Ready for (nearly) anything: Five things to prepare for a cyber security incident

gabrielcurrie.medium.com/ready-for-nearly-anything-five-things-to-prepare-for-a-cyber-security-incident-4fc49d665488

Gabriel Currie August 28, 2021

Gabriel Currie

Jun 20, 2021

.

6 min read

Every organisation has experienced, or will experience, a cyber security incident; depending on what you define the term as, most organisations have multiple every day.

Increasingly punitive data protection regulation (such as the GDPR's ability to fine organisations up to 4% of global turnover for data breaches) coupled with increasing public awareness and scrutiny of organisations' public responses means that it's more important than ever to effectively respond to these incidents.

There are five key things that I think every cyber security team needs to effectively prepare for an incident, and which can minimise the security, operational and financial risk the incident poses:

1. that document the considerations, decisions and actions to be taken in the event of an incident
2. Skilled and experienced to lead, coordinate and execute the response to the incident
3. to inform the investigation into the incident and help gain an understanding of what has happened, when, and how
4. Technology to execute and actions that mitigate risk from the incident
5. technology for incident response teams, to communicate and collaborate, delegate and track response actions, and manage delivery

Processes that document the considerations, decisions and actions to be taken in the event of an incident

Documented processes are key to effectively responding to an incident; they provide a guide-rail for an experienced team, and a lifeline to the less experienced. While every team structures their processes differently, these might typically include:

- . A cyber incident response plan is the overarching document which details what the organisation (or, often a specific part of the organisation such as the SOC) does in response to a cyber incident. This may also be supported by other, related documents, such as an incident management framework, an IT incident management plan, or a disaster recovery plan.
- . Technical runbooks provide detailed guidance on how front-line teams (e.g., the SOC or CSIRT) should respond in the event of a specific incident scenario. CERT SocGen's provides short examples of technical runbooks.
- . Knowledge articles provide detailed guidance on specific actions that underpin the response to one or more incident scenarios. This might include, for example, analysing a potentially malicious IP address, isolating an endpoint from the network, or resetting a user's Active Directory credentials. Knowledge articles are typically held in a wiki, using software such as or .

Skilled and experienced people to lead, coordinate and execute the response to the incident

Larger cyber security teams typically have a dedicated cyber incident response function, whereas others might move staff into this function as and when required. Some teams may lack a cyber incident response function altogether, and rely exclusively on outsourced providers. Regardless of how the function is resourced, cyber security teams should ensure they have access to the skills and experience needed to lead, coordinate and execute the response to an incident.

The necessary skills and experience are not just digital forensics and incident response, but extend to wider cyber security, IT, and business. The NIST Workforce Framework for Cybersecurity articulates many of these (although doesn't cover many of the "soft" skills needed).

If in-house, the cyber incident response function should be resourced and structured to reflect the nature and extent of its role, with well-defined job descriptions for staff, and suitably detailed training plans to allow staff to maintain currency and enable progression. If outsourced, there should be a clear view as to what skills and experience are accessible, when, and how.

Logs to inform the investigation into the incident and help gain an understanding of what has happened, when, and how

Logs provide the evidence for an investigation into an incident, and help to gain an understanding of what has happened, when, and how. (Logs also provide a mechanism for detecting threats in the first place, but that's not something I'll cover here.)

As such, teams should ensure they have the right logs available, for the right amount of time, and that these are accessible in the right ways.

What logs to store

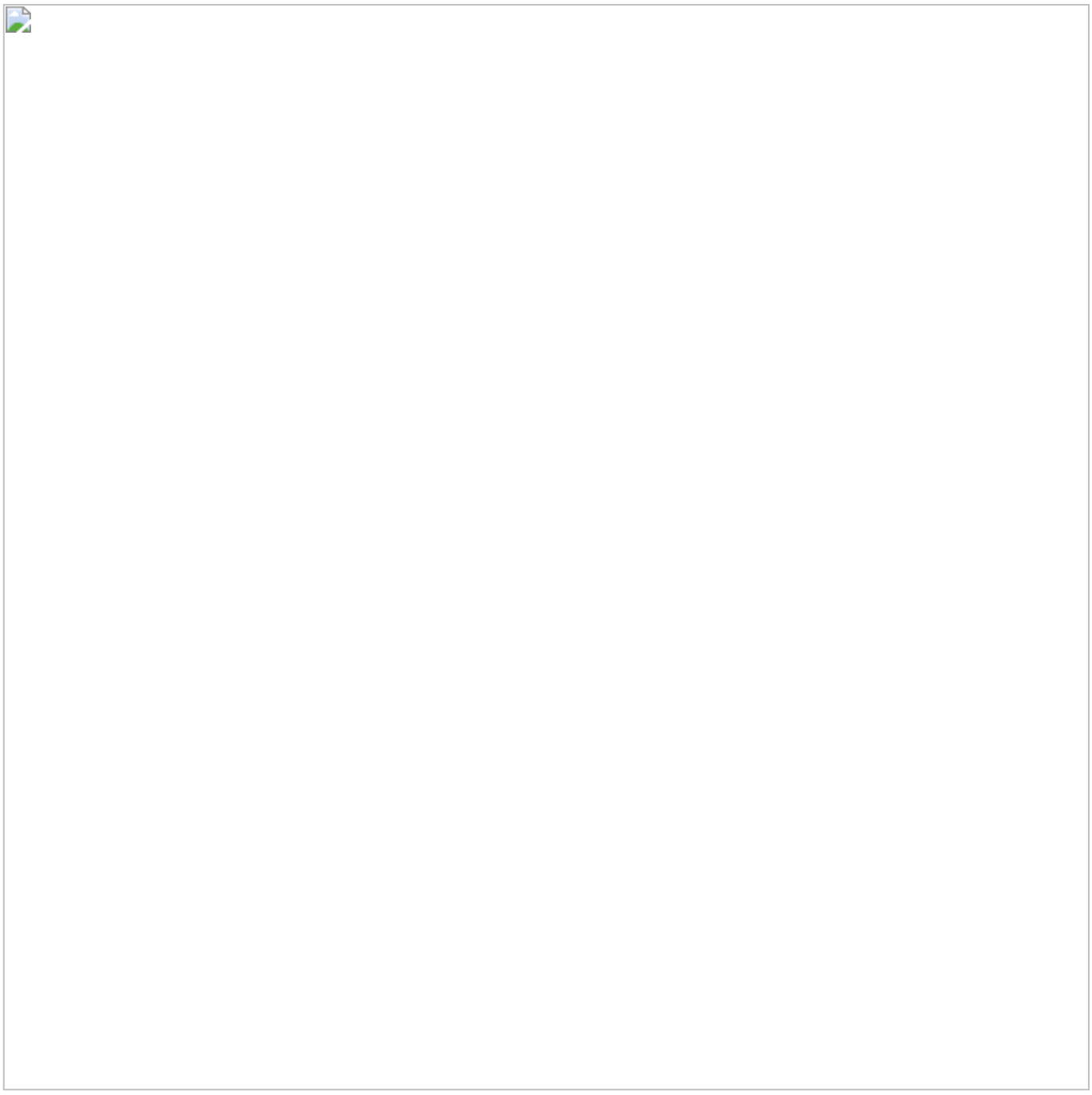
The choice of which logs to store (and which not to) should be aligned to the likely real-world threat and investigative requirements. Logs should be stored which help the team to do their job and answer key questions like "*what systems did the attacker connect to?*" or "*was any data stolen?*" in likely incident scenarios.

