Operational Guidance For Incident Handling

ANSSI, CSSF, CIRCL, GOVCERT, HCPN, ILR

2026-09-28

Contents

Operational guidance for incident handling

Traffic Light Protocol (TLP): CLEAR

Version: 1.0 (stable)

Date: 28 September 2026

Authors:

- Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)
- Commission de Surveillance du Secteur Financier (CSSF)
- Computer Incident Response Center Luxembourg (CIRCL)
- Governmental Computer Security Incident Response Team (GovCERT)
- High Commission for National Protection (HCPN)
- Institut Luxembourgeois de Régulation (ILR)

Disclaimer

These rulebooks are solely intended to be used as a practical guidance by an entity facing a cybersecurity incident and looking for immediate assistance from the competent authorities and the Computer Security Incident Response Teams (“CSIRT”). They have been written by a joint team of experts of the *High Commission for National Protection* (“HCPN”), acting in its role as the *Agence Nationale de la Sécurité des Systèmes d’Information* (“ANSSI”) and as *the Governmental Computer Security Incident Response Team* (“GOVCERT.LU”), the *Computer Incident Response Center Luxembourg* (“CIRCL”), the *Commission de Surveillance du Secteur Financier* (“CSSF”), and of the *Institut Luxembourgeois de Régulation* (“ILR”), in the context of 14(5) of the *Loi du 5 mai 2026 concernant des mesures destinées à assurer un niveau élevé de cybersécurité* (“NIS2 Law”), and in accordance with the missions assigned to the HCPN in its role as ANSSI under Article 3, paragraph 1*ter*, of the *Loi modifiée du 23 juillet 2016 portant création du Haut-Commissariat à la Protection nationale*.

These rulebooks must not be used as a substitute for any policies or procedures in force at the entities. Neither the HCPN, the CIRCL, the CSSF, nor the ILR can be held liable in the event of malfunction or unforeseen circumstances or for any damages resulting from the use of the guidance.

These rulebooks do not address the legal obligations to be fulfilled by the concerned entities (e.g., file a complaint, notification of incidents to the CSSF, the ILR, and the Commission Nationale pour la Protection des Données (CNPD), etc.).

Rulebook 0 – Triage & Routing

Context and objectives

This “rulebook 0” is intended to be used as a starting point for the entities suffering a cyber-security incident and looking for assistance.

The objectives of this “rulebook 0” are the following:

- Stabilize operations, safely collect key evidence, support forensic analysis, and route to appropriate playbooks.
- Tick mandatory regulatory reporting clocks immediately (NIS2, DORA, sectoral rules as applicable).
- Enable support for malicious cyber-attacks (human errors and system failures are out of scope of these rulebooks).

The subsequent rulebooks, #1 to #8, follow a common chronological flow of steps that are traditionally used in incident resolution:

- **Typical initial detection**: the observed artefacts that are relevant triggers for the specific rulebook (note that they are indicatives but not exhaustive, not all the artefacts must be encountered to launch a specific rulebook, and several rulebooks may be applicable to an individual incident).
- **Immediate response (containment)**: useful techniques to consider immediately, to prevent contagion and greater damage.
- **Investigation steps**: useful techniques to further investigate the incident, enabling to look for deeper infection and spot malicious artefacts.
- **Remediation**: useful techniques to move away from the incident situation and consider the entity to be back in a safe state.
- **Evidence keeping**: useful techniques to keep evidences for forensics analysis.
- **Post-incident activity**: useful points to consider when going through the “lessons learnt” process and seek for potential improvement.
- **Communication**: useful communication consideration, such as specific services to contact.
- **Key watchpoints**: useful tips to consider when handling the incident, especially for more sophisticated attacks.

For reference, a traditional and complete framework for incident management is often represented in a cycle of 4 phases:

- Preparation,
- Detection and Analysis
- Containment, Eradication and Recovery
- Post Incident Activity

This set of rulebooks only covers parts of this cycle, addressing generic but still practical operational guidance.

First actions

Assign roles

- Name the responsible people to be involved. For example: a leader, a secretary (for meeting minutes and evidence keeping), analysts and communicator.
- Communication / reporting roles for timely and appropriate communication. This function is to be segregated from incident resolution teams (IT, security).
- If a crisis situation is declared, create a secure war-room (physical or virtual). Track participation and decisions. Also, consider engaging the Business Continuity Management (BCM) lead immediately to assess potential business-critical impact.

Look at the first indicators

- Use monitoring and logs to narrow the attack surface.
- Classify: is the event likely human error, malicious, or uncertain?
- Identify impacted assets, systems, users, and third parties.

Staff wellbeing

- Ensure teams are rotated for sustained incidents. Encourage breaks and provide psychological support as needed.
- Keep clear, calm, factual communication to limit stress.

Open a case log & chain of custody

- Use incident management software if available or standardized template.
- For every artifact: log who / what / when / how, compute hash (SHA-256), store originals read-only.
- Secure all captured evidence in a dedicated, access-controlled repository.
- Carefully consider that the entity's infrastructure may be compromised and the reliance on out-of-band communication and storage may be a necessity.

Fast classification to route to the proper rulebook(s)

- Keep as much evidence as possible.
- Onboard experts to assist you, either internally or externally: cyber experts, consultants, and legal counsel, as needed.

- Keep track of all investigative hypotheses and keep them updated over time.
- Frequently (re)assess the attack classification based on the information you collect over time, to ensure the invocation of the most relevant rulebook(s).
- Based on the collected indicators, use the classification table below and invoke the most relevant rulebook(s):

Note: The lists of indicators are non-exhaustive.

Rulebook 1 - DoS & DDoS

Indicators of compromise	Description
• Sudden or sustained service unavailability or severe latency reported by users or monitoring tools • Saturated network traffic and connection timeouts • Anomalies in network traffic, occurring at unusual pace (e.g., handshake failures, SYN/ACK reset or malformed packages, Web Application Firewall (WAF) origin timeouts, spikes in 4xx/5xx errors) • Outstanding alerts from firewall, load balancer, or Internet Service Provider (ISP) • Sudden drop in availability of external-facing services (Domain Name System (DNS), Virtual Private Network (VPN), email, web portals) • Abnormal load on backend components (e.g., web servers or database servers), such as increased Central Processing Unit (CPU) consumption	This rulebook covers all the kinds of DoS or DDoS attacks: including overflow or crash attacks, at either the network or application layers.

Rulebook 2 – Malware

Indicators of compromise	Description
• Unusual file extensions (`.locked`, `.crypt`, etc.) • Unintended file renaming observed • Antivirus (AV) or Endpoint Detection and Response (EDR) alerts • Suspicious process execution • Outbound connections or beaconing activity to suspicious or known Command & Control (C2) • Persistence artifacts (services, tasks, Windows Management Instrumentation (WMI)) • Sudden inaccessibility of files or performance issues observed • Ransom note discovered in end-user directories or shared drives • Abnormal pop-ups or locked screens observed by users	This rulebook applies to all kinds of malware, used for a variety of purposes, such as: • Data theft and surveillance: infostealers, spyware, keyloggers, etc. • Remote access and control: remote access trojans (RAT), backdoors, rootkits, abuse of RMM tools, etc. • Destruction and extortion: ransomware, wipers, etc. • Propagation and distribution: viruses, worms, trojans, botnets, etc. • Resource exploitation: crypto miners, adware, logic bombs, etc.

Rulebook 3 - Exploitation of communication channels to gain access

Indicators of compromise	Description
• User reports a suspicious email or link • User reports a suspicious SMS • Anomalous email activity (auto-forwarding, mass mails) • Alerts of credentials being re-used • Reports from other entities, third parties, Computer Emergency Response Teams (CERTs), or Threat Intelligence feeds indicating an ongoing campaign targeting similar entities • Detection from an email gateway or Security Information and Event Management (SIEM) showing indicators of exploitation of communication channels • Reported fake websites or login portals imitating the entity's own websites or login portals	This rulebook applies to all kinds of successful exploitation of communication channels, for instance: phishing, smishing (SMS phishing), vishing (voice phishing), quishing (QR code phishing), pretexting (e.g., CEO fraud), Business Email Compromise (BEC), etc.

