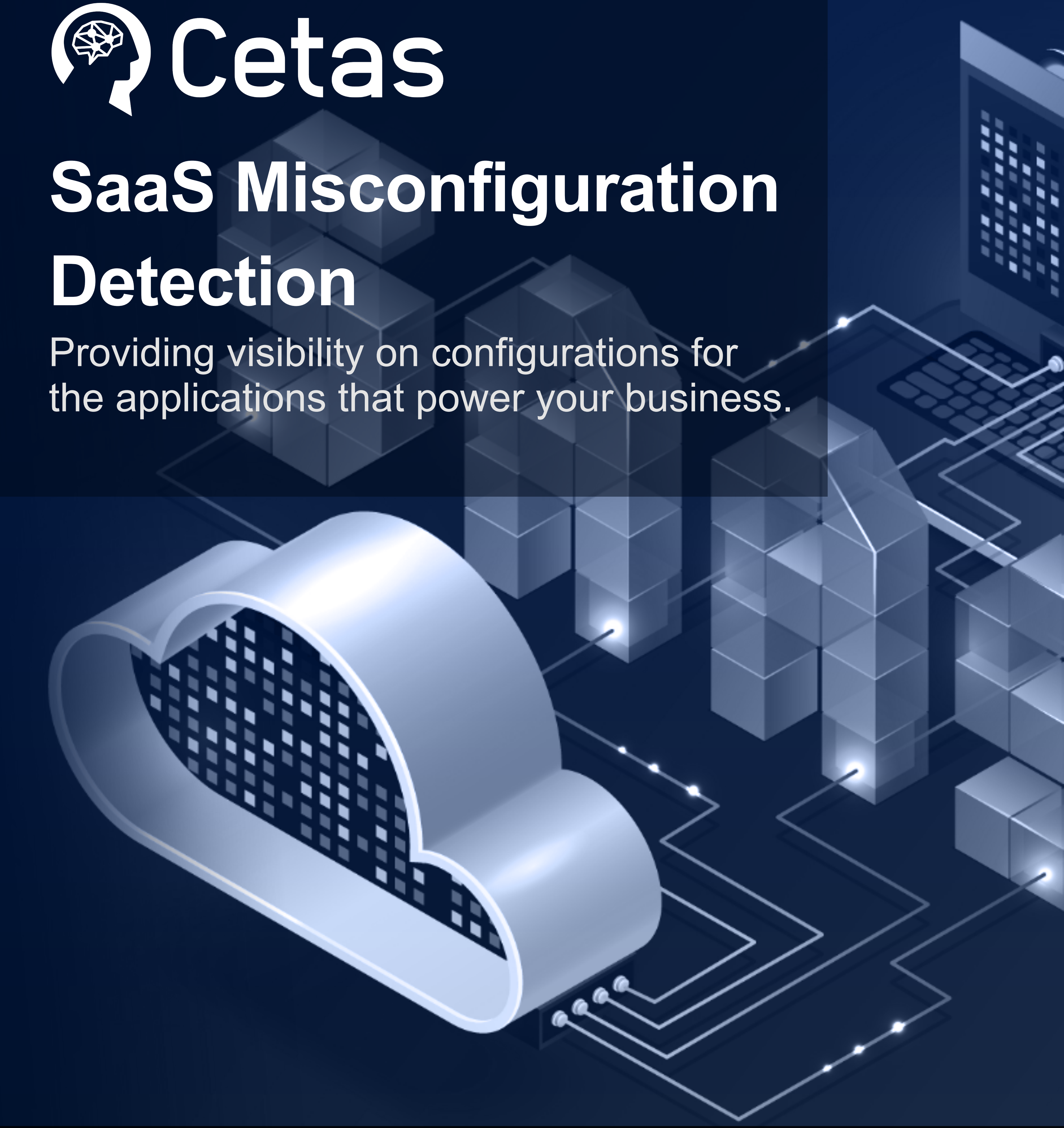
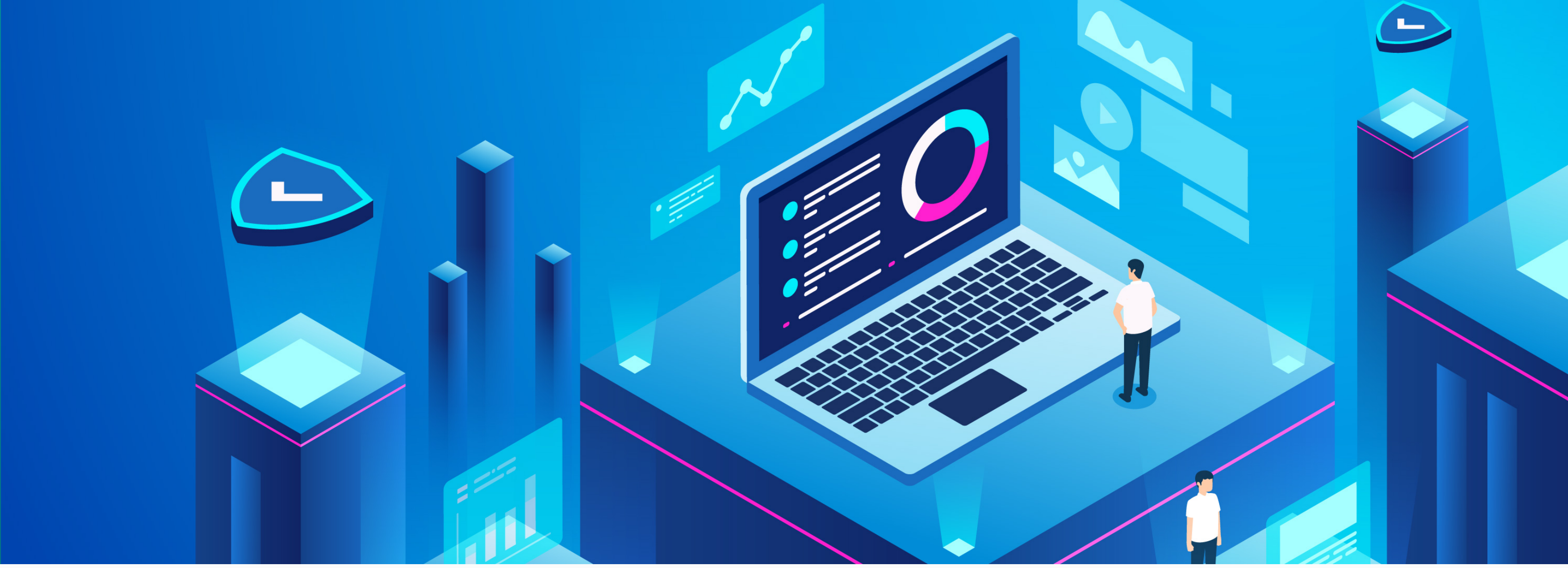
Cetas

