TrustBroker Africa (TBA) IV - SIM3 Auditor Certification Training Report

Introduction

The TrustBroker Africa (TBA) IV - SIM3 Auditor Certification Training, held over four days, provided participants with a comprehensive understanding of the SIM3 (Security Incident Management Maturity Model) framework and its practical application for CSIRT (Computer Security Incident Response Team) auditing. The training also featured an introduction to Shadowserver and its tools for threat intelligence generation and brought together participants from several institutions, including :

Below is a detailed report on the key sessions from each day.

Day1: 14 oct. 2024 Introduction to SIM3 and Organisational Parameters

The first day began with a formal opening and an introduction to the SIM3 (Security Incident Management Maturity Model) framework, as well as the Open CSIRT Foundation, which plays a central role in promoting security response standards. The session aimed to familiarize participants with the purpose and objectives of SIM3, emphasizing its significance in measuring and improving the maturity of CSIRTs. This foundational knowledge helped participants understand how SIM3 fits into the broader context of organizational security strategy.

Following the introductory session, the focus shifted to the **SIM3 Organisational Parameters**. These parameters highlight the structural elements necessary for a CSIRT to function efficiently, such as governance, funding, leadership, and the division of responsibilities. Participants explored how these factors influence the maturity and effectiveness of incident response teams. They also discussed various real-world scenarios where organizational structure plays a crucial role in responding to cyber threats. The day concluded with an in-depth examination of these parameters, setting the groundwork for further exploration of SIM3 components in the following days.

Day2: 15 oct. 2024 SIM3 Human and Tools Parameters

The second day opened with a session on **SIM3 Human Parameters**, which focus on the people who operate within a CSIRT. The session delved into the critical role that skilled personnel play in effective incident response. Participants learned about the competencies required for different roles within a CSIRT, from front-line responders to management, and how these roles contribute to overall maturity. This session underscored the need for continuous training and development to ensure that the team stays current with evolving cybersecurity threats. Through discussions and case studies, participants analyzed the challenges of building and maintaining a high-performing incident response team.

After a break, attention turned to the **SIM3 Tools Parameters**. This session covered the technical tools and infrastructure necessary to support the functions of a CSIRT, such as monitoring systems, ticketing solutions, and incident tracking tools. The trainer emphasized the importance of selecting the right tools that align with an organization's maturity level and how these tools facilitate faster and more accurate responses to security incidents. Participants were introduced to real-world examples of tools and solutions used by mature CSIRTs, providing practical insights into selecting, implementing, and managing these technologies. The day ended with an initial discussion on **SIM3 Process Parameters**, setting the stage for a deeper dive on the following day.

Day3: 16 oct. 2024 SIM3 Process Parameters and Becoming a SIM3 Auditor

The third day resumed with a detailed examination of the **SIM3 Process Parameters**, which outline the key operational procedures and workflows for managing incidents. Participants explored various processes, including detection, response, recovery, and reporting. These parameters are vital for ensuring that a CSIRT can handle incidents efficiently and consistently. The session also discussed how to document and improve these processes to achieve higher maturity levels. Participants engaged in group discussions and scenario-based exercises, which helped them better understand how to streamline incident management processes within their own organizations.

Participants then explored how to utilize Shadowserver's datasets, focusing on metrics such as **Scan/Device Attack Surface, Honeypot Sensors, and CVE Severity**. Using the **Shadowserver Dashboard**, participants were shown how to generate CTI reports that can provide actionable insights into their network's vulnerabilities. The session also included demonstrations on how to incorporate these data feeds into daily incident response processes, allowing participants to understand the real-world impact of Shadowserver's intelligence.

In the afternoon, the focus turned to advanced CTI applications, specifically the use of Shadowserver data to monitor **Sinkhole infections, Compromised Devices, and Exposed/Attacking Devices**. Participants were guided through hands-on exercises, navigating the Shadowserver Dashboard and applying this data in a **cyber incident case study**. Led by the tutor, this scenario-based exercise provided practical experience in analyzing threats and responding to incidents using the intelligence gathered from Shadowserver feeds. The day ended with participants successfully demonstrating their ability to apply what they had learned to real-world cybersecurity incidents.

Conclusion

The TrustBroker Africa (TBA) IV - SIM3 Auditor Certification Training was a comprehensive blend of theory and practice, providing participants with a thorough understanding of the SIM3 framework and the skills needed to audit CSIRTs effectively. The integration of Shadowserver into the final day's sessions added a valuable practical component, equipping attendees with the tools to generate and utilize cyber threat intelligence. By the end of the training, participants were well-prepared to implement and audit SIM3 processes in their organizations, enhancing their incident management capabilities and contributing to a more secure organizational environment.

Annex

Annex 1

Group photo of Participants with trainer SIM3, Don

Group photo of Participants with Shadowserver trainer, Jon Flaherty