerability by a solution positioned upstream of the vulnerable asset. The most classic cases are the activation of rules on a Web Application Firewall (WAF) or an intrusion detection/prevention probe (IDS/IPS);
- Block or restrict access to the vulnerable service through network filtering ;
- Complete disconnection of the network and system affected.

Important: For some vulnerabilities, two or three remediation categories are applicable. It will be up to the organization to define the best remediation plan for its context.
The following attributes can be used to characterize each remediation method:

Remediation #	% correction - from 1 to 100%	Risk associated with procedure (green, yellow, orange, red)	Application time	Level of production disruption
(Required attribute)	(Required attribute)	(Required attribute)	(Optional attribute)	(Optional attribute)
Remediation 1				
Remediation 2				
Remediation 3				

The «Application time» and «Production disruption level» attributes obviously depend on the organization's activity, and will not be useful or systematic in all contexts. Following this study, a remediation plan is drawn up, the organization must now confirm the effectiveness of the selected corrective measures.

VALIDATION OF CORRECTIVES MEASURES

It is extremely important for the organization to validate the selected corrective measures in real-life situations. Several scenarios (nonexhaustive list) justify this step:

- The corrective measure does not achieve the desired objective;
- The corrective measure works, but the time taken to apply it leaves the organization at risk for too long;
- The corrective measure requires a greater interruption of service than calculated;
- The supplier's documentation for applying the corrective action does not accurately take into account the organization's specific context. Tests are therefore needed to document the application of the measure in this context.

Validation tests should be carried out on a platform representative of the production environment, and the procedure documented if necessary. The qualifying terms used to designate the validation environment may vary according to the organization, but here we are generally referring to environments of the following types: test, integration, validation, qualification, certification...

Important: The reasonable period of time required for validation must be assessed in relation to the risk associated with the vulnerability in question. Indeed, if the vulnerability carries a high risk for the organization, it must remain pragmatic and evaluate the duality of «security risk» vs. «risk of service interruption for production». It's not a question of «consuming» a week for additional testing if it's a question of correcting a critical vulnerability for the organization. Unfortunately, there is no universal formula, but the organization must adopt a pragmatic and agile approach.

Once the tests have been finalized, the organization will have to assess whether the expected result has been achieved, and potentially correct the remediation table presented above. In addition, it will now be possible to document the change request and prepare for the meeting with the change validation committee.

CHANGE REQUEST DOCUMENT AND VALIDATION BY THE CHANGE ADVISORY BOARD

Applying a remediation measure means actually changing one or more IT systems. Most organizations have a Change Advisory Board (CAB) to validate the change request linked to the application of the remediation measure.
In smaller organizations, there is no formal CAB, but here again it's a question of being pragmatic and bringing together the people concerned by a potential impact linked to the corrective action.
The creation of a change request document and the organization of a CAB are beyond the scope of this document, but certain questions will be systematically evaluated during a meeting with the CAB, so it's important to prepare the answers well in advance:

- What are the benefits of applying this patch?
- What is the risk involved in applying the patch?
- What is the procedure for going back if a problem arises during the cours of a project procedure? How long does it take?
- Has the reversing procedure been tested?
- Which production services are affected and for how long?
- What is the escalation procedure in the event of a problem during the remediation ?

Once the change request has been validated, the next step is to plan the deployment of remediation measures.
It is important for the CAB to be aware of vulnerability management. This process must not be a major obstacle to maintaining the security of the information system.
In the case of the most critical vulnerabilities, it must be possible to bypass the CAB, thanks in particular to the confidence in the remediation validation provided by tests carried out in an environment representative of production.

DEPLOYMENT PLANNING AND IMPLEMENTATION

RISK PRIORITIZATION

Risk-based prioritization involves defining which fixes are essential to maintain an acceptable security posture, while taking into account the overall workload of production teams. It is quite exceptional to have the capacity to correct all vulnerabilities - in fact, it is generally impossible. We therefore need to be able to analyze the risks resulting from each vulnerability, prioritize those that are essential to correct and plan the treatment of those whose impact is not critical.