Rulebook 4 - Credential theft & account compromise

Indicators of compromise	Description
• Unusual login activity (geographic anomalies, impossible travel, unusual token usage) • Unintended bypass of Multi-Factor Authentication (MFA) • Privilege escalation alerts • Unusual activities detected on mailboxes or cloud services, such as outstanding downloads, unintended permission changes, creation of new rules or delegates, or multiple failed logins or brute-force detections • Alerts from other entities, Computer Emergency Response Teams (CERTs), or Threat Intelligence Feeds identifying compromised accounts in the entity's domains • Suspicious OAuth or Application Programming Interfaces (API) token usage, in particular outside the corporate IP range	This rulebook applies to all types of theft of credentials or compromise of accounts, including for instance: session hijacking, pass-the-hash attack, pass-the-ticket attack, brute forcing, password spraying, Kerberoasting, credential dumping (LSASS), etc.

Rulebook 5 - Vulnerability exploitation

Indicators of compromise	Description
• Unusual behaviour of systems or applications (e.g., errors, crashes, defacement) • Unusual Application Programming Interface (API) calls or access to data • Unusual number of Web Application Firewall (WAF) or Security Information and Event Management (SIEM) alerts (e.g., spikes in 4xx/5xx error messages) • Reverse or web shells observed or suspected to be in use • Abnormal page volumetry (rendered page size / requests per IP) • Abnormal behaviour in logs (e.g., access logs)	This rulebook applies to all kinds of vulnerabilities: web application vulnerabilities, API exploitation, known exploited vulnerabilities (KEV), configuration-flaw exploitation, memory and binary exploitation, etc.

Rulebook 6 - Insider threat

Indicators of compromise	Description
• Unusual access to sensitive data • Unusual large outbound traffic • Unusual traffic outside working hours • Complaints or warnings from the Human Resources (HR) department • Unauthorized use of administrative tools or privilege-escalation attempts	This rulebook applies to situations where an insider (e.g., employee or consultant), having genuine access to the entity's systems, leverages that granted access to perform malicious actions.

Rulebook 7 - Data exfiltration

Indicators of compromise	Description
• Unusual access to sensitive data • Unusual large outbound traffic • Unusual traffic outside working hours • Suspicious (obfuscated) outbound traffic • Alert from Endpoint Detection and Response (EDR) or threat intelligence resources • Sudden large file transfers • Long dwell time • Data Loss Prevention (DLP) or proxy alerts indicating sensitive-data movement outside approved channels • Data discovered outside traditional channels (e.g., Telegram, web forums, press, or other media)	This rulebook applies to situations where an entity’s data is exfiltrated without authorization.

Rulebook 8 - Package compromission & supply chain attack

Indicators of compromise	Description
• Unusual alerts following a software or firmware update, or the integration of a new third-party package • Failures in hash validation or use of unexpected certificates used to sign packages • Outbound traffic to abnormal domains • Endpoint Detection and Response (EDR) alerts on newly updated binaries, installers or side-loaded Dynamic-Link Libraries (DLLs) • Permission abuse of an application or integration (e.g., observed via unexpected OAuth / Single Sign On (SSO) consent or expanded scopes) • Unusual requests originating from third-party services (e.g., API calls to unusual domains) • Software behaviour not in line with the intended design (i.e., Software Bill of Materials (SBOM) drift)	This rulebook applies to situations where an attack leverages third-party dependencies (e.g., software packages, libraries, open-source code, firmware, etc.) to compromise the entity's systems.

General guidance and watch points

- Maintain timeline of actions (detection → response → containment → recovery).
- Record all decisions and rationales.
- Confirm that backup data is intact and isolated before any restoration.
- Consider engaging external CSIRT/CERT or cyber-insurance provider early if contractual clauses exist.
- After triage, continue reassessment: re-classify the incident as new evidence emerges.
- Keep all internal and external communications factual, short, and go through legal review if needed.
- After the incident is resolved and as part of the post-incident improvement, update your internal procedures, considering the lessons learnt.
- Consider using external tools and procedures[1] for the proper incident handling and evidence collection.

[1] Example: the CIRCL Standard Operational Procedures (SOP), available here: https://circl.lu/pub/tr-39

Rulebook 1 – Denial of Service (DoS) & Distributed Denial of Service (DDoS)

This rulebook covers all the kinds of DoS or DDoS attacks: including overflow or crash attacks, at either the network or application layers.

Typical initial detection

- Sudden or sustained service unavailability or severe latency reported by users or monitoring tools
- Saturated network traffic and connection timeouts
- Anomalies in network traffic, occurring at unusual pace (e.g., handshake failures, SYN/ACK reset or malformed packages, Web Application Firewall (WAF) origin timeouts, spikes in 4xx/5xx errors)
- Outstanding alerts from firewall, load balancer, or Internet Service Provider (ISP)
- Sudden drop in availability of external-facing services (Domain Name System (DNS), Virtual Private Network (VPN), email, web portals)
- Abnormal load on backend components (e.g., web servers or database servers), such as increased Central Processing Unit (CPU) consumption

Immediate response (containment)

- Immediately notify the Business Continuity Management (BCM) function and affected business owners
- Identify the type of attack (i.e., volumetric or non-volumetric)
- Contact the Internet Service Provider(s) (ISP) to turn on traffic filtering. If volumetric attack is already suspected, turn on anti-DDoS services that you subscribed (if any)
- If identification is already done, block (or at least implement rate limits) attacking IP ranges, or geo-block
- Mitigate impact on backend systems and critical services e.g., using for instance connection limits (“connections caps”), lower timeouts, or isolating affected systems
- Divert traffic via Content Delivery Network (CDN) if available
- Activate the crisis communication line if customer-facing portals are affected

Investigation steps

- Perform traffic analysis to determine the origin (geographic[2] and logical) and nature of the traffic, collect indicators of compromise (IOCs), such as network packet captures (PCAP), edge logs, and patterns (e.g., User-Agent, URI, source ASNs)

[2] Keep in mind limitations during reflective attacks

- Assess whether the attack is a distraction or part of a multi-vector campaign
- Check if camouflage / obfuscation / data exfiltration techniques are employed at the same time of the attack; if yes, invoke other rulebooks as appropriate
- Identify the business assets that are affected and the bottleneck devices

Remediation

- Review web application firewall (WAF) configurations to mitigate protocol-based attacks, if relevant
- Evaluate the business impact for any countermeasures proposed in response to the incident
- Consider blocking based on geography, deny-lists or IP reputation lists
- Consider blocking high-impact IPs and applying rate limits
- Consider implementing challenge-response mechanisms (e.g., CAPTCHA)
- Consider applying temporary cache rules
- Check if backend services are affected by overload and take action as appropriate
- Consider closely monitoring signs of network disruption to catch changes in the attack techniques (e.g., via Quality of Services (QoS) measures)
- Once stable, gradually remove temporary blocks to validate that the service recovery is effective

Evidence keeping

- NetFlow captures (e.g., short PCAP samples)
- Logs from application servers, firewall, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Content Delivery Network (CDN), load-balancer and WAF
- Maintain timeline and decisions in the incident case log

Post-incident activity

- Identify and patch services that are prone to be leveraged during DDoS attacks (e.g., DNS, Network Time Protocol (NTP) or other amplification vulnerabilities)
- Review your IT architecture to look for resiliency improvement opportunities
- Consider deploying CDN with Anycast routing and caching capabilities, load balancers, multi-region redundancy, and separation of critical and non-critical services
- Perform dependency mapping by identifying all public-facing services (web, Application Programming Interfaces (APIs)), entry points (public IPs and ports), as well as associated CDN, DNS, and authentication mechanisms

- Review alert thresholds and monitoring dashboards for early detection
- Consider subscribing to anti-DDoS services
- If your external communication means were impacted, look for alternate solutions
- Consider including DDoS attacks in your Business Continuity Plan (BCP) / Disaster Recovery Plan (DRP)

Communication

- Coordinate with ISP / hosting provider
- Inform customers and business partners

Key watchpoints

- Application-layer DoS may evade traditional detection mechanisms and volumetric defences may not be reliable
- Attacks may occur on multiple layers (L3/L4 + L7) simultaneously
- Techniques used by attackers shift rapidly and adapt to the defence responses (cat and mouse game)
- Similar campaigns may reappear within days; keep monitoring heightened for a defined period
- Confirm no persistent compromise remains once traffic stabilizes (e.g., injected web shell, backdoor)

Rulebook 2 – Malware

This rulebook applies to all kinds of malware, used for a variety of purposes, such as:

- Data theft and surveillance: infostealers, spyware, keyloggers, etc.
- Remote access and control: remote access trojans (RAT), backdoors, rootkits, abuses RMM tools, etc.
- Destruction and extortion: ransomware, wipers, etc.
- Propagation and distribution: viruses, worms, trojans, botnets, etc.
- Resource exploitation: crypto miners, adware, logic bombs, etc.

