XDR VERSUS SIEM

THIS IS XDR

WHAT IS IT?

XDR is a new acronym and stands for Extended Detection and Response. It is considered the evolution of existing threat detection & response solutions.

WHY SHOULD I CARE?

It applies proactive measures by providing visibility of data across endpoint, network and system components in combination with analytics and automation.

THIS IS HOW IT WORKS

By collecting and analyzing data from multiple sources, XDR solutions are able to better validate alerts, thereby reducing false positives and increasing reliability. This helps reduce time you might waste on inaccurate alerts.

WHO IS IT FOR?

XDR helps security teams to address incidents by centralizing, normalizing and correlating security data from multiple sources.

WHEN DOES IT MAKE SENSE?

If your goals are to increase detection accuracy by correlating threat intelligence and signals across multiple security solutions, and improved security operations efficiency and productivity, then XDR is for you.

THIS IS THE DIFFERENCE

FACT 1

XDR is a system that provides realtime coordinated protection and a deep focus on incident response.

FACT 2

SIEM collects data and gives you a view across your whole enterprise to detect, investigate and respond accordingly.

Credits

This poster was created by Patrick in collaboration with Heike Ritter.

To learn more about Microsoft's XDR & SIEM solution, visit aka.ms/SIEMandXDR

AFRAIT

THIS IS SIEM

WHAT IS IT?

SIEM is another acronym and stands for security information and event management to help you gather insights from your environment.

WHY SHOULD I CARE?

The main purpose of SIEMs is to collect and aggregate data such as logs from different tools and applications for activity, visibility and incident investigation.

THIS IS HOW IT WORKS

At its core, SIEM is a data aggregator, search, and reporting system. SIEM gathers immense amounts of data from your entire networked environment, consolidates and makes that data human accessible.

WHO IS IT FOR?

SIEM helps IT staff to identify, review and respond to security breaches faster and more easily as it gives more insights from different sources.

WHEN DOES IT MAKE SENSE?

If your goal is logging and log management, then security information and event management is for you. Another use case is to help in regards to compliance with regulations like HIPAA, PCI, SOX, and GDPR.