The method is quite similar to conventional risk management. In the context of vulnerability management, risk-based management consists of assessing a number of essential criteria (the list is not exhaustive): the severity of the vulnerability itself, the asset's operational readiness and regular patching, the possibility of attackers actually using the vulnerability, and its potential impact in the context of the organization. All these combined criteria applied to each vulnerability will enable us to draw up a list of priority vulnerabilities to be corrected.

DEPLOYMENT STRATEGY

Deployment strategy is linked to the organization itself, and can be influenced by various criteria:

- Does the organization have one or more deployment tools?
- Are the various IT environments managed by a single team, or are they managed by different teams? is responsibility shared?
- Is an application or structural perimeter more susceptible tovulnerability?
- Does the deployment of the corrective measure require an impact on the availability of this or that service?

Some organizations prefer to manage the pace of updates according to a categorization by type of environment: the SSVC method (see. https://www.cisa.gov/stakeholder-specific-vulnerability-categorization-ssvc) defines a typology with 4 possible choices:

1. «No remediation applied»
2. «Application of remediation to the next scheduled maintenance».
3. «Application of the remediation at a specifically defined date without waitibg for the next scheduled maintenance».
4. «Immediate application of remediation»

Note: The term scheduled maintenance refers to one or more known, pre-planned dates dedicated to the application of scheduled remediations. These are dates when the production service is interrupted in order to carry out specific tasks, usually including hardware changes, heavy application updates and, of course, the application of scheduled remediations. Throughout the remediation process, the status of the remediation plan and vulnerability can be modified as follows:

- Environment A: Risk accepted, date undefined
- Environment B: Accepted risk until scheduled maintenance
- Environment C: Risk accepted until defined date
- Environment D: Undergoing remediation

Some of the more complex remedial measures could potentially be integrated into current projects, or lead to the creation of a new project, as in the case of obsolescence management.

DEPLOYMENT

It is possible to categorize several types of deployment:

1. Automatic deployment using tools;
2. Deployment requiring manual intervention via an interactive session on the system itself ;
3. Centralized deployment entails action on the source code and therefore redeployment.

Depending on the nature of the assets concerned, technical management may vary. The main situations encountered are as follows:

- Workstations are managed by a central tool
- Servers are managed by a central tool or by individual interventions.
- Cloud environments are managed using templates and code, and specific tools.

Once the remediation has been deployed, the status of the vulnerability can be changed to «declared corrected».

REMEDIATION VALIDATION

Once deployed, it is essential to check that the correction is correct. or mitigation through a new vulnerability scan.

- In a business as usual context, the verification will be carried out during scheduled scans according to the usual workflow (for example: scan every week or continuously);
- In the event of a crisis (such as a 0-day vulnerability), it is advisable to carry out a scan immediately after remediation has been deployed.

In some cases, particularly in the case of mitigation measures, scans will not be sufficient to confirm correct remediation. Specific checks, such as a Red Team exercise, a penetration test or a script test, are required, depending on the criticality or the level of confidence attributed to the editor.

Once the remediation has been validated, the treatment status of the vulnerability can officially be changed to «corrected».

PRECAUTIONARY DEACTIVATION MEASURES

In addition to applying mitigation, bypass or correction measures, the remediation phase may involve temporarily disabling perimeters of the information system, Cloud solutions or vulnerable products. The aim of these conservative deactivation measures is to minimize risks and prevent any potential exploitation before the remediation process has been completed.
Deactivation is a radical solution that needs to be prepared for, in particular to limit its technical and business impact.

PRINCIPLES

Potential deactivation of vulnerable perimeters must be anticipated on the following points:

- Technical impact analysis: which technical services vital to the IS, solution or product could potentially be affected by a vulnerability requiring them to be deactivated?