Typical initial detection

- Unusual file extensions (.locked, .crypt, etc.)
- Unintended files renaming observed
- Antivirus (AV) or Endpoint Detection and Response (EDR) alerts
- Suspicious process execution
- Outbound connections or beaconing activity to suspicious or known Command & Control (C2)
- Persistence artifacts (services, tasks, Windows Management Instrumentation (WMI))
- Sudden inaccessibility of files or performance issues observed
- Ransom note discovered in end-user directories or shared drives
- Abnormal pop-ups or locked screens observed by users

Immediate response (containment)

- Decide on the strategy based on the malware impact: either keep the system running or power off; knowing that keeping power on preserves memory for forensic analysis and **may** enable the extraction of the encryption key (in case of ransomware), while powering off **may** limit the immediate damage and **may** avoid propagation
- Isolate affected systems from the network immediately (e.g., disconnect network cables, disable Wi-Fi, isolate at switch / Network Access Control (NAC) / hypervisor level)
- In case a ransomware has already impacted the availability of infected systems, notify the Business Continuity Management (BCM) function for potential business impact
- Block suspected domains and IPs
- Change credentials used on infected devices and monitor accounts
- Disable administrative shares and remote access (e.g., Server Message Block (SMB), Remote Desktop Protocol (RDP)) to limit lateral movement

- Prevent spread by disabling scheduled tasks and tools usually used in lateral movement (e.g., PsExec)
- If ransomware is suspected, disconnect backup systems from the network immediately and temporarily suspend automated backups to prevent encryption spread or tampering
- Check integrity of offline copies

Investigation steps

- Create forensic copies for analysis: at first acquire key artifacts by relying on the EDR if available, and perform full disk acquisition (e.g., using "dd" tool) on critical workstations (entry point, domain controllers, attacker pivot)
- Identify initial point of infection (e.g., specific end-user laptop) and initial vector (e.g., phishing, RDP access, exploited vulnerability, etc.)
- In case of ransomware, determine encryption scope, identify ransomware strain (to check for decryptors) and persistence artifacts[3]
- In case of ransomware, investigate the firewall logs to determine potential data exfiltration
- Review logs for lateral movement, privilege escalation or indicators of persistence
- Use threat-intelligence sources to look for known indicators (e.g., hashes, domains)
- Assess if other rulebooks apply (e.g., *Rulebook 3 – Phishing* for initial infection, or *Rulebook 7 – Data Exfiltration* if leaks suspected)

Remediation

- Entities should not pay the ransom (if any is requested) — it does not guarantee recovery and may breach sanctions law
- Before restoring, apply latest patches / updates and perform Antivirus (AV) and Endpoint Detection and Response (EDR) scan
- Restore infected systems from trusted sources (e.g., clean backups or gold images), and keep them disconnected from the network at first and check file integrity
- Invalidate tokens cached on infected hosts
- Although restoration is often the preferred option, it may not be always possible; in this situation, remove artifacts or tools (e.g., registry keys, tasks) used for persistence purpose
- Re-enable network connectivity gradually, while monitoring for indicators of re-infection
- Verify proper operation of restored systems before reintroducing them to production

[3] External tools may assist in this task, such as: https://pandora.circl.lu

Evidence keeping

- Keep ransom note, a sample of encrypted files and a sample of the malware
- Before wiping any system, create disk images
- Collect logs (Windows Event Viewer, Sysmon, EDR, network captures), use automation for collection where possible
- Collect volatile data (e.g., memory dumps) from infected machines before power-down (if feasible)
- Document timeline of actions, decisions, and containment steps in the case log

Post-incident activity

- Patch vulnerabilities and entry vectors used in the attack
- Reset credentials (especially admin accounts)
- Consider using “tiered credential rotation”
- Consider reviewing the Group Policy Objects (GPOs) to harden endpoints
- Consider reviewing the configuration of remote management tools (e.g., RDP) and look for potential security improvements
- Consider enabling Multi-Factor Authentication (MFA) for all administrator and remote access
- Consider reviewing endpoint security posture and look for security improvements
- Consider segmenting the internal network
- Consider improving the employees’ awareness
- Consider deploying application whitelisting and EDR behavioural rules

Communication

- Alert IT and Security Operations Centre (SOC) teams immediately
- Inform affected users if their accounts were involved

Key watchpoints

- Beware of double extortion attacks (i.e., data theft and encryption)
- Malware may act as dropper only, pre-positioning attackers for future malicious acts, so watch for dormant second-stage payloads (e.g., triggered scheduled tasks) or abnormal network traffic or system behaviour
- Before recovery steps, validate all recovery sources as infections may re-trigger from persistent devices or offline backups

- Cloud storage or synchronization services can re-propagate infected content if not sanitized
- For ransomware attacks, consider referring to additional specialized guidance[4]

[4] Example: the CIRCL ransomware FAQ available here: https://circl.lu/pub/tr-73/

Rulebook 3 – Exploitation of communication channels to gain access

This rulebook applies to all kinds of successful exploitation of communication channels, for instance: phishing, smishing (SMS phishing), vishing (voice phishing), quishing (QR code phishing), pretexting (e.g., CEO fraud), Business Email Compromise (BEC), etc.

Typical initial detection

- User reports suspicious email or link
- User reports suspicious SMS
- Anomalous email activity (auto-forwarding, mass mails)
- Alerts of credentials being re-used
- Reports from other entities, third-parties, Computer Emergency Response Teams (CERTs) or Threat Intelligence feeds indicating an ongoing campaign targeting similar entities
- Detection from email gateway or Security Information and Event Management (SIEM) showing exploitation of communication channels indicators
- Reported fake websites or login portals imitating the entity's own websites or login portals

Immediate response (containment)

- Identify malicious domains and URLs and block them in proxy, email gateways and spam filters
- Purge the email from all user mailboxes via administrative search-and-remove
- Reset credentials of impacted user and invalidate active sessions (e.g., OAuth tokens, browser sessions)
- Check for unintended auto-forwarding rules and remove them
- Check endpoints of affected users for malware or credential stealers (run an Endpoint Detection and Response (EDR) scan)
- If internal domains are spoofed, consider blocking the delivery from external sources using these spoofed internal domains
- Keep evidence (e.g., copy of original emails and headers) before deletion
- If multiple users reported identical messages, consider that a large-scale campaign is ongoing and notify the Security Operations Centre (SOC) and the Management

Investigation steps

- Due to volume, investigations may not always be performed duly; keep processes simple and prioritised
- Analyse the email headers to check sender authenticity, the message's path and any trace of anomalies
- **Don't** click on the payloads or URLs, however inspect them in a safe sandboxed environment to determine the malicious intent (e.g., credential harvesting, malware delivery, scam, OAuth token abuse).
- Identify the users' interactions (e.g., click, download, open) and the related impacts
- Correlate Indicators of Compromise (IoCs) (e.g., IP, domain, hash, email subject) with other alerts and external sources (e.g., Threat Intelligence feeds, warning from CERTs)
- Examine the phishing page[5] to identify all involved parties, such as an initial redirector, or credentials posted to another website
- Collect any artifacts you can fetch (e.g., phishing kit, Telegram ID/key, etc.)

