itb
cyber solutions

LOGPOINT

UNDERSTANDING THE UK'S NCSC CYBER ASSESSMENT FRAMEWORK

How SIEM helps organizations address CAF Objective-C

The cybersecurity landscape is increasingly complex, with threats evolving rapidly. Organizations need robust frameworks to ensure their defenses are up to the task.

The UK's National Cyber Security Centre (NCSC) has developed the Cyber Assessment Framework (CAF), encompassing four key objectives designed to help government, education, healthcare, public safety and critical infrastructure providers ensure their systems are well protected.

In this document we will explore CAF Objective C and explain how Security Information and Event Management (SIEM) can play a pivotal role in meeting it.

OVERVIEW OF THE CAF

CAF is designed to help organizations manage cybersecurity risks in a structured and comprehensive manner. The framework is divided into four objectives, each focusing on a different aspect of cybersecurity.

Objectives

- **A** Managing security risk
- **B** Protecting against cyber attack
- **C** Detecting cybersecurity events
- **D** Minimizing the impact of cybersecurity incidents

The importance of Objective C

Objective C of the CAF emphasizes timely detection of cybersecurity events. Effective detection is crucial for initiating an appropriate response and minimizing potential damage.

Objective C is broken into several principles, including:

- **C1** Security monitoring to detect anomalous activity
- **C2** Analyzing security data to identify potential threats
- **C3** Regular testing and tuning of detection capabilities
- **C4** Ensuring detection coverage aligns with the risk profile

How SIEM helps organizations meet Objective C

Security Information and Event Management (SIEM) systems provide real-time analysis of the security alerts generated by applications and network hardware. This addresses the requirements of Objective C in immediate and practical ways:

C1
Security Monitoring

SIEM systems continuously monitor network traffic and user activity. They collect logs from various sources, including firewalls, servers, and endpoints. This centralized log management is crucial for detecting anomalies and potential security incidents.

Benefits:

- Real-time alerting on suspicious activities
- Aggregation of data from diverse sources for a comprehensive security view
- Automation of routine monitoring tasks, reducing the burden on security teams

C2
Analyzing Security Data

SIEM tools use advanced analytics and correlation rules to analyze security data. They can identify patterns that indicate potential threats, such as repeated failed login attempts or unusual data transfers.

Benefits:

- Correlation of events across different systems to identify sophisticated attacks
- Use of machine learning to improve threat detection accuracy
- Historical data analysis to understand trends and prevent future incidents

C3
Regular Testing and Tuning

For detection capabilities to remain effective, they must be regularly tested and fine-tuned. SIEM solutions provide insights into the performance of detection rules and allow for course adjustments based on evolving threats.

Benefits:

- Continuous improvement of detection rules and policies
- Simulation of attack scenarios to test detection capabilities
- Feedback mechanisms to enhance the SIEM system's effectiveness over time

C4
Ensuring Detection Coverage

A SIEM system helps ensure that detection coverage is comprehensive and aligned with the organization's risk profile. It integrates with other security tools and technologies to provide a unified view of the security landscape.

Benefits:

- Comprehensive coverage across the entire IT environment
- Integration with other security tools (e.g., IDS/IPS, antivirus)
- Customizable to align with specific organizational risks and priorities

Three key take aways:

1. **The UK's NCSC Cyber Assessment Framework provides a robust structure for managing cybersecurity risks**
2. **Objective C focuses on the detection of cybersecurity events, a critical component of any security strategy**
3. **SIEM systems are invaluable in achieving the goals of Objective C by providing real-time monitoring, advanced data analysis, regular testing, and comprehensive detection coverage**

By integrating a SIEM solution, organizations can significantly enhance their ability to detect and respond to cyber threats, thereby aligning with the NCSC's guidance and improving their overall security posture.

Want to learn more?

Contact Logpoint partner ITB Ltd at solutions@it-b.co.uk and accelerate your CAF journey today.

About Logpoint

Logpoint is the creator of a reliable, innovative cybersecurity operations platform — empowering organizations worldwide to thrive in a world of evolving threats. By combining sophisticated technology and a profound understanding of customer challenges, Logpoint bolsters security teams' capabilities while helping them combat current and future threats.

Logpoint offers SIEM, UEBA, SOAR and BCS technologies converged into a complete platform that efficiently detects threats, minimizes false positives, autonomously prioritizes risks, responds to incidents, and much more.

Headquartered in Copenhagen, Denmark, with offices around the world, Logpoint is a multinational, multicultural, and inclusive company.

For more information, visit: www.it-b.co.uk

For more information on CAF, visit: https://www.ncsc.gov.uk/collection/cyber-assessment-framework.