For example, if the vulnerability affects a centralized authentication service, disabling it can block access to all resources.

- Business impact analysis: what would be the customer, legal, image, operational and financial impact of a forced deactivation of the IS, solution or product, and what would be the maximum acceptable duration for the organization?

For example: if access to an e-commerce site is deactivated for more than n days, this would have an unacceptable impact in terms of potential loss of sales and customers.

- Alternative IT solutions: is it possible to switch the vulnerable perimeter on an alternative, non-vulnerable perimeter?

Example: Use a Web presentation server with alternative technology, or switch to an earlier, non-vulnerable version.
Example for an IS: backup chains based on different security equipment, different OS, etc.

- IT degraded modes to reduce impact.

Example for a deactivated website: use DNS or reverse proxy to switch flows to a «maintenance» or information page to limit the impact on the image.

- Precautions to be taken to enable investigation teams to determine whether or not the vulnerability has been exploited.

Example: Disconnect/isolate vulnerable perimeters if necessary, but do not switch them off.

The effort required to prepare these alternative plans, and their effectiveness, may fluctuate. Their appropriateness and feasibility must be studied taking into account :

- Expected impact reduction

Example for a website: a simple switch to a maintenance page may limit the impact on image, but would not reduce the impact on sales linked to the unavailability of a particular service.

- The effort and cost involved in implementing and maintaining the system in operational conditions, in particular through periodic testing.

Example: The development and maintenance of a back-up system based on alternative technologies may involve efforts and costs that are disproportionate to the expected potential efficiency and the financial loss associated with the unavailability of the nominal system.

ACTORS / TEAMS INVOLVED

- **Businesses** will be able to assess the impact of deactivating a particular IS perimeter, Cloud platform or product, and contribute to the decision to opt for a particular alternative solution;

- **IT teams** (applications and infrastructure) will also help to identify the impact of deactivating a given perimeter and, if necessary, propose alternative solutions to limit this impact.

BUSINESS CONTINUITY PLAN AND DISASTER RECOVERY PLAN

A vulnerability impacting transversal services of an information iystem or access to a Cloud platform (e.g.: core of trust, DNS, identity repository, SSO...) may require the deactivation of these services and consequently impact a wide perimeter of business activities.

Likewise, the exploitation of a vulnerability can render a large perimeter of services unavailable for the time needed to remedy it. In order to limit the impact, two types of response should be considered:

- The Business Continuity Plan (BCP) - which aims to continue business activities according to an established and rehearsed plan;
- The Disaster Recovery Plan (DRP) - a component of the BCP which aims to rebuild, in the more or less long term, the information system on which business activities are based, generating partial or total unavailability.

PRINCIPLES

These emergency plans are mainly based on the following activities:

- **Preliminary identification of the risk scenarios to which they must answer.** For example:
  - «Classic» scenarios, such as the unavailability of a critical supplier or the unavailability of a hosting site following a physical disaster (fire, flood);
  - Scenarios of a logical compromise/destruction of the nominal IS propagated to its replicas hosted on backup sites;
  - Scenarios linked to critical vulnerabilities that can only be addressed by shutting down the organization's IS or its IT supplier e.g. critical vulnerability massively impacting the IS of the outsourcer or Cloud service provider).

These risk scenarios are characterized in particular by the likelihood of their occurrence (depending on the threat, the proven effectiveness of existing protection measures, etc.) and by their impact on the organization if they do occur (up to and including calling into question the organization's existence in the event of bankruptcy, for example). This characterization makes it possible to prioritize the risks to be covered, and consequently the plans to be implemented.
For example, an organization may decide that, given the state of the threat and its cyber maturity, the main risk to be covered is that of a cyber attack on its information system, before that of a physical disaster impacting the hosting of its IS, or the failure of one of its critical suppliers.