Remediation

- Check with external sources (e.g., Threat Intelligence feeds, warning from CERTs) if other similar phishing kits or campaigns are on-going and block them
- Ensure that your email security settings (i.e., Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), Domain-based Message Authentication, Reporting & Conformance (DMARC)) are in line with leading security practices
- Reset or rotate credentials and tokens for all confirmed victims
- Monitor post-incident activity on affected accounts for at least 72 hours, in particular check in logs if malicious downloads, macros or fileless payloads are executed

Evidence keeping

- Keep the original malicious communication, including the headers
- Collect mail server logs and user mailbox export
- Screenshots of phishing pages6, if safely captured in a sandbox

[5] External tools may assist in this task, such as: https://lookyloo.circl.lu/

Post-incident activity

- Consider improving the user awareness on social engineering communication focusing on recognizing suspicious messages and reporting procedures
- Strengthen email gateway rules, condition access/ Multi-Factor Authentication (MFA), OAuth and third-party app approval flows and sandboxing
- Consider conducting a phishing campaign exercise for training evaluation
- If a proxy is deployed, verify that SSL/TLS termination is enabled and that request methods are properly logged (the ability to identify “POST” requests is particularly valuable)
- Evaluate the SPF configuration

Communication

- Notify impacted users promptly, explaining the steps they must take (password reset, token revocation, vigilance)
- Escalate to Top Management if multiple users are targeted
- Consider making a communication to all employees about an on-going deceptive/malicious communication campaign

Key watchpoints

- Beware of phishing attempts looking to gather OAuth tokens, these may be used to bypass password resets
- Attackers may collect compromise access now, and reuse later
- Mobile users are increasingly targeted via SMS (i.e., smishing) or messaging applications (i.e., vishing)

Rulebook 4 – Credential theft & account compromise

This rulebook applies to all the types of theft of credentials or compromise of accounts, including for instance: session hijacking, pass-the-hash attack, pass-the-ticket attack, brute forcing, password spraying, Kerberoasting, credential dumping (LSASS), etc.

Typical initial detection

- Unusual login activity (geographic anomalies, impossible travel, unusual token usage)
- Unintended bypass of Multi-Factor Authentication (MFA)
- Privilege escalation alerts
- Unusual activities detected on mailboxes or cloud services, such as outstanding downloads, unintended permission changes, creation of new rules/delegates, or multiple failed logins or brute-force detections
- Alerts from other entities, Computer Emergency Response Teams (CERTs) or Threat Intelligence Feeds of identified compromised accounts in the entity's domains
- Suspicious OAuth or Application Programming Interfaces (API) token usage, in particular outside of the corporate IP range

Immediate response (containment)

- Force logoff and password reset of compromised accounts
- Terminate compromised sessions and revoke associated tokens
- Notify the Security Operations Centre (SOC) and the Identity and Access Management (IAM) team to monitor for potential reuse or reauthentication attempts, used in password spraying attacks

Investigation steps

- Identify entry vector (e.g., phishing, brute-force, token theft)
- Review access logs
- If MFA was by-passed, understand how (e.g., application-based attack or phishing relay) and determine whether the first rogue IP that logged in was also a phishing website
- Check for lateral movements and privilege escalation
- Check for persistence mechanisms, such as new MFA devices, new application accounts or passwords, tokens with long expiration date, unintended delegated mailbox access
- Review logs of Endpoint Detection and Response (EDR) and affected components for credential dumping tools

- Look for potential privilege-escalation events or newly created accounts
- Look for unintended OAuth consents and API tokens, to detect potential unauthorized application integrations
- Look for malicious mail rules

Remediation

- Consider the scale of the impact and resetting passwords, API keys and tokens as appropriate
- Consider implementing conditional access (e.g., MFA, geo-fencing), in particular for sensitive, administrator and remote access
- Review the roles in the identity directory (e.g., Active Directory (AD)) and remove unauthorized privileges
- Apply patches on affected components and/or apply mitigation measures to avoid new capture of credentials or tokens
- Implement detection rules to detect ongoing or renewed attacker activity — such as repeated login attempts or the creation of new unauthorized sessions — even after credentials are changed
- Primarily for cloud hosted email platforms, remove malicious application permissions and clean up mail forwarding/filtering rules

Evidence keeping

- Authentication logs (e.g., Active Directory (AD), Identity Provider (IdP), Virtual Private Network (VPN))
- Endpoint Detection and Response (EDR) logs

Post-incident activity

- Consider hardening the password policy and enforcing MFA at large scale
- Review the use of service accounts and Application Programming Interface (API) keys, and look for security improvement opportunities
- Review and look for improvements in Identity and Access Management (IAM) policies and permissions
- Consider raising awareness among users about phishing and credentials hygiene
- Consider implementing detection use cases based on behavioural analytics and automated risk-based conditional access

Communication

- Notify impacted users promptly and advise them to verify their other accounts for reuse risks
- Inform Security Operations Centre (SOC) and IT
- Inform Management and legal / compliance departments if sensitive data was accessed, altered or exfiltrated

Key watchpoints

- Token-based attacks may not be impacted by password reset attempts
- Attackers often use automation for persistence (e.g., scheduled tasks)

Rulebook 5 – Vulnerability exploitation

This rulebook applies to all kinds of vulnerabilities: web application vulnerabilities, API exploitation, known exploited vulnerabilities (KEV), configuration flaws exploitation, memory and binary exploitation, etc.

Typical initial detection

- Unusual behaviour of systems or applications (e.g., error, crashes, defacement)
- Unusual Application Programming Interface (API) calls or access to data
- Unusual number of Web Application Firewall (WAF) or Security Information and Event Management (SIEM) alerts (e.g., spikes in 4xx/5xx error messages)
- Reverse or web shells were observed or suspected to be used
- Abnormal page volumetry (rendered page size / requests per IP)
- Abnormal behaviour in logs (e.g., access logs)

Immediate response (containment)

- Isolate affected systems or applications
- Identify the vulnerable path and kill-switch it
- Consider disabling exposed API endpoints
- Consider deploying or updating blocking WAF rules based on observed attack patterns
- Notify the Business Continuity Management (BCM) function if critical systems or applications are affected
- Keep logs and snapshots before patching or rebooting systems
- Monitor for lateral movement from the web hosting systems to internal networks

Investigation steps

- To identify the exploited vulnerability, review web, API and systems access / error logs and reverse-proxy logs
- Check if the vulnerability was introduced by a recent change, by checking the source code (e.g., use "*diff*" command between recent deploys)
- Look for web shells (e.g., unusual server-side scripts (PHP, Python, Ruby, Node.js, ASP.NET (or other) files))
- Inspect active network connections and running processes for signs of unauthorized outbound traffic or reverse shells

- Check files integrity by comparing hashes with baseline (if available), and verify timestamps for unexpected modifications
- Look for traces of persistence, such as new or modified scheduled tasks, system services or startup scripts
- If possible, perform a memory analysis to detect fileless malware or injected code that does not exist on disk
- Determine whether attackers accessed, altered or exfiltrated (sensitive) data (invoke Rulebook 7 – Data Exfiltration if suspected)

Remediation

- Patch vulnerable components or, if not possible, consider disabling
- Rotate secrets / credentials (e.g., tokens, API keys, database credentials)
- Remove shells and implants
- After cleaning steps, consider rebuilding the entire stack where the compromised application is hosted
- Conduct a full vulnerability scan and validate remediation of exploited paths
- Re-enable services progressively, under close monitoring

Evidence keeping

- Full HTTP logs, access / error logs and WAF alerts
- System and application layers logs (if any)
- Keep images of the stack where the application is hosted (e.g., container, virtual machine)
- "*diffs*" of the system hosting the compromised application

Post-incident activity

- Consider hardening the deployment pipeline and ensuring security review / security testing is part of the development lifecycle
- Consider improving (or at the very least enabling) API authentication and rate-limits
- Consider performing a full code review if custom development
- Consider improving access and input validation controls
- Consider implementing Server-Side Request Forgery (SSRF) and deserialization guards
- Consider conducting improving the security review practice, such as regular penetration testing, vulnerability scans and source code reviews

Communication

- Alert the development team and/or infrastructure team accordingly to the attack vector
- Notify business owners of any application downtime or user impact
- Inform Management and legal / compliance departments if sensitive data was accessed, altered or exfiltrated

Key watchpoints

- Exploits often lead to data theft: assume exfiltration until disproven
- Attacks may exploit business logic flaws, not just technical bugs

Rulebook 6 – Insider threat

This rulebook applies to situations where an insider (e.g., employee, consultant), having genuine access to the entity's systems, leverage the granted access to perform malicious actions.

