# Log Collection Analysis & Review

By: Ryan Stewart

## SIEM Introduction

Security Information and Event Management (SIEM) is a robust security solution designed to collect, interpret, and analyze data within an organization to identify potential threats. SIEM enables **real-time** monitoring of security threats, providing a proactive approach to cybersecurity. By the end of this training, I will have a general understanding of:

- How SIEMs operates
- Log collection mechanisms
- Log storage processes
- Alert creation methodologies

## SIEM Product

The market offers a plethora of SIEM solutions, with the most successful commercial options highlighted in the Gartner 2021 report, as depicted below:


Source: Gartner (June 2021)

## SIEM and SOC Analysts

SOC analysts play a crucial role in reviewing potential threats detected by SIEM. **For instance, alerts featured on the LetsDefend Monitoring page exemplify notifications generated by SIEM in action.**