Cetas

A guide on how Cetas can maximize your SOC investment

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

Background

According to a report from Ponemon, over half of respondents believe the ROI of a SOC is getting worse rather than better. As the world shifts further towards cloud, immutable infrastructure, and SaaS, companies' digital infrastructures are vast and extremely complex to secure. From 2020 to 2021, the average MSSP cost has increased by 20% and the need for more SOC analysts has continued to grow to compensate for the growing environments. Leaders in the cybersecurity world are under pressure to deliver better results with higher costs, more data to parse through, and against adversaries who are often supported by nation-states that continually develop increasingly sophisticated Tactics Techniques and Procedures (TTPs) to compromise a system.

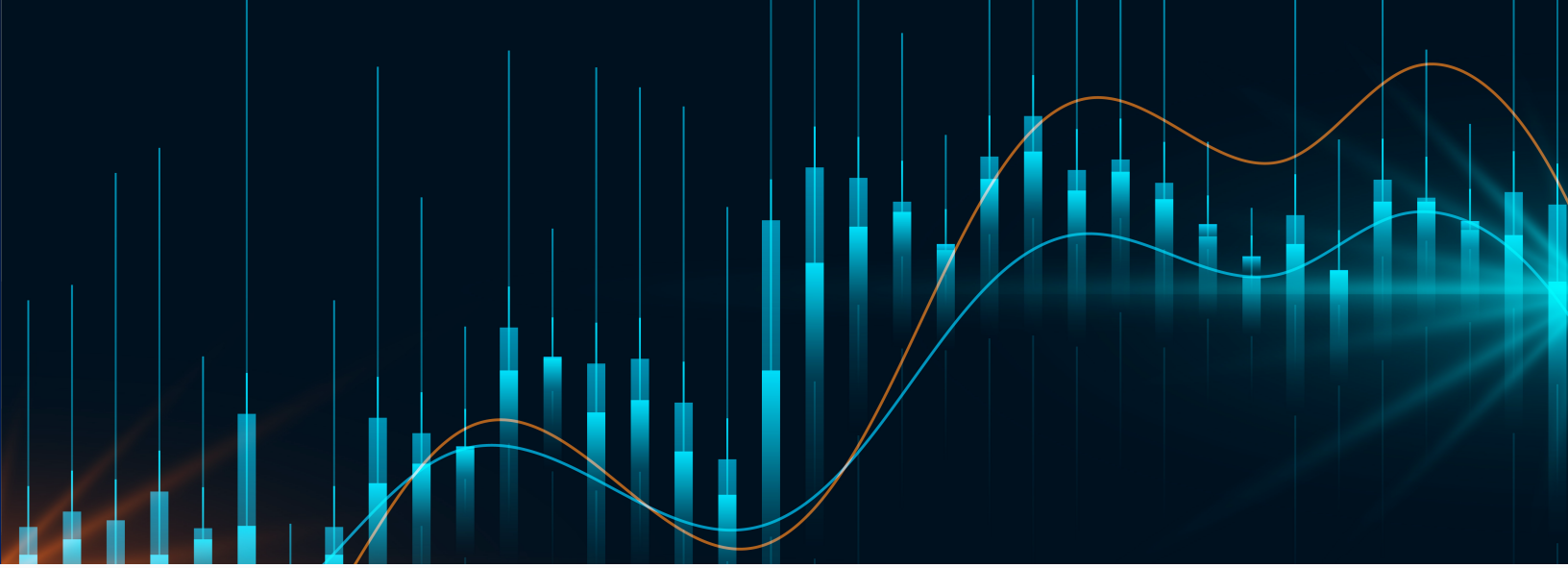
One-Stop Shop

To bring better value at a lower cost, Cetas works at a different angle than traditional approaches to addressing a SOC's concerns. Currently, a broad library of tools exists that allows an analyst to improve their ability to detect and address threats. These tools provide necessary capabilities while also creating a challenge for the SOC: analysts now need knowledge and understanding of a large variety of tools to be effective. Additionally, with the ever increasing scale of data needing monitoring, more analysts with these skillsets are required. Cetas works to make both of these issues a moot point through automation. The Cetas AIR integrates the functions of various different tools making it the one-stop-shop needed by any analyst. Automation provides risk scoring, auto-remediation, and predictive analysis to the analyst so they can see and do more in less time. These features make it so a SOC doesn't need to spend excessive time training analysts or require analysts to have extensive training prior to joining.

Sophisticated Detections

Additionally, Cetas continues to customize itself and provide efficiency improvement after unboxing through its various iterative methods. All results that analysts interact with provide the analyst opportunity to give feedback. This feedback is put through the Cetas Brain using machine learning algorithms so the system can learn how to improve its prediction capabilities and efficacy in threat detection overall. The system also uses these inputs along with statistical analysis to build and implement new rules. These rules work in conjunction with existing ones to contour specifically to the environment and its needs. On top of these automatically generated rules, Cetas AIR also provides the organization the ability to create custom rules if they find there are additional conditions they wish to apply in their environment. Cetas goes another step further and gives them threat hunting capabilities by allowing them to build custom dashboards and data visualizations to determine where issues might be and what needs to be done about them. These iterative features continually improve the security capabilities of Cetas AIR and allow analysts to prioritize meaningful tasks and work more efficiently.

[1]*Ponemon Institute. (2021). Second Annual Study on the Economics of Security Operations Centers: What is the True Cost For Effective Results?*



The Virtual Analyst

Prioritization and ability to improve efficiency makes all the difference in today's hiring climate. According to a study done by the Information Systems Security Association, 57% of cybersecurity professionals believe a lack of cybersecurity skills within their teams has impacted the organization they work for. The lack of skills has resulted in an increase in work for the remaining information security staff, of which 38% say they experienced burnout as a result of this increase. Truly shocking is that 39% of the 500 cybersecurity professionals surveyed stated that their organization is struggling to fill cloud computing security roles. The trends are clear. As technology expands an organization's infrastructure and the vulnerable workspace grows along with it, organizations are unable to fill roles quickly and consistently enough and as a result, those that are working are faced with more challenging working environments. By giving analysts the tools they require to focus on the real priorities, Cetas AIR can help bring the stress levels down and fill the gap left by the lack of available skill.

Conclusion

At the end of the day, all these features and tools work towards one goal, securing an environment against a breach. With tools that are currently in place, many breaches have occurred already and the rate of occurrences has continued to increase. In 2020, 1120 breaches occurred according to Lessons from Analyzing 100 Data Breaches. These breaches cost an average of $3.86 million per breach. By amassing all the functionality that Cetas AIR offers into one program, analysts can focus on the right alerts. They improve their mean time to response (MTTR) by avoiding the sea of false positives that come from the millions of data points ingested and, as a result, keep the organization secure.

[2] *Enterprise Strategy Group. Information Systems Security Association International. Oltsik, J. Lundell, B. (2021). The Life and Times of Cybersecurity Professionals 2021.*

[3] *IBM Security. (2020). Cost of a Data Breach Report.*

Schedule a Demo Today!

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

Cetas

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