- Identification of the business activities whose shutdown will have the greatest impact on the organization. These plans must make it possible to resume:
  - Within a defined timeframe;
  - With data freshness in line with defined RTO/RPO.

Example: Disaster recovery plans must enable sales-related activities to be resumed within x days and without having lost more than 24 hours' worth of data, otherwise the company's survival is at stake.

- Definition of the main principles of emergency plans: *Example: A plan may enable the business to resume a degraded activity for x weeks, using resources that are independent of the company's nominals. This plan might involve exporting data from management applications customer and supplier lists, inventories, orders, etc.) to the Cloud on a daily basis, in desktop format, so that they can then be processed using standard tools that are immediately available.*

- Implementation of resources related to these plans ;
- Documentation of the sequencing of operations linked to the resumption of IS functions/business activities and associated procedures, triggered and monitored as part of crisis management;
- Tests (unit / global) and periodic updates of plans and documentation.

ACTORS/TEAMS CONCERNED

A **sponsor**, aware of business and IS issues, able to arbitrate the allocation of the human and financial resources needed to draw up and maintain the plans;

- The business lines, which will express their needs, contribute to the choice of plans and to the development of business degraded modes without IS or with alternative IS solutions;
- IT teams (applications and infrastructures) who will document, implement and test IS recovery plans;
- A «pilot» who will coordinate and monitor actions related to the preparation of these plans and their maintenance and testing ;
- External correspondents (e.g. outsourcing correspondent, cloud service provider).

LEGAL ASSESSMENT & SLA COMPLIANCE

Legal assessment is a crucial step in the overall management of vulnerabilities, as it ensures that all actions taken by companies to remedy a vulnerability comply with current regulations and contractual obligations.
It is essential to ensure that Service Level Agreements (SLAs) with customers or partners are respected throughout the remediation process.
To ensure proper compliance and effective management of the legal aspects of vulnerability, legal consultations and exchanges with the appropriate stakeholders are essential. When it comes to vulnerability management, both from the point of view of the supplier and the consumer of services/solutions/products, regulatory compliance is an important issue. Non-compliance with regulations and directives can in some cases lead to significant financial penalties, legal action, loss of customer confidence and negative repercussions on the company's reputation.

PRINCIPLES

Preparation phase :
Independently of the process described in this document, it is essential for a company to carry out the following activities in order to operate effectively when dealing with a vulnerability:

1.Identify the various legal issues: it is important to identify the security regulations, laws and directives that apply to the company and the systems concerned. It is also necessary to determine the potential consequences of non-compliance with legal and regulatory obligations. In particular, this phase enables us to list the solutions to be monitored on a regular and close basis when applying a vulnerability management process;

2.Legal consultation: if the organization does not have a legal / compliance department, it is strongly recommended that external legal consultation is used to obtain expert advice in these situations.

Identified vulnerability phase

When a vulnerability is identified at the level of an organization providing a service, solution or product, it is essential to follow specific legal steps to ensure appropriate risk management and legal compliance tailored to the business. Here are the main steps to follow:

1.Identifying and documenting the vulnerability: the first step would be to accurately identify and document the vulnerability to make it understandable to the legal team, including its potential impact on the service, as well as the systems or data that could be affected.
Example: SQL injection vulnerability on the XX server, with the possibility of recovering information linked to all users, such as surnames, first names, e-mail addresses and passwords.

2.Involvement of legal teams: when a vulnerability is identified, it is essential to involve the legal department and/or legal consultant as early as possible to assess the necessary legal implications.
Example: if the vulnerability affects a service essential to the nation, this may involve specific actions within the framework of the LPM.

