TATA

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

#BeCyberReady

Feed Your SOC with Advanced Threat Intelligence

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

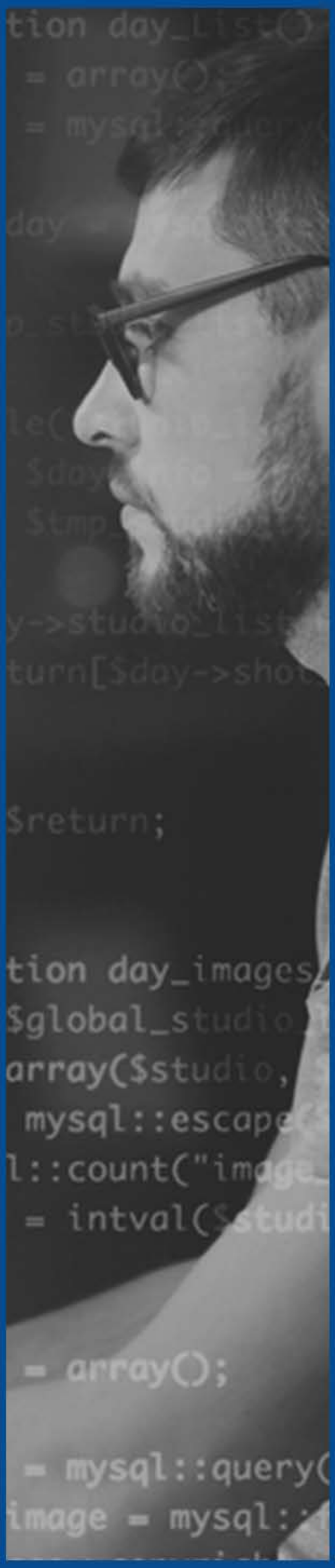
Why SOC Needs Threat Intelligence?

Growing security threats and the rising volume of related data are making the job of a Security Operations Center (SOC) cumbersome. In a survey conducted by Ponemon Institute in 2019, 53% of respondents reported that their SOC is ineffective at gathering evidence, investigating, and finding the source of threats. There may be several reasons for it. For instance, SOC professionals go through a heap of tasks that include log monitoring, incident response, compliance, alert management, recovery and remediation, root cause investigation, and much more. As a result of which, the number of tasks SOCs have to deal with is overwhelming, which in turn, making it difficult for the security teams to swim through the flood of alerts and prioritise them accordingly.

TATA

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE



Threat Intelligence – Utilizing Different Types of Threat Data

In order to turn the tide, organizations need to provide their SOC with some "threat intelligence" that can act as an antidote to most SOC analysts' troubles. With the help of Advanced Threat Intelligence, an organization can successfully withstand evolving threats, enable a more productive and engaged workforce, and fill the gap between end-user expectations and experiences, as well as enable SOC teams to work faster and smarter.

Threat intelligence provides organizations with valuable insights into the situational and contextual risks and the knowledge to effectively correlate data from several distinct sources to anticipate attacks before they occur. It helps SOC analysts to address the three most commonly faced issues:

Lowering the overwhelming volume of alerts

Due to alert fatigue, SOC analysts are often unable to review and investigate all the alerts on their own. They either chase false positives or ignore alerts.

Prioritization of incoming alerts

A major portion of the time spend by SOC analysts goes into responding to alerts generated by internal security systems, such as SIEM or EDR technologies. Determining if an alert is relevant and urgent requires gathering related information (context) from a wide variety of internal system logs, network devices, and security tools, and external threat databases. Searching all of these threat data sources is time consuming.

Collection of data from multiple sources to get the finest picture of an event

Threat intelligence provides organizations with valuable insights into situational and contextual risks. These insights are very useful while assessing organizational vulnerabilities and often leads to finding infection vectors as well.

TATA ADVANCED SYSTEMS
CYBER SECURITY PRACTICE

Benefits

Advanced Threat Intelligence plays an important role in improving the effectiveness of the SOCs of organizations of all sizes. It helps in processing the threat data to better recognize the attackers' TTPs, identify high-risk targets, respond quickly to security incidents, etc. In simple words, it is defined as evidence-based knowledge. With all such information in hand, an organization can tailor its defence and go way ahead of the cybercriminals.

Let's explore some key advantages of embedding advanced threat intelligence in the first line of defence.

- Provides in-depth information on what threats are most likely to affect the organization
- Exposes attackers' motives and their TTPs to help security teams make better decisions
- Empowers security professionals to understand threat actors' decision-making process
- Helps business stakeholders to invest wisely to mitigate risks and become more efficient
- Improved focus on protecting high-risk targets
- Quickens investigations for the incident response team
- Improves response time and remediation efforts

Towards The End

Modern day's threat actors utilize tactics and techniques that can wreak havoc in a very short period. These cybercriminals have a far reach irrespective of industry vertical or infrastructure classification. Taking this into account, we must implement a comprehensive threat intelligence program that allows organizations to aggressively address the constantly changing threat landscapes as a combined effort.