Typical initial detection

- Unusual access to sensitive data
- Unusual large outbound traffic
- Unusual traffic outside working hours
- Complaints or warnings from Human Resources (HR) department
- Unauthorized use of administrative tools or privilege escalation attempts

Immediate response (containment)

- Restrict user access thanks to need-to-know and least-privilege principles
- Monitor ongoing activities, using approved tools and procedures, in respect of applicable laws and internal policies
- Notify HR, legal, and third-party if affected
- Suspend access (at least temporarily), if risk of data theft or sabotage is suspected

Investigation steps

- Collect access history, behavioural anomalies and recent changes in permissions or roles
- Keep evidence, in respect of applicable laws and internal policies, for further (forensics) analysis
- Use secure communication channels for inquiries with involved stakeholders
- Perform intent analysis (e.g., looking at disciplinary sanctions, internal business changes, departures, etc.) and leverage threat intelligence

Remediation

- Suspend or, at least, limit access if threat is confirmed
- Use psychological support in case of internal conflict or distress
- Change shared passwords and rotate Application Programming Interfaces (API) keys that the insider could have accessed

Evidence keeping

- Collect end-user computer logs (e.g., email activity, file access), in respect of the Law
- Communication with HR, legal, or management about the case
- Role history within the entity
- Maintain strict access control to investigative data (“need-to-know” principle)

Post-incident activity

- Consider enhanced background screening procedures
- Consider implementing user behaviour analytics (UBA)
- Consider reviewing the Data Loss Prevention (DLP) policy and related measures
- Consider enforcing stronger segmentation, based on need-to-know and least-privilege principles, and role-based access

Communication

- Continuously communicate with legal, compliance, HR, and management
- Limit information sharing to those strictly required (“need to know” principle) to protect confidentiality

Key watchpoints

- Do not confuse malicious acts with negligence
- Personal motives are common

Rulebook 7 – Data exfiltration

This rulebook applies to situations where entity's data is exfiltrated, without authorization.

Typical initial detection

- Unusual access to sensitive data
- Unusual large outbound traffic
- Unusual traffic outside working hours
- Suspicious (obfuscated) outbound traffic
- Alert from Endpoint Detection and Response (EDR) or threat intelligence resources
- Sudden large file transfers
- Long dwell
- Data Loss Prevention (DLP) or proxy alerts indicating sensitive data movement outside of approved channels
- Data discovered outside traditional channels (e.g., Telegram, web forums, press, or other media)

Immediate response (containment)

- Decide on the strategy based on the sensitivity and leakage impact: either block or monitor
- Monitor or isolate suspected compromised systems, ensuring forensic integrity is preserved
- Limit or block suspected exfiltration channels (e.g., Secure File Transfer Protocol (SFTP) or Hypertext Transfer Protocol Secure (HTTPS) to unusual Autonomous System Numbers (ASNs) or cloud platform)
- Disable remote access (e.g., Virtual Private Network (VPN), Secure Shell (SSH)) on suspect compromised accounts and machines
- Monitor for Command and Control (C2) traffic
- Perform full disk acquisition (e.g., using "dd" tool)

Investigation steps

- Check for persistence traces (e.g., scheduled tasks, web shells, "Living Off the Land" (LOTL) use)
- Identify exfiltrated data and volume
- Build a timeline
- Determine dwell time and entry point (e.g., exploited vulnerability)

- Look for locations used for data staging (e.g., temporary folders, shared drives, cloud synchronization directories)
- Check systems that can be used for lateral communication (e.g., email, chat, and collaboration platforms)

Remediation

- Remove attacker persistence (e.g., web shells, implants, scheduled tasks)
- Consider restoring the whole IT infrastructure, or at least the part that is for sure compromised
- Consider resetting all the credentials and tokens (i.e., user accounts, technical accounts, administrative accounts, etc.), including long-lived and cloud-integrated tokens
- Consider using “tiered credential rotation”
- Consider reviewing the Data Loss Prevention (DLP) policy and related measures
- Consider segmenting access (e.g., Zero-Trust and least-privilege principles)

Evidence keeping

- Network captures, proxy logs, system images
- Any log evidencing a staged attack (e.g., relying on collaboration, chat or email)
- DLP and Cloud Access Security Broker (CASB) alerts

Post-incident activity

- Patch all entry vectors (e.g., VPN, email, apps)
- Consider implementing a threat-hunting practice
- Consider deploying detections mechanisms for LOTL and unusual outbound traffic

Communication

- Escalate to Top Management, legal, and compliance
- Coordinate with Data-Protection Officer (DPO), if personal data was exfiltrated (c.f., General Data Protection Regulation (GDPR))

Key watchpoints

- Exfiltration may be stealthy and encrypted (e.g., sent to common cloud services, and chunked in small packets)
- Advanced attackers may use fileless techniques and hide in legitimate processes (LOTL)

Rulebook 8 – Package compromission & supply chain attack

This rulebook applies to situations where an attack leverages third-party dependencies (e.g., software packages, libraries, open-source codes, firmware, etc.) to compromise the entity's systems.

Typical initial detection

- Unusual alerts following a software or firmware update, or the integration of a new third-party package
- Failures in hash validation or use of unexpected certificates used to sign packages
- Outbound traffic to abnormal domains
- Endpoint Detection and Response (EDR) alerts on newly updated binaries, installers or side-loaded Dynamic-Link Libraries (DLLs)
- Permission abuse of an application or integration (e.g., observed via unexpected OAuth / Single Sign On (SSO) consent or expanded scopes)
- Unusual requests originating from third-party services (e.g., API calls to unusual domains)
- Software behaviour not in line with the intended design (i.e., Software Bill of Materials (SBOM) drift)

Immediate response (containment)

- For all the systems, freeze the deployments and disable the auto-updates
- At network level, move affected hosts, containers and build agents (i.e., the worker machines that execute the Continuous Integration / Continuous Delivery (CI/CD) jobs) to quarantine
- Block the observed Indicators of Compromise (IoCs) (e.g., domains, IP addresses, hashes, certificates)
- Restrict the outbound traffic of affected systems to a small allowlist of trusted software-update endpoints
- Revoke or rotate affected (or suspected to be affected) secrets and tokens
- Disable suspicious OAuth and SSO integrations
- Require an additional authentication challenge (beyond the initial login) for administrators
- Inform the Security Operations Centre (SOC) and the Business Continuity Management (BCM) function of the incident, to seek for additional technical and business impact
- Look for vendors or maintainers' advice

Investigation steps

- Identify the compromised components; in particular note the affected versions and install times
- List all the subsequent assets at risks, including those installed, updated, or used by the compromised components
- Verify digital signatures and compare hashes with trusted sources
- Validate certificate chain and revocation
- Look for full process descendant chains (i.e., children processes, grandchildren processes, etc.) originating from affected installers
- Review the CI/CD logs, the artifact repository records and SBOMs for potential traces of alteration
- Audit logs to identify potential token abuse or data access
- Hunt for traces of persistence (e.g., services, scheduled tasks, Windows Management Instrumentation (WMI), etc.)
- Check for traces of lateral movement, privilege escalation and exfiltration
- Verify the authenticity and integrity of upstream update channels and sources (e.g., golden images, Mobile Device Management (MDM) baselines, mirrors, update proxies like Windows Server Update Services (WSUS)) by validating signatures, certificate chains/revocation, and digests
- Keep a timeline and take note of remediation decisions and actions