Any applicable regulations should also be considered when determining what logs to store. For example, the GDPR's requirement for "data minimisation" means that security logs should not contain personal data unless this is specifically required for the purpose the logs are themselves stored (i.e. to enable the investigation of potentially malicious activity). If personal data is stored, then the logs should be handled appropriately (i.e. according to the other requirements of the GDPR, such as accuracy and security).

How long to store logs for

The choice of logging retention periods should again be aligned to the likely real-world threat and investigative requirements. Logs should be stored for the amount of time that they will typically be of use to the team.

This might be, for example, based on the average dwell time of likely attackers. FireEye's 2021 M-Trends report identified a median dwell-time for non-ransomware investigations of 45 days, with 25% of these non-ransomware investigations having a dwell time of 200+ days. If incidents are going to be investigated that occurred 200 days ago, the logs should be available to enable this.



Global dwell time during 2020 broken down by investigation type (Source:)

Again, any applicable regulatory requirements should be considered when determining retention periods. For example, PCI-DSS requires a minimum retention period of one year.

Making logs accessible

Logs should be accessible to cyber security teams, whatever is stored and however long they are stored for.

Logs should be initially stored in a central location so they can be correlated with each other, and accessed by analysts ideally through a “single pane of glass”. Access should be near-instant, with the ability to rapidly search through and analyse data.

As logs age, they may be moved to different locations (for example, to warm or cold storage). They should remain accessible, however, this may be slower to achieve with less compute power readily available for analysis, reflecting their drop in usefulness.

Technology to execute containment and eradication actions that mitigate the risk from the incident

Technology should be in place to execute containment actions that temporarily limit the attacker's ability to do further harm, and to execute eradication actions that remove their access to the environment.

Example containment and mitigation actions that might be taken (primarily with a network intrusion scenario in mind) are shown below; incident response teams should ideally have direct access to technology or tools which perform these actions, or otherwise be able to easily request these actions and have defined SLAs in place for their completion.

Example **host-based containment and eradication actions** include:

- Switching off systems, or restarting systems.
- Isolating hosts from the environment to prevent further attacker actions on the host, or lateral movement from it.
- Identifying (e.g., based on file name or path) and removing files from hosts.
- Blocking files from executing on hosts.
- Removing persistence mechanisms (e.g., services, registry keys, startup folder items) from hosts.

Example **network-based containment and eradication actions** include:

- Blocking known IOCs (e.g., IP addresses, domains, or traffic signatures) on external network infrastructure to prevent malware calling home, or the attacker connecting in.
- Isolating one or more areas of the network.

Example **identity-based containment and eradication actions** include:

- Changing account permissions, access or privileges (e.g., remove unauthorised administrator privileges).
- Resetting individual account credentials (including Active Directory user and service accounts, application accounts, and cloud provider accounts).
- Disabling accounts.
- Resetting credentials at scale.

Capability for incident response teams to communicate and collaborate, delegate and track response actions, and manage delivery

Cyber security incidents are often complex and fast-moving, and organisations may have multiple incidents of varying complexity and severity taking place at any one time. The ability for response teams to work effectively in such circumstances is key. Effective working in a cyber incident response scenario requires the following capabilities:

- . Synchronous (e.g., video and phone calling and conferencing) and asynchronous (e.g., text chat) communication internally and with external partners.
- . Collaborating on work internally and with external partners.
- . Documenting the tasks required to respond to the incident, tracking due dates, effort, status, assignees, and next steps. This can be achieved with something as simple as a spreadsheet, or a purpose-built task tracking system like Jira.
- . Capturing key statistics for each incident (e.g., using common schemas such as), and outputting these to enable management reporting.

All of these capabilities should be resilient (i.e., remain available in the event of a domain compromise or destructive attack) and secure (i.e., monitor and prevent eavesdropping by an attacker).