CYBER MANAGEMENT ALLIANCE

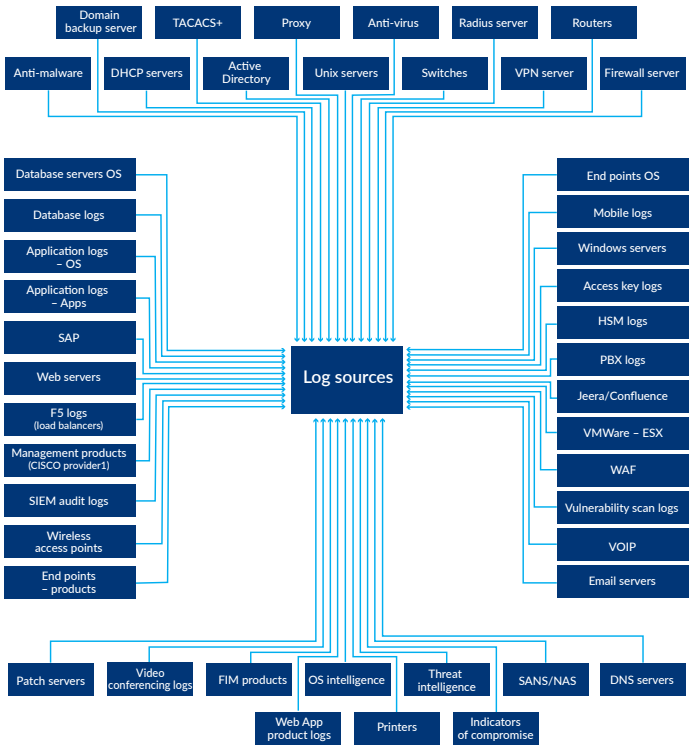
SIEM & USE-CASE ASSESSMENT

SIEM or Security Incident and Event Management systems are intended to provide organisations a 'one-window' view of and enhanced visibility into all security related activity.

The basic building blocks of a healthy and effective SIEM is an effective log management strategy. Put simply, the better and wider the log coverage (monitoring) in an organisation, the better the performance and output of its SIEM and the better the visibility into early malicious activity.

In addition to the above, use-cases form an integral part of SIEM systems and organisations rely heavily on use-cases to trigger malicious activity alerts (We call them threat scenarios or cyber-attack scenarios).

In this audit, we assess how your SIEM system is configured, assess the operational aspects of the SOC team and review the related monitoring technology stack. Importantly, we also review a sample of your existing use-cases to highlight any critical gaps in the use-case logic and configurations.



We DO not audit the SOC as an operational entity in this assessment.

info@cm-alliance.com https://cm-alliance.com +44 203 189 1422 @cm_alliance

Benefits:

- Understand how your approach to log management aligns with NIST's Computer Security Incident Handling Guide: NIST SP 800-61 Revision 2.
- Determine if your current SIEM implementation, configuration and its coverage are fit-for-purpose.
- Assess a sample of current 'use-cases' and alerts in the SIEM tool and determine if they align with your organisation's threats, threat actors and risk mitigation strategy.
- Identify improvements in your monitoring and SIEM systems.
- Recommend improvements in your use-cases and propose new, more relevant use-cases.
- Pinpoint specific technical improvements to boost detection and response capabilities.
- Identify potential cost savings on current and future spends.

What We Examine:

During our SIEM assessment, we will:

- Review your existing SIEM design.
- Review the use-cases (alerts etc.) that are configured.
- Review the monitoring policy, processes and standards.
- Gain an understanding of your technology landscape (infrastructure & application).
- Gain an understanding of the organisation's critical assets and risk appetite.
- Review incident triage, analysis and investigations.

