GUIDANCE

10 Steps to Cyber Security

Guidance on how organisations can protect themselves in cyberspace.

IN THIS GUIDANCE

PUBLISHED

11 May 2021

REVIEWED

11 May 2021

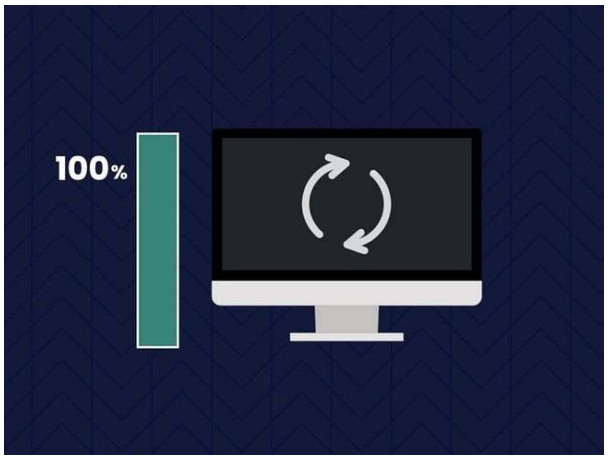
VERSION

1.0

WRITTEN FOR

Cyber security professionals

Logging and monitoring



Design your systems to be able to detect and investigate incidents.

Collecting logs is essential to understand how your systems are being used and is the foundation of security (or protective) monitoring. In the event of a concern or potential security incident, good logging practices will allow you to retrospectively look at what has happened and

understand the impact of the incident. Security monitoring takes this further and involves the active analysis of logging information to look for signs of known attacks or unusual system behaviour, enabling organisations to detect events that could be deemed as a security incident, and respond accordingly in order to minimise the impact.

What are the benefits?

- **Good logging practices provides the ability to understand, trace and react to system and security events**
- **Security monitoring provides insight into systems, and allows for the active detection of threats and potential security incidents**
- **Security monitoring introduces an additional layer of defence to systems**
- **Actively monitoring systems affords the opportunity to react to early signs of compromise, meaning organisations can respond effectively**

What should you do?

Understand your objectives for logging and monitoring

- When designing a monitoring solution, it should be proportionate to the context of the system, the threat that your organisation faces and the resources available to you. Doing this will build a picture, which will enable you to determine what is actually proportionate. This picture will help you decide the level of monitoring that is appropriate to your system. There is no one-size-fits-all solution, the case might be that simply be collecting logs in case of a security incident is the right fit for you.
- Conversely, your organisation might be subject to frequent cyber attacks, or may need to address risks with monitoring controls, which may require a security operations centre (SOC) with the ability to detect and respond to advanced attacks.

- At all levels, the main priority should be the ability to respond to incidents and to do this, logs are required. The NCSC's Introduction to logging for security purposes guidance provides a good place to start and will help organisations devise an approach to logging that will help answer the most critical questions during an incident.
- The NCSC's 'What exactly should we be logging' blog post introduces the MITRE ATT&CK framework and how it can be used to help define monitoring strategies. It also touches on outcome based and threat modelling approaches that can be used

Make sure your logs are available for analysis when you need them

- Understand where your logs are stored and ensure you have the appropriate access to be able to search through them.
- Ensure logs are held for long enough to be able to answer the questions you'll be asked during an incident. It can be months before incidents are detected so NCSC recommends storing your most important logs for at least 6 months. The amount of time you keep log data may vary for each source depending on things like cost and availability of storage, and the volume and usefulness of different data types. Plan for storage to roll-over, avoiding disks filling and the service failing.
- Consider which logs you want to draw into a centralised location for analysis across data sets. For some data sets it may be suitable to just call out to those log stores as required. If sending logs to a central log service, use transport encryption and one-way flow control where appropriate.
- Develop a method for ensuring that logs are still being captured as expected. This could be an automated alert when log messages stop arriving centrally, or an alert for when a periodic test event isn't captured (when it should be).
- Protect your logs from tampering so that is it hard for an attacker to hide their tracks and you can be confident that they accurately represent what has happened.

Use your logs to generate useful insights

- Setting security policies that define appropriate use and configuring systems based on business need (combined with an assessment of risk) will enable you to develop a monitoring service that analyses logs to verify that those policies are being enforced or followed as you expect. This is also useful in ensuring that all user activity complies with relevant legal or regulatory constraints.
- Use your understanding of the context of your system to create detection alerts based on the expected threats. This helps ensure the alerts generated will be relevant to your organisation's needs and that the action is relevant to inform the risks.
- Consider where you need to be monitoring, this should include on your network, devices and cloud services, as applicable. Monitoring solutions can provide both signature-based capabilities to detect known attacks, and heuristic capabilities to detect unusual system behaviour.

Develop an incident response plan

- Test your ability to detect incidents with exercising, and incorporate any lessons learnt from actual incidents into your monitoring solutions. Many organisations only realise their logging and monitoring systems are broken or insufficient when an actual incident occurs. Active exercising can help avoid you being caught out and improve your systems.
- Ensure your organisation's incident management plan is aligned with your logging and monitoring strategy so you already have a plan to deal with any incident that can be detected by your monitoring systems. This plan can then be exercised to ensure that any issues with communication and capability are highlighted and resolved, and practice will enable the team to react more confidently to any real incidents.

Stay informed

- Make use of threat intelligence. Sign up to the Cyber Security Information Sharing Partnership CiSP to receive and share threat information and indicators of compromise with industry and government counterparts.

Learn more

[Introduction to logging for security purposes]
Laying the groundwork for incident readiness.

[Logging made easy (LME)]
How to set up your own basic security logging system.

[Logging and protective monitoring]
Using logging and monitoring to identify threats and protect smartphones, tablets, laptops and desktop PCs.

[Security operations centre (SOC) buyers guide]
Guidance is for organisations that are considering procuring a Security Operations Centre (SOC) from a third party.

← Data security

Incident management →

Topics

Operational security

Risk management

Logging

PUBLISHED

11 May 2021

REVIEWED

11 May 2021

VERSION

1.0

WRITTEN FOR

Cyber security professionals

Also see

Weekly Threat Report 23rd July 2021
The NCSC's weekly threat report is drawn from recent open source...
Report
23 July 2021

The first Certified Cyber Professional (CCP) Specialism is now live!
'Risk Management' is the first certifiable specialism under the...
Blog Post
8 July 2021

NCSC statement on Kaseya incident

The NCSC's official statement on the Kaseya cyber incident.

News
5 July 2021