Cetas

MITRE ATT&CK Use-Cases

Cetas has engineered a detailed catalogue of use-cases mapped to MITRE techniques. With ~95% coverage of known techniques, Cetas has been able to develop detections that provide explainable alerts across critical infrastructure.

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

Reconnaissance

Background

Reconnaissance is the first phase in a breach as laid out by the MITRE ATT&CK Framework. This is typically the planning phase for the attacker as they perform scans to get a lay of the land of the target network. Some of the details they might be scoping out include infrastructure (both on-premise and cloud) details as well as user information. Once the attacker has identified his targets and mapped out a plan, they will likely attempt to gain initial access through a phishing campaign or leaked credentials.

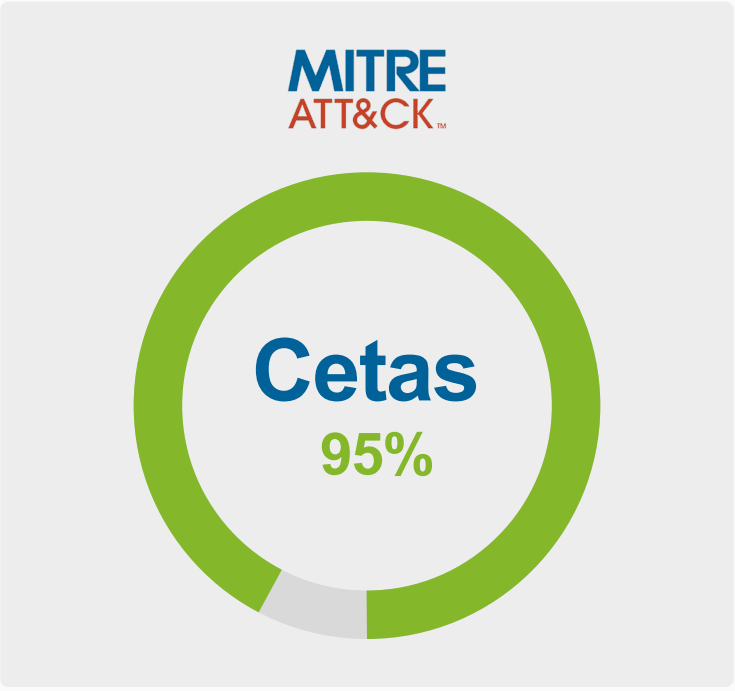
Cetas Threat Hunter Detection

The Cetas Threat Hunter has the ability to detect potential enumeration of system details, such as which ports are open by correlating rarity detections with threat intelligence to determine if an external system is indeed performing reconnaissance. Since email addresses are fairly easy to guess and often used in whole or in part as user IDs, an attacker will also attempt to gain credential information by attempting brute force logins. The Threat Hunter can determine spikes in authentication attempts on a single or various systems to flag a user account. The Threat Hunter will also perform peer-group analysis if other user accounts are exhibiting similar behavior over an overlapping time period.

Remediation

By providing alerts on these typical reconnaissance activities, there are a number of mitigation steps that can be taken. In the case where we see port enumeration from an external system, we will predict and show the next likely action that will occur if that system does in fact have an infrequently used port open. This signifies that the attacker can exploit that port with known techniques so by showing this in real-time, the system can be patched before the attack has chance to escalate. If a user account is displaying anomalous behavior such as attempting to access multiple systems repeatedly without success, then this account owner can be informed to strengthen their password or the account can be outright blocked if we observe a successful login preceded by a long string of failures.

Cetas MITRE Coverage



Account Compromise

Background

Once an adversary performs reconnaissance and establishes which accounts to leverage for further attack operations, they then proceed to compromise the targeted accounts. The type of accounts an attacker will aim for are usually highly privileged to avoid raising alarms when doing things like creating accounts or access tokens. Typically, account compromise is carried out through socially engineered phishing campaigns that lead to an employee installing malicious software from their emails. The contents of this software are a series of scripting commands that give the attacker a foothold to execute further commands remotely. Unless the executed file is immediately detected by an EDR tool, the attacker is free to progress due to limitations of existing detection capabilities.

Cetas Threat Hunter Detection

If software like VirusTotal fails to flag a malicious file as a true positive, Cetas Threat Hunter which comprises over 2000 models is capable of detecting any immediate action taken by the attacker to leverage a user account. These models are a combination of heuristics, time-series analysis, and machine learning algorithms that detect 99% of the tactics and techniques highlighted by the MITRE ATT&CK and NIST frameworks.

One example of Cetas' endpoint detection capability is the use of natural language processing to find probabilistically matching patterns of known malicious executables with files downloaded by a user. After looking at a massive volume of publicly available blacklisted malicious and benign file names, the Threat Hunter is able to classify a file at greater than 99% accuracy. Another example is Cetas' ability to determine land-speed violations which exist if a user account is logging in from various geographical locations over a period of time that would be physically impossible. Beyond these two examples, the Cetas Threat Hunter uses a variety of Boolean conditions and time-series analysis to further enhance its degree of visibility across all identities and assets.

Remediation

Beyond making detections, an incident responder can further enhance the case from action by the predictions the Cetas Digital Incident Responder makes. Since every alert is mapped to a kill-chain phase, we are able to provide a probability of outcome for where the attack is heading next. This is meant to give the incident responder greater confidence in taking action and triage an incident much quicker than the standard manual process. Based on the risk score of the user account, Cetas can automatically generate an incident with an associated virtual playbook appropriate for remediation on a compromised user account.