Remediation

- Put the compromised packages in a blocklist and remove them from the registries and caches
- Patch with clean updates or roll back to last know clean versions
- Rebuild, or redeploy or replace the compromised components, using trusted sources
- Recreate the impacted systems
- Rotate or invalidate, as appropriate, the secrets, API keys, certificates, signing keys, SSH keys, SSO / OAuth refresh tokens, etc., potentially exposed to the attack
- Remove the persistence artifacts (e.g., services, scheduled tasks, Windows Management Instrumentation (WMI), etc.)
- Perform integrity checks, check packages execution in sandboxes and increase the monitoring sensitivity (temporarily)

Evidence keeping

- Take snapshots of compromised Virtual Machines (VMs) and take capture of memory on key affected hosts
- Keep copies of the malicious components (e.g., installers, packages, containers, certificate chains, etc.)
- Keep a list of the instructions used to produce the malicious components (e.g., URL of repositories, applied patches, required packages, compiler, commands, etc.) and the traces of who / what built it and when
- Keep logs of EDR, endpoints, CI/CD, artifact registries, proxies, access, etc.
- Capture network traffic of key affected systems
- Keep trace and a timeline of the communications with the vendors or the maintainers

Post-incident activity

- Consider enforcing the source verifications, for instance via verified SBOMs and attestations
- Consider implanting private registries and update proxies (rather than connecting directly to the Internet) together with a source allowlist
- Consider using “tiered credential rotation” and reducing the lifetime of tokens for third-party access
- Consider reviewing CI/CD hardening controls and look for potential improvements (e.g., only accept components with valid signatures, Multi-Factor Authentication (MFA) for privileged access to the pipeline, least privilege principle, enforce isolation for runners (i.e., not privileged, destroyed after each build, segregated as much as possible))
- Consider implementing a careful strategy for deployments (e.g., “canary” releases and staged rollouts with rollback mechanisms)
- Consider ongoing controls over third-party components, verifying software authenticity with digital signatures, and limiting connections to known certificates only where appropriate
- Consider improving the vendors and maintainers’ risk review, including contract security clauses and “kill-switch” rights (i.e., possibility to disable product, or update or data flow, on the entity’s end)
- Consider monitoring exfiltration via tunnelling techniques

Communication

- Coordinate with the Security Operations Centre (SOC) and IT teams
- Contact the vendors or the maintainers for IoCs, patches, advice and root cause analysis
- Inform business owners and clients if appropriate

Key watchpoints

- Beware of stolen certificates, which are commonly used, and prevent relying solely on code signing
- Beware of auto-update feature that can lead to new infection
- Third-party application may have excessive access rights
- Beware of long dwell time and potential second-stage payloads
- Attackers often target build systems; therefore, isolation and monitoring are key
- Offline and immutable backups are key to recover

Glossary (generated via artificial intelligence tools)

Acronym / expression	Meaning
AD	Active Directory. A directory service developed by Microsoft for Windows domain networks that functions as a centralized database for network information. It stores data about network objects (users, computers, printers) and manages security policies, authentication, and authorization across the entire network infrastructure
Adware	Software that automatically displays or downloads advertising material (often unwanted) when a user is online
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
API	Application Programming Interface. A set of defined rules and protocols that allows different software applications to communicate with each other, enabling them to exchange data and functionality without needing to understand each other's internal code
ASN	Autonomous System Number. Unique number assigned to a network or group of IP prefixes under a single routing policy, used to identify it in BGP routing on the internet
AV	Antivirus. Software designed to detect, prevent, and remove malicious software (malware), such as viruses, worms, and Trojans
Backdoor	A covert method of bypassing normal authentication or encryption in a computer system, a product, or an embedded device
BCM	Business Continuity Management. A holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause
BCP	Business Continuity Plan. A document that outlines the processes and procedures an organization will follow to maintain essential functions during and after an unplanned event or disruption
BGP	Border Gateway Protocol. Standard exterior routing protocol that exchanges routing and reachability information between autonomous systems on the internet
Botnet	A network of private computers infected with malicious software and controlled as a group without the owners' knowledge, often used to launch DDoS attacks, send spam, or spread malware
Brute Forcing	An attack method that involves systematically checking all possible combinations of passwords or keys until the correct one is found. It is a "trial-and-error" approach that can be time-consuming but effective against weak or short credentials

Acronym / expression	Meaning
C2	Command and Control. The server infrastructure used by attackers to communicate with compromised systems, send commands, and exfiltrate data
Canary	Refers to “Canary Deployment” or “Canary Release”. A software release strategy where a new version of an application is rolled out to a small subset of users (the “canaries”) before being deployed to the entire user base. If the new version contains bugs or performance issues, only a small group is affected, and the rollout can be quickly reversed.It can also refer to “Canary Tokens”, which are digital tripwires used to detect breaches
CASB	Cloud Access Security Broker. A security policy enforcement point (software or service) that sits between cloud service consumers (users) and cloud service providers. It allows organizations to extend their security policies into the cloud by providing visibility into cloud application usage, enforcing data security (like encryption and DLP), and detecting threats across cloud environments
CDN	Content Delivery Network. A geographically distributed group of servers that work together to provide fast delivery of Internet content
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team. An expert group responsible for handling computer security incidents, including detection, response, and recovery
CI/CD	Continuous Integration/Continuous Delivery (or Deployment). A DevOps practice that automates the software development lifecycle.CI (Continuous Integration): Developers frequently merge code changes into a central repository, where automated builds and tests run to detect bugs early.CD (Continuous Delivery/Deployment): Automates the release process, ensuring code can be reliably released to production at any time (Delivery) or is automatically released to production after passing tests (Deployment)
CIRCL	Computer Incident Response Center Luxembourg
CNPD	Commission Nationale pour la Protection des Données
Container	A lightweight, standalone executable package that includes everything needed to run a piece of software, including the code, runtime, libraries, and system tools. Containers share the host OS kernel but run in isolated user spaces, offering a more efficient alternative to full virtual machines

Acronym / expression	Meaning
CPU	Central Processing Unit. The primary component of a computer that acts as its “brain”, executing instructions and performing calculations necessary for software to run
Credential Dumping	The technique of extracting sensitive authentication data (like cleartext passwords, hashes, and Kerberos tickets) from the memory of the Local Security Authority Subsystem Service (LSASS) process on Windows. Tools like Mimikatz are commonly used to “dump” this memory, allowing attackers to steal credentials for privilege escalation and lateral movement
Crypto miner	Malware that uses a victim’s computer processing power to mine for cryptocurrencies without their consent or knowledge, often leading to significant performance degradation
CSIRT	Computer Security Incident Response Team. A specialized group of IT professionals responsible for managing, coordinating, and responding to cybersecurity incidents within an organization to minimize damage and ensure recovery.
CSSF	Commission de Surveillance du Secteur Financier
DDoS	Distributed Denial of Service. A type of cyberattack where multiple compromised systems (botnets) are used to target a single system or network, overwhelming it with traffic to render it unavailable
DevOps	Development and Operations. A collaborative software development methodology that bridges the gap between software developers (Dev) and IT operations teams (Ops)
DKIM	DomainKeys Identified Mail. An email security standard that adds a cryptographic digital signature to emails. This signature verifies that the email was indeed sent by the claimed domain and that its contents have not been altered in transit
DLL	Dynamic Link Library. A file format used in Microsoft Windows that contains shared code and data (such as functions or resources) which can be used by multiple programs simultaneously
DLP	Data Loss Prevention. A set of tools, strategies, and processes designed to ensure that sensitive data is not lost, misused, or accessed by unauthorized users
DMARC	Domain-based Message Authentication, Reporting, and Conformance. An email authentication protocol that builds on SPF and DKIM. It allows domain owners to publish a policy telling receiving servers what to do if an email fails authentication (e.g., reject it or mark it as spam) and provides reports on email activity

