

#### **Blue Team 2 Objectives (BT2Os)**

**Cyber Threat Intelligence**

Report Author: Christen Reinhart | Thierry Tran | Edwin Pretel | Michael Roberts

Report Date: 3/14/2024

**Blue Team Guardians**

BTO1: Construct Initial Threat Model and Perform STRIDE Analysis

Action: Utilized the Microsoft Threat Modeling Tool to create a Data Flow Diagram (DFD) that maps out the SimCorp system architecture, highlighting critical components like the web server hosting SimCorp's web application. Additionally the link is below for the complete report.

STRIDE Analysis: Analysis is in link below and each component within the DFD for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege threats. This analysis identified critical vulnerabilities such as spoofing attacks against human users and the thick client, data tampering possibilities, and elevation of privilege through brute force attacks.

BTO2: Deploy Additional Threat Detection Tooling

Action: Integrated advanced monitoring solutions like AWS GuardDuty and enhance the use of Splunk Enterprise and Zeek for deeper network analysis. Deploy additional Intrusion Detection Systems (IDS) and installed Splunk forwarders/ agents for layered defense monitoring mechanisms.

BTO3: Configure Methods of Detection

Action: Developed and refined IDS rules to detect unusual login attempts, brute force attacks, and reconnaissance activities. This includes configuring WAF settings to prevent XSS and other web-based attacks targeting the web server hosting SimCorp's web application.

BTO3a: Implement Detective Controls for Key Assets

Action: For the web server hosting SimCorp's web application, implemented detective controls such as real-time traffic monitoring, anomaly detection algorithms, and log analysis to detect and alert on suspicious activities.

BTO4: Observe Adversarial Actions and Collect Evidence

Action: Continuously monitored network traffic and system logs to identify adversarial actions. Document evidence of scanning activities, TTPs, and any anomalies that suggest a deviation from normal behavior. Utilize tools like Splunk for log analysis to compile comprehensive evidence of the attack patterns and IOCs. This is displayed in the incident reports linked below along with our cyberthreat timeline.

BTO5: Implement Scripted Automation for Alerting

Action: Developed scripted automation that utilizes the capabilities of Splunk, Cloudwatch and GuardDuty, combined with custom scripts(Lambda), to analyze logs and network traffic in real-time. This automation should trigger alerts based on predefined indicators of compromise (IOCs) and anomalous behavior indicative of adversarial activity. This could include repeated login failures, unusual outbound traffic, and patterns consistent with reconnaissance.

These targeted actions and strategies, aligned with the Blue Team Objectives, leverage the insights gained from the STRIDE analysis and incident reporting to fortify SimCorp's cybersecurity posture. By addressing the identified vulnerabilities and implementing robust defense mechanisms, SimCorp can enhance its resilience against ongoing and future cyber threats.

Reference

[Stride Report](<https://docs.google.com/document/d/1UQukIQ9ScEVJvBkVB4NXG6SSKMVP9JRtrEL9gu85zhM/edit?usp=sharing>)

[Comprehensive Cybersecurity Threat Report](<https://docs.google.com/document/d/1TqUUDoLmZ8KFwpQ0UjEeiSPiuYNf09Tc9ve_bI6oAb8/edit?usp=sharing>)

[Threat Model](<https://docs.google.com/document/d/1SB70Cthk3Dkph8M9zJ44O9naEWofPipEHfG45IGrXOI/edit?usp=sharing>)

[Threat Report1](<https://docs.google.com/document/d/1aevjFTVWqp7lrjTR01WCpAnWDXo0kMJw2KjuX0j_u30/edit?usp=sharing>)

[Threat Report2](<https://docs.google.com/document/d/1NpR03PktGIbq7RJs6_EevIQ0KBmFwKPYK94bXjl_5BY/edit?usp=sharing>)

[Threat Report3](<https://docs.google.com/document/d/1lN6ItpfLaLMY2t4oVk6HVFIdniNwXWGnFyZ_A8mp56k/edit?usp=sharing>)

[Threat Report4](<https://docs.google.com/document/d/1lMVQJTaXd1sGw8PuqPQYVhbxEUYmAId9Bw6ESPfbqRU/edit?usp=sharing>)

[OWASP](<https://owasp.org/www-project-top-ten/>)

[MITRE ATT&CK](<https://attack.mitre.org/>)