Cetas

Detection as Code

Simplifying the identification, implementation, and deployment of threat detections.

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

Overview

One of the biggest challenges in SecOps is understanding what vulnerabilities exist in modern digital infrastructure. In the past, designing security architecture meant implementing NIDS devices in strategic choke points throughout the network. However, due to modern complexity of serverless and public multi-cloud environments, detection engineering is not as straightforward.

While the SIEM has been used for this purpose, it is constrained by the SOCs ability to write complex detections. One can imagine a SIEM as a blank canvas and depending on the resources and expertise of the SOC, the end result can be a masterpiece or lackluster.

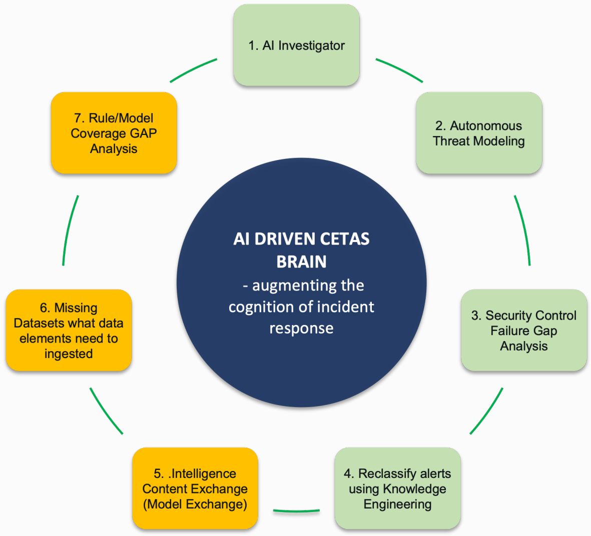
The task of understanding what detections to implement can be incredibly daunting and involves spending months understanding different tactics, tools, and procedures as well as the security configurations of applications and containers. Furthermore, understanding how to implement a detection, whether it be a rule or algorithmic model, requires an investment in time and expertise. In our experience, this is not feasible for many understaffed security teams with limited resources. A tool that provides complex and accurate models out-of-the-box is critical in achieving depth of functionality for detections.

Cetas XDR and vSOC

A lot of the inefficiency in threat hunting today is the manual process of configuring static rules and sifting through the mostly inconsequential alerts they output. The Cetas XDR was designed to be an artificial limb that automates the banal parts of an incident responder's cognition so they can free up bandwidth to focus on the more nuanced parts of threat hunting.

Take the common example of a user spiking in authentication failures to an application. Is this seemingly anomalous behavior worthy of creating an incident or is it actually a true negative? The analyst using a SIEM for threat hunting would lose valuable time by manually analyzing the associated logs.Through the combination of time-series analysis and machine learning, the AI-powered XDR provides the most rapid, accurate, and in-depth threat hunting capability in the cybersecurity toolspace. Highly accurate detections are combined with rich threat content where every model is mapped to stages in the MITRE and NIST security frameworks.

With much of the detection automated, Cetas XDR enables the analyst to quickly make an informed decision and take action on an incident before it increases in severity. Acting as an incident responder on shift 24/7, Cetas XDR augments the rest of existing security operations to unlock the full potential of the SOC--enabling L1 analysts to perform like L3 analysts.



AI DRIVEN CETAS BRAIN

- augmenting the cognition of incident response

1. AI Investigator

2. Autonomous Threat Modeling

3. Security Control Failure Gap Analysis

4. Reclassify alerts using Knowledge Engineering

5. .Intelligence Content Exchange (Model Exchange)

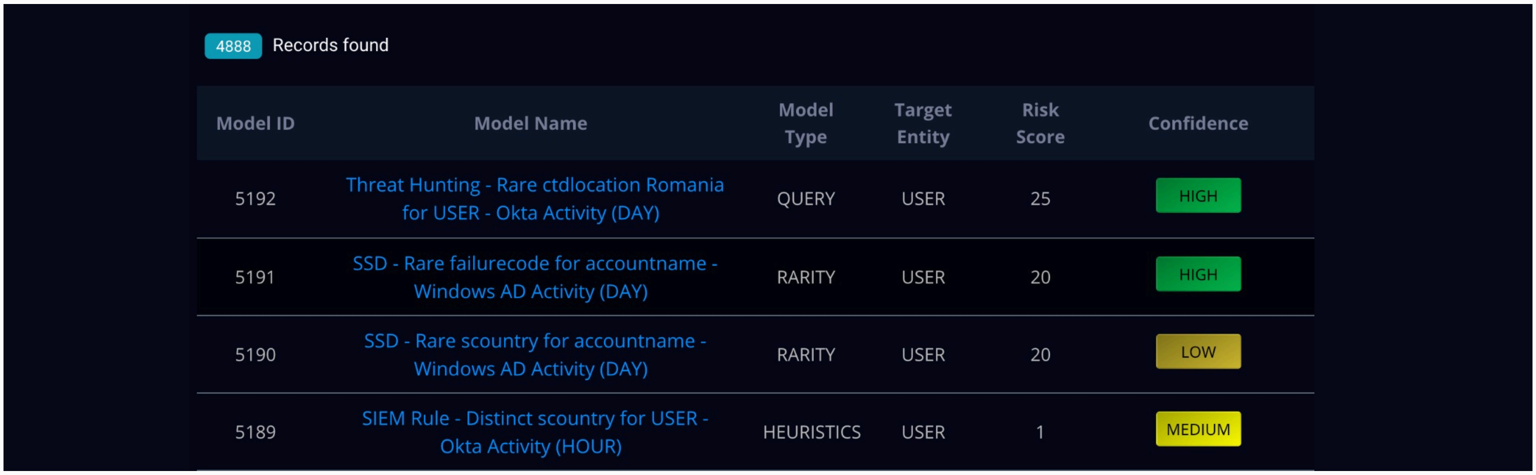
6. Missing Datasets what data elements need to ingested

7. Rule/Model Coverage GAP Analysis

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

Cetas ModelX

While having an out-of-the-box catalogue of threat content is a fine starting point, the reality is that existing detection solutions do not monitor vulnerabilities that might not exist yet in your environment. As a proactive measure, the Cetas Model Exchange, or ModelX, is a repository of detections we have found in other customer environments. If we determine the posture of an existing company is a match, we consolidate these learnings to be added sensors in your environment. For example, if you introduce Azure for data storage into your public cloud posture, we can include new detection models we have found from an existing customer who is also using Azure Blob Storage. This way, your security engineers do not need to spend time thinking about detections that we are already aware of. They can instead put on their creative hats and think of novel and more complex scenarios to be included.



4888 Records found

Model ID	Model Name	Model Type	Target Entity	Risk Score	Confidence
5192	Threat Hunting - Rare ctdlocation Romania for USER - Okta Activity (DAY)	QUERY	USER	25	HIGH
5191	SSD - Rare failurecode for accountname - Windows AD Activity (DAY)	RARITY	USER	20	HIGH
5190	SSD - Rare scountry for accountname - Windows AD Activity (DAY)	RARITY	USER	20	LOW
5189	SIEM Rule - Distinct scountry for USER - Okta Activity (HOUR)	HEURISTICS	USER	1	MEDIUM

Schedule a Demo Today!

https://www.cetas.ai/request-demo/

Cetas

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