Acronym / expression	Meaning
DNS	Domain Name System. The hierarchical naming system that translates human-readable domain names (like www.example.com) into machine-readable IP addresses
DORA	Digital Operational Resilience Act
DoS	Denial of Service. A cyberattack that aims to make a machine, network, or service unavailable to its intended users by overwhelming it with excessive traffic or exploiting vulnerabilities to crash the system
DPO	Data Protection Officer
Dropper	A type of Trojan horse designed to “drop” (install) other malware onto a target system. Unlike a downloader that fetches malware from the internet, a dropper typically contains the malicious payload within itself, often encrypted or compressed to evade detection by antivirus software. Once executed, it extracts and installs the payload (such as ransomware or a backdoor) and may then delete itself to hide evidence of the infection
DRP	Disaster Recovery Plan. A documented, structured approach that describes how an organization can quickly resume work after an unplanned incident. A DRP is a subset of a Business Continuity Plan (BCP) and focuses specifically on restoring IT infrastructure and operations after a crisis
EDR	Endpoint Detection and Response. A cybersecurity technology that continuously monitors endpoint devices (like laptops and servers) to detect and respond to advanced threats that may bypass traditional antivirus solutions
GDPR	General Data Protection Regulation
Geo-fencing	A security mechanism that creates a virtual geographic boundary (“fence”) around a physical location
GOVCERT.LU	Governmental Computer Security Incident Response Team
GPO	Group Policy Object. A feature in Microsoft Windows Active Directory that allows administrators to define and control the working environment of users and computers. GPOs are used to enforce security settings and user configurations across a network
Hash	A fixed-size alphanumeric string generated from data of any size using a mathematical formula (hashing algorithm). Hashes are like “digital fingerprints”; if even a single bit of the original data changes, the resulting hash changes completely. They are used to verify data integrity and store passwords securely
HCPN	High Commission for National Protection

Acronym / expression	Meaning
HR	Human Resources
HTTP/HTTPS	Hypertext Transfer Protocol (HTTP) is the fundamental protocol for transferring data (like webpages) over the internet. However, it transmits data in “plain text”, meaning anyone intercepting the traffic can read it.HTTPS (HTTP Secure) is the secure version that adds an encryption layer using TLS (Transport Layer Security). It ensures that data exchanged between a user’s browser and the website is encrypted and authenticated, preventing attackers from eavesdropping, tampering with data, or impersonating the site
Hypervisor	Software, firmware, or hardware that creates and runs virtual machines (VMs) by separating a computer’s operating system and applications from the underlying physical hardware. From a security perspective, hypervisors provide isolation between VMs, but if compromised, an attacker could gain control over all guest systems
IAM	Identity and Access Management. A framework of policies and technologies that ensures the right individuals have the appropriate access to technology resources. It manages digital identities (like user accounts) and controls user access permissions to critical information and systems within an organization
IdP	Identity Provider. A system component or service that creates, maintains, and manages digital identity information for users and devices. It provides authentication services to other applications, allowing a user to log in once (Single Sign-On) and gain access to multiple different systems without creating new credentials for each one
IDS	Intrusion Detection System. A security tool that passively monitors network traffic or system events for suspicious activity and known threats, alerting administrators when potential breaches are detected without actively blocking them
ILR	Institut Luxembourgeois de Régulation
Infostealer	Malware designed specifically to find and exfiltrate sensitive information from a victim’s computer, such as login credentials, financial data, and personal documents
IOC	Indicator of Compromise. Forensic artifact or data point that indicates a system or network has likely been breached or is under malicious activity
IP	Internet Protocol. Network protocol that defines how data packets are addressed and routed between devices, using unique IP addresses to identify and locate each device on a network

Acronym / expression	Meaning
IPS	Intrusion Prevention System. An active security control that sits in-line with network traffic to inspect packets in real-time, detecting malicious activity and automatically blocking or mitigating threats before they can damage the network
ISP	Internet Service Provider. A company or organization that provides customers with access to the internet and related services
IT	Information Technology
Kerberoasting	A post-exploitation attack targeting Active Directory service accounts. An authenticated attacker requests a Kerberos service ticket for a specific Service Principal Name (SPN). The returned ticket is encrypted with the service account's password hash. The attacker then takes this ticket offline to crack the hash using brute force, revealing the service account's plaintext password
KEV	Known Exploited Vulnerabilities
Keylogger	A type of spyware that records every keystroke made on a computer. This allows attackers to steal sensitive information such as usernames, passwords, and credit card numbers
Kill-switch	A security mechanism designed to immediately shut down or disconnect a system, application, or network connection in an emergency
Lateral movement	Techniques used by attackers after initial access to move from one compromised system to others within the same network, in order to discover, access, and control additional assets or sensitive data while evading detection
Logic bomb	A piece of malicious code intentionally inserted into a software system that will set off a malicious function when specified conditions are met
LOTL	Living Off the Land. A cyberattack technique where attackers use legitimate, pre-installed tools and features already present in the target system (such as PowerShell, WMI, or BASH) to conduct malicious activities. Because these tools are trusted and standard, the attack activity blends in with normal system operations, making it difficult for traditional security tools to detect

Acronym / expression	Meaning
LSASS	Local Security Authority Subsystem Service. A critical Microsoft Windows system process (lsass.exe) responsible for enforcing security policies on the system. It verifies users logging on to a computer or server, handles password changes, and creates access tokens. Crucially for cybersecurity, LSASS stores sensitive credentials (like password hashes and Kerberos tickets) in its process memory to facilitate single sign-on. Because of this, it is a primary target for attackers using tools like Mimikatz to “dump” this memory and steal credentials for lateral movement
MDM	Mobile Device Management. A type of security software used by IT departments to monitor, manage, and secure mobile devices (smartphones, tablets, laptops) that access corporate data
MFA	Multi-Factor Authentication. A security method that requires users to provide two or more verification factors to gain access to a resource, such as an application or online account, adding a critical layer of security beyond just a password
NAC	Network Access Control. A security approach that restricts unauthorized users and devices from gaining access to corporate networks. NAC can enforce security policies on devices before they are allowed to connect
NIS2 directive	Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union
NTP	Network Time Protocol. A networking protocol used to synchronize clocks between computer systems over packet-switched, variable-latency data networks, ensuring devices maintain accurate and consistent time for logs, security certificates, and scheduled tasks
OAuth	Open Authorization. An open standard protocol that allows users to grant third-party websites or applications access to their information on other websites without sharing their passwords. It functions by exchanging tokens rather than credentials
Pass-the-Hash Attack (PtH)	A lateral movement technique where an attacker captures a hashed user credential (not the plaintext password) and uses it directly to authenticate to a remote server or service. This exploits authentication protocols that accept hashes for verification, allowing attackers to bypass the need for the actual password

Acronym / expression	Meaning
Pass-the-Ticket Attack (PtT)	A post-exploitation technique where an attacker steals a valid Kerberos ticket (such as a Ticket Granting Ticket or TGT) from a compromised system and uses it to authenticate to network resources. This allows the attacker to move laterally across the network appearing as a legitimate user, often bypassing MFA
Password Spraying	A specific type of brute force attack where an attacker tries a single common password (e.g., “Winter2025!”) against many different user accounts. This “low-and-slow” approach is designed to avoid triggering account lockout policies that would normally block repeated failed login attempts on a single account
Payload	The component of a cyberattack or malware that executes the malicious activity. While the “delivery mechanism” (like a phishing email) gets the threat to the target, the payload is the cargo that performs the actual harm, such as encrypting files (ransomware), stealing data (spyware), or installing a backdoor
PCAP	Packet Capture. File or data format that stores raw network packets captured from a network interface for later analysis
Privilege escalation	A cyberattack technique where an attacker, having already gained initial low-level access to a system, exploits vulnerabilities, bugs, or misconfigurations to elevate their permissions
PsExec	A command-line tool from the Sysinternals suite that allows users to execute processes on remote systems with full interactivity. While a legitimate administrative tool, it is frequently abused by attackers for lateral movement and remote code execution within a compromised network
QoS	Quality of Service. A set of technologies and mechanisms that manage data traffic on a network to ensure reliability and performance for critical applications
Ransomware	Malware that encrypts a victim’s files or locks them out of their system, demanding a ransom payment, often in cryptocurrency, in exchange for the decryption key or access
RAT	Remote Access Trojan. A type of malware that provides an attacker with remote administrative control over an infected computer
RDP	Remote Desktop Protocol. A proprietary protocol developed by Microsoft that provides a user with a graphical interface to connect to another computer over a network connection