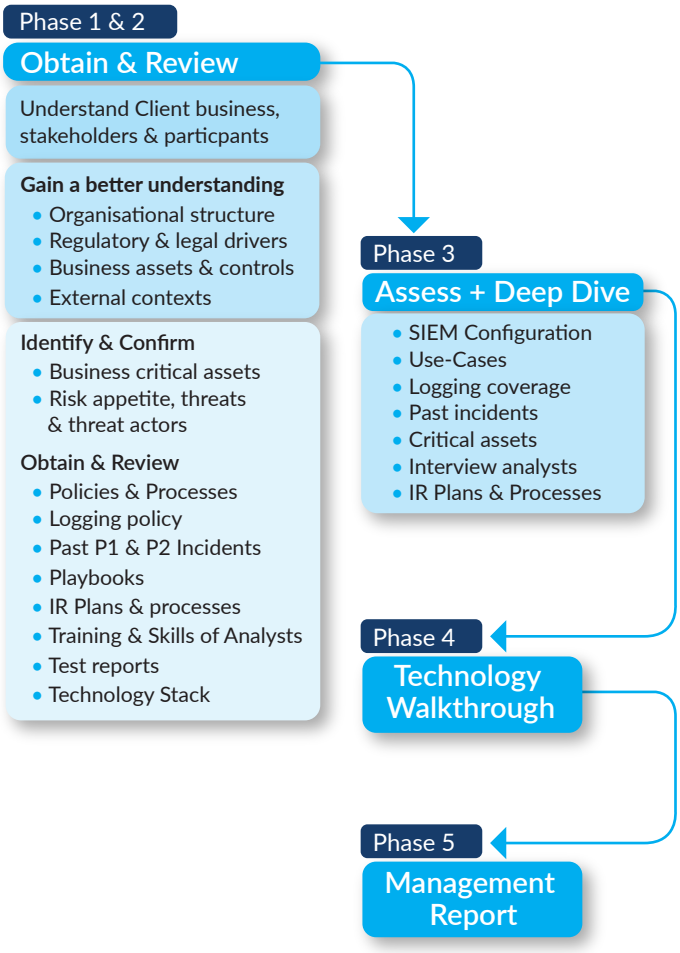
Stakeholders:

One of the primary objectives of this exercise is to collate and understand what the expected outcome of the service is. We seek to speak to stakeholders including, but not limited to:

- Sponsors of the SIEM project.
- Service manager/service delivery managers.
- The 'customer' or recipients of the SIEM service.
- Security analysts operating the SIEM.
- Head of Security Operations.
- Information Security representative(s).
- Threat intelligence operations.

Approach:

We adopt the same rigour, discipline and evidence-based approach to all our assessments. In Phase 1 & 2, we are in a 'fact-finding' mode and want to read and consume all the necessary information. Although we speak to staff in Phase 1, we tend to have more meaningful discussions in Phase 3 as we are more informed and hence more prepared with the right questions.