3.Regulatory compliance analysis: depending on the need, the legal department/consultant should conduct an in-depth analysis to determine whether the identified vulnerability leads to violations of specific regulations relating to information security, personal data protection or other legal obligations. *This analysis will enable us to understand the potential legal risks and develop an appropriate approach to remediation.*

This phase depends on the company's sector of activity and geographical location, and there may be specific standards, regulations or security frameworks that need to be taken into account in the remediation process. *Example: GDPR, LPM, etc.*

4.Contracts and SLAs with customers: if the company provides services/solutions/products to customers, it is important to check the contracts and service level agreements (SLAs) in place to ensure that remediation actions are in line with the commitments made to customers in terms of security and service availability. *Example: customer notification within 48 hours in the event of a vulnerability critical in accordance with a legal clause in the contract.*

5. Notifications to relevant stakeholders: depending on the nature and scale of the vulnerability, it may be necessary to notify relevant stakeholders, such as customers, users or even, in some cases, regulatory and/or certification authorities such as ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) or ENISA (European Union Agency for Cybersecurity).

Example: in the context of a GDPR-related breach in France, in the event of confirmation of the exploitation of a vulnerability enabling personal data to be recovered, this may involve specific actions such as notifying the CNIL (Commission nationale de l'informatique et des libertés) within 72 hours.

6. Drawing up a remediation plan: In collaboration with the legal department, the company draws up a remediation plan that takes into account both technical and legal aspects. The plan should include specific measures to correct the vulnerability, as well as actions to comply with applicable regulations.

7. Internal communication: depending on the legal remediation plan, managers inform the relevant internal teams, such as the technical team, security managers and key stakeholders, of the remediation measures envisaged. Depending on the case, the parties involved may have a different role in the vulnerability resolution and legal compliance process.

8. Implementation of remediation measures: the company must ensure that the agreed remediation measures are implemented in a way that complies with legal requirements, and that they are effective in correcting the vulnerability.

9. Tracking and documentation: Traceability is a key activity from a legal point of view. The company must ensure that all actions taken to remedy the vulnerability, as well as discussions and decisions taken in collaboration with the legal department, are tracked, documented and auditable.
Example: confirmation by e-mail from the technical team of the resumption of a service subject to strict contractual recovery clauses.

ACTORS / TEAMS INVOLVED

- **Legal and Compliance Department:** these are the key players involved in the legal assessment of vulnerability, the analysis of legal risks, the identification of regulatory and legal obligations, the potential impact on the company from a legal and compliance point of view, and the definition of planned remedial measures in relation to regulations and directives.

- **IT security/operations teams:** these teams provide technical information on the vulnerability, such as its impact and possible remediation measures from an operational point of view. This collaboration is essential to understand the nature of the vulnerability and its technical context.

- **Customer or partner legal departments:** in cases where the vulnerability has a direct impact on customers or partners, their legal teams may be involved to assess the impact on their own contractual obligations and SLAs.

- **Corporate management:** corporate management is generally kept informed of important legal aspects relating to vulnerability and SLAs, in order to make strategic decisions.

- **Communication team:** the communication team needs to be kept abreast of the legal implications of vulnerability, so that it can effectively manage external and internal communication when necessary.

- **Auditors and regulators:** depending on the nature of the company and its regulatory obligations, internal or external auditors, as well as regulators, may be involved in assessing the company's compliance with information security regulations.

UPDATING COMMUNICATION

This stage of the process involves updating vulnerability and remediation communications that have already been initiated. Clear, proactive and regular communication helps to maintain trust and ensure effective coordination throughout the remediation process.

PRINCIPLES

Communication updates are based mainly on the following activities:

1. **Communication frequency:** determines the frequency with which communication updates will be provided. This may evolve according to the criticality of the vulnerabilities and the time required for remediation. Certain regulations may also dictate the timing and frequency of communication requirements.
Example: when a critical vulnerability is confirmed, the company should communicate at least once a week on the progress of the remediation plan to the customer, in order to respect a specific contract.

2. **Communication content:** any changes to the action plan, progress made and results achieved.

3. **Communication in the event of delays or changes:** it is advisable to set up a specific communication process in the event of a delay in remediation or a change in the initial plans, to quickly inform the stakeholders concerned, provide clear explanations and propose alternative solutions if necessary.