Acronym / expression	Meaning
Registry	A hierarchical database in Microsoft Windows that stores low-level settings and configuration information for the operating system and for applications that opt to use it. It is a critical component for system function and a frequent target for malware, which may use it for persistence, configuration changes, or storing malicious data
Reverse Shell	A type of connection where the target machine (victim) actively initiates a network connection back to the attacker's machine. This technique is used to bypass inbound firewall rules, which typically block outside connections but allow internal systems to connect out to the internet
RMM	Remote Monitoring and Management. Software platforms, often used legitimately by IT administrators, that allow for the remote management and monitoring of endpoints. However, attackers can abuse these tools to gain persistent access to a network, appearing as legitimate traffic to evade detection
Rootkit	A collection of malicious software tools that gives an unauthorized user privileged ("root") access to and control over a computer system without being detected. Rootkits can hide their presence and other malware on a system
SBOM	Software Bill of Materials. A comprehensive inventory or "ingredients list" of all components, libraries, and dependencies that make up a piece of software. It is critical for supply chain security, allowing organizations to quickly identify if they are using vulnerable open-source components within their applications
Session Hijacking	A cyberattack method where an attacker intercepts or steals a valid session token (like a cookie) to impersonate a legitimate user. This allows the attacker to access the user's active session and services without needing to know their username or password
SFTP	Secure File Transfer Protocol (or SSH File Transfer Protocol). A network protocol used for securely transferring files between systems over an encrypted connection. Unlike standard FTP, which sends data in plain text, SFTP uses the SSH (Secure Shell) protocol to encrypt both commands and data, protecting sensitive information from interception during transit
SHA-256	Secure Hash Algorithm 256-bit. A cryptographic function developed that converts data of any size into a fixed 256-bit string (hash).

Acronym / expression	Meaning
SIEM	Security Information and Event Management. A security solution that provides real-time analysis of security alerts generated by applications and network hardware. It aggregates log data from various sources, identifies deviations from norms, and enables security teams to detect, investigate, and respond to threats more effectively
SMB	Server Message Block. A network file sharing protocol that allows applications on a computer to read and write to files and to request services from server programs in a computer network
SMS	Short Message Service
Snapshot	A record of the state of a system, disk volume, or file system at a specific point in time
SOC	Security Operations Centre. A centralized unit that deals with security issues on an organizational and technical level. A SOC is comprised of a team of cybersecurity professionals who monitor, analyse, and respond to cybersecurity incidents
SPF	Sender Policy Framework. An email authentication protocol that allows domain owners to specify which mail servers are authorized to send email on behalf of their domain. This helps prevent attackers from spoofing (impersonating) the domain in phishing emails
SPN	Service Principal Name. A unique identifier used in the Kerberos authentication protocol to identify a specific service instance (like a SQL server or HTTP service) running in an Active Directory environment. It maps a service to the account it is running under (a user or computer account), allowing the network to authenticate the service. Attackers often scan for SPNs to identify service accounts that can be targeted in “Kerberoasting” attacks to crack their passwords
Spyware	Malware that secretly observes the user’s computer activities without permission and reports it to the software’s author
SSH	Secure Shell. A network protocol that gives users, particularly system administrators, a secure way to access a computer over an unsecured network
SSL	Secure Sockets Layer. An older encryption protocol designed to secure communications over a computer network. While the term “SSL” is still widely used colloquially to refer to web encryption certificates, the protocol itself has been deprecated and replaced by the more secure TLS
SSO	Single Sign-On. An authentication process that allows a user to access multiple applications and services with one set of login credentials

Acronym / expression	Meaning
SSRF	Server-Side Request Forgery. A web security vulnerability that allows an attacker to trick a server into sending requests to unintended locations. Attackers often use this to force the server to connect to internal-only services (like metadata services in cloud environments) to access sensitive data or credentials
Supply chain attack	A cyberattack that targets an organization by infiltrating a trusted third-party vendor, supplier, or partner in its supply chain. Instead of attacking the primary target directly (which may have strong defences), attackers compromise a less secure external provider – such as a software vendor, hardware manufacturer, or managed service provider – to gain access to the target's network
SYN/ACK	Synchronize/Acknowledge. The second step in the TCP three-way handshake used to establish a reliable network connection
Sysinternals	A suite of free, advanced system utilities and technical resources designed to manage, diagnose, troubleshoot, and monitor Microsoft Windows environments. The suite includes a wide range of tools, many of which are essential for cybersecurity professionals for tasks like malware analysis, incident response, and performance troubleshooting. Popular tools in the suite include Process Explorer, Autoruns, Sysmon, and PsExec
Sysmon	A Windows service and device driver from the Sysinternals suite that provides advanced system monitoring. It logs detailed information about process creations, network connections, and changes to the file system to a dedicated event log, offering deeper visibility for threat hunting and incident response than standard Windows logs provide
Threat Intelligence	The process of collecting, analysing, and applying data about cyber threats, adversaries, and their methods. It transforms raw data into actionable insights, helping organizations understand threat actors' motives and targets, and allowing them to shift from reactive defences to proactive strategies
TLP	Traffic Light Protocol
TLS	Transport Layer Security. The modern cryptographic protocol that provides end-to-end communications security over networks. It encrypts data sent between a client (like a web browser) and a server, ensuring privacy and data integrity, and is the standard technology behind secure HTTPS connections

Acronym / expression	Meaning
Token	In authentication, a digital object (software or hardware) that provides a second factor of authentication or represents a user's identity and permissions after they have logged in (e.g., a session token). This allows users to access resources without re-entering credentials for every request
Trojan	Malware that disguises itself as a legitimate program or file to trick a user into downloading and executing it. Unlike viruses and worms, Trojans do not self-replicate
UBA	User Behaviour Analytics. A cybersecurity process that uses machine learning and statistical analysis to establish a baseline of "normal" behaviour for users and devices on a network. By continuously monitoring activity, UBA detects anomalies – such as unusual login times, mass file downloads, or lateral movement – that may indicate a compromised account, insider threat, or cyberattack
URI	Uniform Resource Identifier. Text string that uniquely identifies a resource on a network, such as a document, image, or service (includes URLs as a subset)
URL	Uniform Resource Locator. Text string that specifies the address of a resource on a network and how to retrieve it, commonly used as a web address in browsers
Virus	A type of malicious code or program written to alter the way a computer operates and that is designed to spread from one computer to another by inserting its own code into other programs
VM	Virtual Machine. A software-based emulation of a physical computer that runs its own operating system and applications in an isolated environment, separated from the underlying physical hardware
VPN	Virtual Private Network. A technology that creates a secure, (often) encrypted connection (tunnel) over a less secure network, such as the public internet
Vulnerability	A weakness or flaw in a system's design, implementation, or configuration that can be exploited by an attacker to compromise the system's confidentiality, integrity, or availability
WAF	Web Application Firewall. A security system that filters, monitors, and blocks HTTP/HTTPS traffic to and from a web application

Acronym / expression	Meaning
Web Shell	A malicious script or program uploaded to a compromised web server to give an attacker persistent remote administration capabilities. Once installed, it acts as a “backdoor”, allowing the attacker to execute system commands, modify files, and pivot deeper into the network through their web browser, often bypassing firewalls that allow standard HTTP/HTTPS traffic
Windows Event Viewer	A built-in Microsoft Windows tool that lets administrators and users view event logs generated by the operating system and applications
Wiper	A destructive form of malware designed to permanently erase or overwrite all data on a compromised system, rendering it unrecoverable
WMI	Windows Management Instrumentation. A core component of the Windows operating system that provides a standardized way for managing devices and applications on a network. Attackers can abuse WMI for lateral movement, code execution, and persistence within a compromised environment
Worm	Standalone malware that replicates itself to spread to other computers, often using a computer network to spread itself, relying on security vulnerabilities on the target system
WSUS	Windows Server Update Services. A Microsoft tool that allows IT administrators to manage and distribute Windows updates and patches to computers within a corporate network
Zero-Trust	A security framework based on the principle “never trust, always verify”. It assumes that no user, device, or network connection – whether inside or outside the corporate perimeter – should be trusted by default. Instead, every access request is continuously verified for identity, authorization, and device health before granting access to specific resources