SIEM Glossary

This document is designed to cover acronyms and terms used in the SIEM domain of the Blue Team Level 1 certification training course.

This document is TLP:White, and can be shared without breaching the Terms and Conditions of the BTL1 course.

Learn more about Blue Team Level 1 and purchase the certification here – https://securityblue.team/why-btl1/

SEM // Security Event Management – SEM is a process that can come in the form of security software specialized in the identification, collection, monitoring, evaluation, notification and correlation of real-time of events and alerts from different log sources, such as workstations, intrusion detection and prevention systems, antivirus software, firewalls, etc.

SIM // Security Information Management – SIM is a process that can come in the form of specialized security software that helps with the collection, monitoring, and analysis of data and event logs generated from endpoints and security devices in a network such as intrusion detection and prevention systems, antivirus software, firewalls, etc.

SIEM // Security Information and Event Management – A software solution that aggregates and analyzes activity from different resources across an organization's entire IT infrastructure. SIEM is a combination of security information management (SIM) and security event management (SEM) that uses rules and statistical correlations to help organizations detect threats and turn log entries, and events from security systems, into actionable information.

Log // A log is data that is produced by systems, applications, services, and other processes, generating an output that states what actions have been taken. An example of a log is when a user logs into a Windows system, the operating system will make a note that a user has logged in and record it.

WEL // **Windows Event Logs** – Windows Event logs or Event Logs are files in binary format (with .evtx extension) stored locally in the Windows directory of a computer. These logs keep a detailed record of anything that happens on a Windows system, from users logging in to program execution. We can use these logs to monitor what happens on Windows endpoints.

Sysmon // **System Monitor** – Sysmon is a Windows system service and device driver that monitors and logs system activity to the Windows event log, but can provide more valuable information than standard Windows Event logs

Regex // **Regular Expression** – Regex is a string of text that allows you to create patterns that help match, locate, and manage text. Regular expressions can also be used from the command line to find and sort specific files or data on a system.

API // **Application Programming Interface** – An API is an interface that allows interactions between multiple software instances, managing different calls and requests that can be made. If we had access to the API for our SIEM product, we could query the SIEM to retrieve information which can then be used to power dashboards, visual displays that regularly make API requests to fetch data and update the graphs to reflect metrics such as firewall allows or denies, number of login failures, number of alerts generated in the past 24 hours, and more.