4. **Incident and post-remediation analysis reports:** for any vulnerability identified, which may be associated with a crisis and finally corrected, it is advisable to produce at least one postremediation analysis report.
These reports detail the lessons learned, improvements made to the vulnerability management process and preventive measures for the future. This content can be used in communications to raise awareness and build good habits.

UPDATING THE REMEDIATION PLAN

The remediation plan is updated iteratively until :

- The absence of residual risk ;
- Sustainable residual risk (risk acceptance) ;
- Treatment of residual risk in project mode with established planning.

At this stage of the process, the choice made to manage the vulnerability is bound to have an impact on the nominal operation of the system in question, whether through the implementation of new measures, the deactivation of functions or the application of continuity or recovery procedures.

The level of risk initially assessed must then be recalculated in all cases (even if it was initially accepted) on the basis of the effectiveness of the measures adopted, or with regard to the consequences of deactivating functions or resorting to business continuity and recovery plans. The risk reassessed in this way is called residual risk. In this sense, residual risk is the part of the original (initial or gross) risk that is not addressed by the remediation.

Several postures are possible. If the residual risk (initial or gross) is :

- Above the acceptability threshold: work must continue to reduce the risk by supplementing or modifying the action plan, and iterate on the process;

- Below the acceptability threshold: the impacted component has returned to nominal operation in terms of availability, performance and security, in accordance with any SLAs defined. The residual risk must be recorded in the Risk Treatment Plan and accepted as such by management and the defined owner. Work may continue in order to reduce / totally eliminate the risk if possible, but this may take place outside the exceptional organization (crisis management, etc.) which was initially put in place when the risk exceeded the acceptability threshold.

FEEDBACK (RETEX)

At the end of the eradication phase, or more generally when the incident is considered to be under control and is being handled again in a nominal context (outside the crisis/enhanced monitoring framework), it is worthwhile systematically continuing the treatment with a feedback phase (RETEX). Treatment requires resources and time. To this end, it is important to capitalize on the investments made. Capitalization is understood in terms of event qualification, management and escalation, treatment, reactivity and reproducibility of the event.

This phase is based on a report written by the incident manager, generally including a managerial summary, a list of positive points and areas for improvement recorded, if possible, as the incident progresses, and a chronogram of major actions and highlights, extracted if possible from the incident management logbook, which records the history of events, actions, decisions, results and failures.

This report is presented at an on-the-spot RETEX meeting scheduled for the following days, to ensure that we still have a very detailed memory of events. If necessary, the incident manager can interview some or all of the protagonists to complete the report and prepare the meeting.

This meeting should bring together all those involved in the incident to record their comments and collectively update the report. Ultimately, this meeting aims to draw up the action and improvement plan, with unit actions allocated to a bearer, a desired and jointly agreed deadline, and overall monitoring of these actions by a governance team over the long term. A cold meeting can also be organized at the end of the incident to record any additional elements or make adjustments to the observations already made during the hot phase and to the action plan.

The whole RETEX process contributes to the continuous improvement of qualification and treatment processes and actions, and closes with a new phase of preparation for the occurrence of a similar event, via the processing of the action plan and the enrichment of a knowledge base. The approach complies with numerous standards (e.g. ISO27001, ISO22301).

This RETEX can also be used for training purposes:

- Staff training in the event of a crisis, either in the form of tabletop exercises or by replaying the vulnerability in the form of crisis cell simulations.
- Technical teams in terms of case studies for skills transfer.

<GLOSSARY>

SOFTWARE: What is developed.

PROGICIELS: Ce qui est acheté à un éditeur et intégré. Le terme de «logiciel sur étagère» est parfois employé.

0-DAY: An error in a software, with a security impact (a flaw), discovered and known only to the discoverer and a limited circle of people or entities with whom he has shared it. In general, the software publisher is excluded from this circle. The term can also be used to describe vulnerabilities that are publicly known but not patched https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043228194 .