SaaS Misconfiguration Detection

Providing visibility on configurations for the applications that power your business.





Background

For critical SaaS applications like Office 365, Github and Salesforce, the most glaring vulnerability is a lack of visibility of identity and access. In an on-premise system, monitoring all possible identities and points of access was already a challenge. With SaaS applications, this challenge increases in scale exponentially. SaaS applications are becoming more prevalent and more companies find themselves handing over responsibility of the application to someone ill-equipped to manage it. Untrained users leave errors like misconfigurations and inadequate authentication protocols in place. As a result, if a malicious actor were to exploit the lack of visibility and misconfigurations, all sensitive data in the ecosystem could be at risk. At Cetas, we see that SaaS is the future for many companies and want to provide a product that guarantees security. With the Digital Threat Hunter, we are able to mitigate the risk in your SaaS application posture by giving your analysts the visibility they need.

Cetas XDR and vSOC

Through a deep understanding of the configurable settings that exist across the most commonly used SaaS applications, we have been able to model what a safe security posture should be. The Cetas Brain, made up of a combination of deep and evolutionary learning, identifies probabilistic signals that suggest a deviation from the safe model which is then available for the SOC to triage. With automated incident creation and remediation steps available, the Cetas Incident Responder enables an analyst to intuitively and swiftly move through the process of closing a vulnerability. Our transferred learning mechanism allows the user to provide feedback on detections so that the platform learns about behaviors specific to the organization. Here are a few scenarios of how Cetas is able to identify seemingly innocuous misconfigurations:

Scenario #1: Microsoft O365 Identity Misconfiguration Detection

- Microsoft offers different applications in their service including Teams, Outlook, and SharePoint. Given all of these applications may contain sensitive information, the level of configuration and monitoring required is extensive.
- Unfettered access to a Teams or SharePoint folder opens the door to insider threats where a bad actor can ultimately exfiltrate data by either downloading it or sending files to a personal email.
- The Cetas Brain has 100+ models dedicated to O365 to provide both complete monitoring of all assets and identities as well as deep behavioral and statistical analytics to determine if abnormal behavior is occurring.
- One example of detectable abnormal behavior is as follows:
  - An employee may be concerned about their position and, as a result, act in bad faith. They may attempt to send information either to their personal email or to Dropbox. In either case, Cetas Brain is capable of identifying this behavior as anomalous, high risk, and give the analyst an immediate alert of the actions, why they are concerning, and how to remediate for the given situation.

Scenario #2 GitHub Identity Misconfiguration Detection

- One of the biggest misconfiguration challenges for CI/CD is improper admin access on GitHub. Lackadaisical access management can ultimately escalate to account compromise which can branch into more detrimental stages of an attack such as privilege escalation, lateral movement, or even data exfiltration.
- The Cetas Brain is able to detect real-time change in privilege and will immediately alert an analyst if this change is followed by actions such as the addition or deletion of a user on a repository.
- Through constant monitoring of every user's level of access across all repos, the Cetas Brain can quickly determine probabilistically rare behavior in real-time.

Conclusion

In summary, the only way to avoid the exploitation of a SaaS misconfiguration is through constant monitoring. As the enterprise continues to use more SaaS applications, each with their own unique configurations, the process of detecting abnormal user behavior manually is not a scalable solution.

With SaaS breaches usually the result of excessive privileges, Cetas mitigates access drift by monitoring who has access to what, which files are being shared externally, which third-party applications are accessing sensitive data, and who has admin access but likely doesn't need it.

The Cetas Autonomous Incident Responder (AIR) performs deep learning analysis across all of these vectors to let your team know, with confidence, if and when abnormal behavior is occurring. With Cetas, you can be assured of total visibility across your SaaS application posture to protect the tools that drive your business.

Schedule a Demo Today!

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

Cetas

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