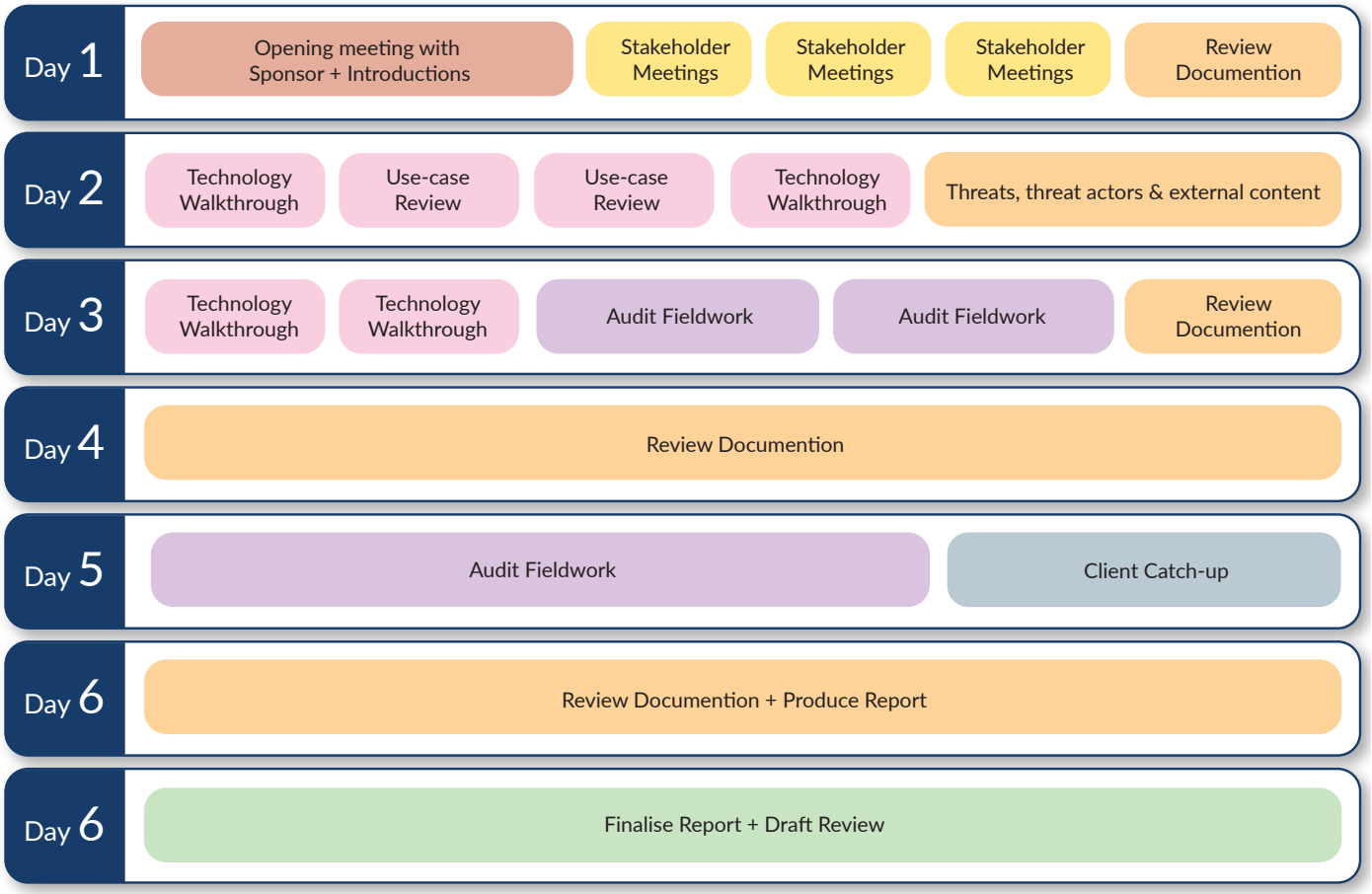


For the SIEM and technology assessments, we prefer technology walkthroughs so we can get a feel of the setup, mode of use and configurations. We also want to see the use-cases 'in action' and have an analyst walk us through several random use-cases and related incident tickets. We want to get a feel of what a 'day' looks like for the operator of the technology.

We then finish the assignment with a management report.

Sample Assessment Schedule:

Please note this is an approximation and the actual effort may vary depending on the client, the size of the SOC, the number of analysts and other factors.



Description	Total Duration
Initial meetings with Key stakeholders	2 hours
Multiple meetings with Analysts*	8 hours
SIEM use-case walkthrough with analysts	16 hours
Meetings with security engineering	4 hours
Documentation review	8 hours
Review, analyse and examine all inputs	8 hours
Report writing	8 hours
Total	**54 hours**

**Analysts = (SoC manager, IR team, threat intel team, Tier 1, Tier 2 Tier 3 analysts)*

Output:

You will receive a report with an executive summary accompanied by detailed findings.
The report will also contain clear and easy-to-understand recommendations to close the gaps.