BLUE TEAM: The Blue Team includes an SOC and/or CERT .

BUG BOUNTY (VULNERABILITY PRIME): An approach that consists of setting up a reward program when a vulnerability is discovered, with or without going through an intermediary. The idea is to propose a perimeter to be evaluated (all or part of applications, services, etc.), publicly or privately, to everyone or to a selection of cybersecurity professionals, with the bounty amounts associated with the vulnerability categories (the total bounty amount must be capped, but runs the risk of stopping in progress if it is reached).

CERT (COMPUTER EMERGENCY RESPONSE TEAM) OR CSIRT (COMPUTER SECURITY INCIDENT RESPONSE TEAM): Team and coordination of response to cybersecurity incidents. Depending on the organization, the CERT may also be in charge of monitoring.

CERT-FR: French governmental center for monitoring, alert and response to computer attacks, operated by the Operations Sub-Directorate (formerly COSSI / Centre Opérationnel de la Sécurité des Systèmes d'Information) of the Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).

CESIN (CLUB DES EXPERTS DE LA SÉCURITÉ DE L'INFORMATION ET DU NUMÉRIQUE): Association promoting feedback between information security and digital professionals.

CLUSIF (CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS): public interest association bringing together information security professionals (users, CISOs and suppliers) through working groups, publications and conferences, since 1982.

CLUSIR: decentralized regional associations linked to Clusif.

CMDB (Configuration Management Database): A database containing all relevant information on an organization's IT components and the relationships between them, used primarily for IT service management.

< GLOSSARY >

CVSS (COMMON VULNERABILITY SCORING SYSTEM): Standardized system for assessing the criticality of vulnerabilities according to objective, measurable criteria.

COMEX (EXECUTIVE COMITEE): A term generally used to designate a company's executive committee, which is the group of senior executives responsible for making strategic decisions.

COORDINATED DISCLOSURE: An approach to cybersecurity where the discovery of a vulnerability is shared confidentially with the affected entity before being publicly disclosed, enabling the development and distribution of a patch.

CVE (COMMON VULNERABILITIES AND EXPOSURES): A public referencing system for known IT security vulnerabilities, offering a standardized method for identifying each unique vulnerability.

CWE (COMMON WEAKNESS ENUMERATION): A system classification and referencing system for software vulnerability types, designed to help raise awareness and prevent weaknesses in code that can lead to security vulnerabilities.

DAST (DYNAMIC APPLICATION SECURITY TESTING): Solution dynamic application security testing to detect vulnerabilities and weaknesses in the security of an application as it runs.

DENIAL OF SERVICE / DOS: Attack aimed at render a service unavailable either by exploiting a blocking vulnerability or by saturating its resources (CPU, memory, etc.)

DISTRIBUTED DENIAL OF SERVICE / DDOS: Network attack aimed at making a service unavailable by sending a large number of requests from a large number of sources, saturating either its bandwidth (volumetric attack) or its resources (application attack).

EBIOS RISK MANAGER: method for assessing and dealing with digital risks published by the Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) with the support of the EBIOS club.

FIRST (FORUM OF INCIDENT RESPONSE AND SECURITY TEAMS): An international association of incident response and security professionals, which aims to promote cooperation and coordination in the management of IT security incidents.

< GLOSSARY >

IAST (INTERACTIVE APPLICATION SECURITY TESTING): The interactive naming comes from the fact that this tool will make it possible to test the application in use during automated or human acceptance tests, or during technical interaction.

LIBRARY / SOFTWARE LIBRARY: Collection of routines, which can be already compiled and ready for use by programs.

LOCAL CODE EXECUTION: Attack to inject arbitrary, uncontrolled code into a vulnerable system by connecting to it locally.

LOCAL PRIVILEGE ESCALATION: Attack enabling you to locally elevate your privileges on a vulnerable system, in order to perform actions that would not normally be authorized.

