# CyberSecurity XDR: A Panacea for a Secure Virtual World


## Marcos Pinto

***Computer Systems Technology Department***



19th Annual City Tech
2021 Poster Session


## Introduction

Cybersecurity XDR (eXtended Detection and Response) is a cloud-based, on-demand service, that integrates multiple security products into a cohesive security operations system

## XDR Development

. Identify all types of stored data
. Where information is stored
. List network hardware/software
. Train employees/users on cybersecurity best practices
. Conduct Penetration Testing and Risk Assessments

## XDR In-Action

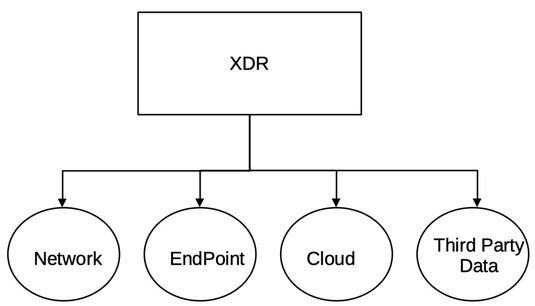
XDR depends on SIEM and SOC.

SIEM( Security Incident Event Management): System that collects and analyzes aggregated log security data

SOC(Security Operations Center): People, processes and technology designed to deal with security events picked up from the SIEM log analysis.

An incident responder determines a threat or a bona fide security event: identify the action to take and deploy the proper remediation.

## XDR Operation




XDR unifies prevention, detection, investigation, and response in one platform for unrivaled security and operational efficiency for networks, endpoints, clouds, and third party data.

## XDR Knowledge-Base

. Cryptography
. Access control mechanisms
. Authentication models
. Security models
. Operating systems security
. Malicious code
. Security-policy formation and enforcement
. Vulnerability analysis
. Evaluating secure systems