Cetas

Hybrid XDR:

The Modern Threat Detection Hub

XDR

www.cetas.ai | info@cetas.ai | 586-789-9878

Background

The traditional approach to cybersecurity monitoring can best be described as a categorized set of tools each providing their own set of alerts i.e. EDR and UEBA. While the SIEM stands out in its log management capabilities, it often falls short in detection and response due to the high level of burden it places on SOC resources and expertise. Furthermore, the disjointed nature of these tools leads to a lack of streamlined case management and response. This experience is inefficient, duplicative and overwhelming to a SOC, and the lack of cohesiveness between the different phases of the security operations lifecycle is the leading cause of a detrimentally high mean-time-to-response (MTTR). As data volume and complexity continues to increase, the security operations experience of today deserves a modern platform that synthesizes the activities of detection, correlation, incident creation, and remediation into a single interface.

Hybrid XDR

Forrester defines the hallmark capabilities of an effective Extended Detection & Response (XDR) tool as the following:

1. Correlation Across Telemetry to Provide a Single Incident
2. Automation of Root-Cause Analysis
3. Automation of Response Recommendations
4. Enablement of Visibility Across Tools into a Single Place
5. Lowers the Barrier to Threat Hunting

Let's take a closer look at what these mean.

Correlation Across Telemetry to Provide a Single Incident

A true XDR should autonomously be able to tie alerts together into a common identity profile. Another way of viewing this is as a threat story that is abstracted by MITRE ATT&CK categories to create a chronological understanding of the alerts comprising an incident. It is also imperative that a modern XDR is cloud native and capable of obtaining data from cloud services. Automated correlation of cloud data sources to detect abnormal behavior in the usage of critical cloud resources is required. The Cetas Autonomous Incident Responder (AIR) automates this correlation of alerts into a single incident through identity access management. By tying alerts back to identity, analyzing access in relation to a peer group, and displaying alert information in an incident in a chronological timeline view, Cetas AIR creates a central hub to detect and respond to any threat confidently and quickly.

Automation of Root-Cause Analysis

Another defining factor of the modern XDR is the ability to automate root-cause analysis to thoroughly define the scope of an incident. An XDR should be able to contextualize alerts by explaining how likely they are to be malicious. To take this a step further, a highly advanced XDR will be able to tell you the probability of an attack progressing to a future, more severe stage. With all of the analytics and detections visible through a single virtual pane of glass, the Cetas XDR can show information such as which systems were exploited and tie that back to vulnerability data. Along with the analytics we provide on the same timeline view for each incident, we are able to give analysts what they need to respond confidently and quickly.

[1] *Forrester. Mellen, A. (2021). Adapt or Die: XDR is on a Collision Course with SIEM and SOAR.*

Automation of Response Recommendations

A modern XDR must be able to streamline response by having the capability to recommend the proper next step. This capability is best achieved if the platform has the ability to integrate with the identity management source so that action against a malicious entity can be done within the XDR itself. After the Cetas AIR autonomously creates an incident, the prediction engine will then show an incident responder how an attack will progress if unmitigated. The incident responder now has information on which system or user was compromised along with risk score data to determine relatively how risky the actions from the incident were and what could occur as a result of those through the prediction engine.

Enablement of Visibility Across Tools into a Single Place

The two different classifications of XDR are native and hybrid (open). A native XDR will fit into a suite of existing security tools as an independent entity that will act in parallel to SIEMs, SOARs, UEBAs, and others. A hybrid or open XDR serves to complement these other tools in that it ingests logs from these sources to correlate them for deeper analysis. A Hybrid XDR can be thought of as consolidating these sources into a single detection hub. By 2023, Gartner projects 75% of cloud breaches will be due to access misconfigurations. The Cetas AIR vigilantly monitors configurations and access to all cloud applications, data stores, compute clusters, serverless containers, etc. to ensure that an organization isn't crippled by a configuration oversight.

Lowers the Barrier to Threat Hunting

Arguably the most significant aspect of a modern XDR is its ability to both lower the barrier to threat hunting and elevate the quality of experience for SOC teams. A powerful XDR will have an intuitive and streamlined UI to enable a less experienced analyst or incident responder to feel at ease as they work through the security operation lifecycle from detection to response. Ultimately, the XDR should improve the quality of life of SOC operators. As a company built by and for security practitioners, we at Cetas have strived to enable security operators to focus on what truly matters: rapid incident response and vulnerability remediation.

Summary

With all of the challenges modern infrastructure brings, it is imperative that detection and response tools are cloud-native and capable of automating the trivial aspects of security operations. An automated solution brings the benefit of detecting breaches and responding to incidents quickly so that the incident responder does not need to spend bandwidth on low-hanging fruit. Through augmentation, the Cetas AIR enables L1 analysts to perform like an L3 analyst and therefore allows a SOC to focus on the most complex security problems to ensure you are ahead of the attacker curve.

[1] *Gartner Research. Mezzera, P. (2020). Managing Privileged Access in Cloud Infrastructure.*