LOI DE PROGRAMMATION MILITAIRE / MILITARY PROGRAMMING ACT (LPM): French law which sets the guidelines and financial resources allocated to defence over a multi-year period.

CONTEXTUAL MENU: List of commands or options appearing on the screen when the user clicks with the right mouse button or presses a contextual menu button. It may vary according to the user's location, the program being used or other variables.

NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY): U.S. government agency responsible for the development and promotion of advanced standards and technologies in many fields, including cybersecurity.

NVD (NATIONAL VULNERABILITY DATABASE): Database managed by NIST, which provides detailed information on known security vulnerabilities in IT.

OSSIR (OBSERVATORY OF SYSTEMS AND NETWORKS SECURITY): Association bringing together information security professionals around monthly workshops with two technical presentations and a review of security news including vulnerabilities. All presentations are publicly available at https://www.youtube.com/c/ossirFrance

RSSI / CISO (CHIEF INFORMATION SECURITY OFFICER): Key position in companies and organizations that need to protect their information systems and sensitive data against internal and external threats.

SAST (STATIC APPLICATION SECURITY TESTING): Tool for static application security testing enables developers to look directly for potential vulnerabilities in application source code as early as possible in the software development lifecycle.

< GLOSSARY >

SCA (SOFTWARE COMPONENT ANALYSIS): Tool for checking the composition of an application in terms of third-party dependencies and licenses. Since applications generally embed frameworks, open-source or proprietary libraries, etc., it is necessary to check that the resulting artifact does not embed components known to be vulnerable or obsolete, and that there are no license compatibility defects.

SBOM (SOFTWARE BILL OF MATERIALS): List of software components found in a particular system. This list is essential for understanding potential vulnerabilities and cybersecurity risks.

SHADOW IT: The use of software, devices or services outside the company's official control and governance, often driven by convenience or cost concerns.

RED TEAM: People authorized and organized to simulate the attack or exploitation capabilities of a potential adversary against a company's security posture. The aim of the Red Team is to improve the company's cybersecurity according to predefined scenarios.

REMOTE CODE EXECUTION: Attack used to inject arbitrary code remotely into a vulnerable system (via the local network or the Internet) and take control of it.

RPO (RECOVERY POINT OBJECTIVE): According to ISO 22301, the RPO is defined as the target duration of the period during which data may be lost as a result of an incident or disruption.

SOC (SECURITY OPERATION CENTER): Human and technical resources responsible for continuously monitoring and analyzing a company's security system, and responding to alerts. Depending on the organization, the response to a security incident may be handled by the CERT or the SOC.

VDP VULNERABILITY DISCLOSURE POLICY: The internal framework consists of defining a Vulnerability Disclosure Policy (VDP). A VDP is an organization set upto enable the legal collection of vulnerabilities reported by sources outside the company, in complete security.

VOC (VULNERABILITY OPERATION CENTER): set of human and technical resources responsible for monitoring and managing the treatment of technical vulnerabilities. Note that this term is a French invention and does not exist in the English-speaking world, which prefers «vulnerability management»*.

ZERO DAY / 0-DAY: This term refers to a security vulnerability in software or an information system that is exploitable by hackers before vendors or developers have been able to create and release a patch.

< REFERENCES >

Crisis management guide published by ANSSI: https://www.ssi.gouv.fr/guide/crise-dorigine-cyber-les-cles-dune-gestion-operationnelle-et-strategique/

RM EBIOS risk analysis methodology guide: https://www.ssi.gouv.fr/uploads/2018/10/guide-methode-ebios-risk-manager.pdf

< Studio des Communs >

CAMPUS CYBER

MORE INFORMATION: WIKI.CAMPUSCYBER.FR
CONTACT: COMMUNAUTES@CAMPUSCYBER.FR / 5 - 7 RUE BELLINI 92800, PUTEAUX