

Often Used Acronyms

ReliaQuest SOC

MSSP – Managed Security Service Provider

MDP – Managed Detection and Response

What's the difference? See <https://www.msspalert.com/cybersecurity-news/mdr-vs-mssp-security-services-whats-difference/>

M&A – Mergers and Acquisitions

CISO – Chief Information Security Office

CAM – Cyber Analysis Methodology

IDS – Intrusion Detection System

SIEM – Security Information and Event Management

EDR – Endpoint Detection and Response (**EDR**) is a cybersecurity technology that addresses the need for continuous monitoring and response to advanced threats. It is a subset of endpoint **security** technology and a critical piece of an optimal **security** posture. ... Many **EDR** tools, however, combine **EDR** and EPP.

SOAR - (*Security* Orchestration, Automation and Response) is a solution stack of compatible software programs that allow an organization to collect data about *security* threats from multiple sources and respond to low-level *security* events without human assistance.

UEBA - (User and Entity Behavior Analytics) enables *security* teams to proactively monitor for high risk behavior inside the enterprise.