Model Coverage by MITRE Tactic

Tactic Name	Count of Techniques + Sub-Techniques	Coverage by Cetas	Count of Use-cases in Cetas Library
Initial Access	19	100%	100+
Execution	28	100%	100+
Persistence	93	100%	150+
Privilege Escalation	87	100%	150+
Defense Evation	135	100%	200+
Credential Access	46	100%	100+
Discovery	35	100%	100+
Lateral Movement	21	100%	75+
Collection	31	100%	100+
Command and Control	35	96%	100+
Exfiltration	16	100%	50+
Impact	26	95%	50+

Privilege Escalation

Background

Once an account is compromised, the attacker needs to gain higher-level privileges in order to access sensitive data from an application or data store. Typically, the attacker will attempt to gain root access by getting administrator rights by either compromising a local admin account, compromising a domain/central repository admin account, or elevating the access level of the compromised account. If the attacker is able to gain elevated privileges on a system, then nothing is preventing them from gaining credentials to a privileged user account of a system containing sensitive data to perform lateral movement and eventually data exfiltration.

Cetas Threat Hunter Detection

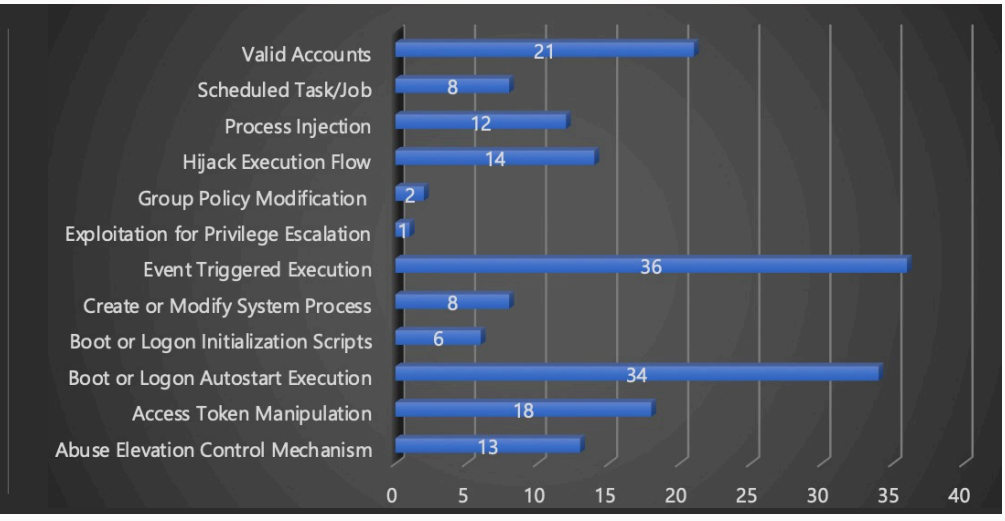
With application breaches overwhelmingly due to excessive privileges, The Cetas Threat Hunter is able to detect privilege escalation techniques by vigilantly monitoring the level of access of all user accounts across hosts, SaaS applications, as well as data and code repositories. With Cetas' probabilistic rarity and spike models some sample detections we are able to make include determining abnormal additions or deletions of user accounts from a security group and increase in authentication token requests by a highly privileged account. By correlating behavior such as this with patterns of reconnaissance and account compromise.

Remediation

Now that a detection has occurred for privilege escalation, the next step is to perform case management and incident prioritization for the incident responder to mitigate the damage quickly. The Cetas Digital Incident Responder autonomously connects sets of alerts into incidents which are then scored based on aggregate score of the weighted alerts that comprise them. The alerts with these incidents are represented in a chronological timeline view with analysis on each such as peer group analysis, previously observed false positive rate, and a prediction for the next likely alert to take place.

Privilege Escalation Tactic Coverage

Number of Models per Tactic



Data Exfiltration

Background

The last stage in an attack progression, data exfiltration, is when an adversary is able to steal data by transferring it out of the organization, typically leading to the organization incurring massive financial and reputation penalties. The main reason why an adversary can progress this far is because existing security tools of that company failed to alert on a true positive while also likely bogging down analysts with a large number of false positives. Low-efficacy alerts are some of the most consequential pain points facing security operations today.

Cetas Threat Hunter Detection

If an attack were to progress this far, the Cetas Threat Hunter would give the entity in question the maximum risk score of 100 and create an automatic incident. A maximum risk score is very rare and is reserved to signal on-going loss in sensitive data. With the creation of an incident the analyst will be able to block any further activity from the user account on the respective UI profile. Additionally, if approved by the SOC, at high risk scores Cetas Threat Hunter can automatically remediate threats that appear to mitigate loss or spread of a threat throughout an environment.

Remediation

With the automatic creation of an incident due to highly scored violations, an analyst can immediately see the severity and priority level of this type of an event and take quick action without having to investigate further. They will be able to see exactly the volume of data that was exfiltrated, what type of connections were made to specific external command and control IPs, and which applications were affected. They will be able to automatically block a user account from the Cetas UI and have a clear understanding of the vulnerability points that were exploited for patching.

Schedule a Demo Today!

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

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