TATA COMMUNICATIONS

TATA

Cyber threats are inevitable

Is your business prepared?

Proven best practices for effective threat management

Index

01
Introduction

02
Why threat management is a top priority

03
Best practices for threat management

04
Unifying threat management with a platform-based approach

05
A five-step approach to effective threat management

06
Explore Tata Communications' Managed Detection and Response (MDR) Solution

Introduction

Threat management, also called cyber threat management, is a framework that cybersecurity experts use to keep track of a threat over its entire life cycle. The goal of a threat management strategy is to stay ahead of threats by finding them and responding quickly and correctly.

According to the 2020 State of SecOps and Automation report, 56% of large companies handle at least 1000 alerts per day. 99% said the alert volume created problems for their IT security teams and 93% said they could only address some alerts on the same day.[1] This trend has continued well beyond the pandemic.

56% **of large companies handle at least 1000 alerts per day**

99% **said the alert volume created problems for their IT security teams**

93% **said they could only address some alerts on the same day[1]**

Along with increasing complexity, skills shortage is emerging as a major concern. The role of cybersecurity professionals is very crucial as they have a significant impact on the overall culture of the industry. However, according to a study conducted by the Information Systems Security Association (ISSA) and the analyst firm ESG, most cybersecurity professionals need help maintaining the required skill sets.

Why threat management is a top priority

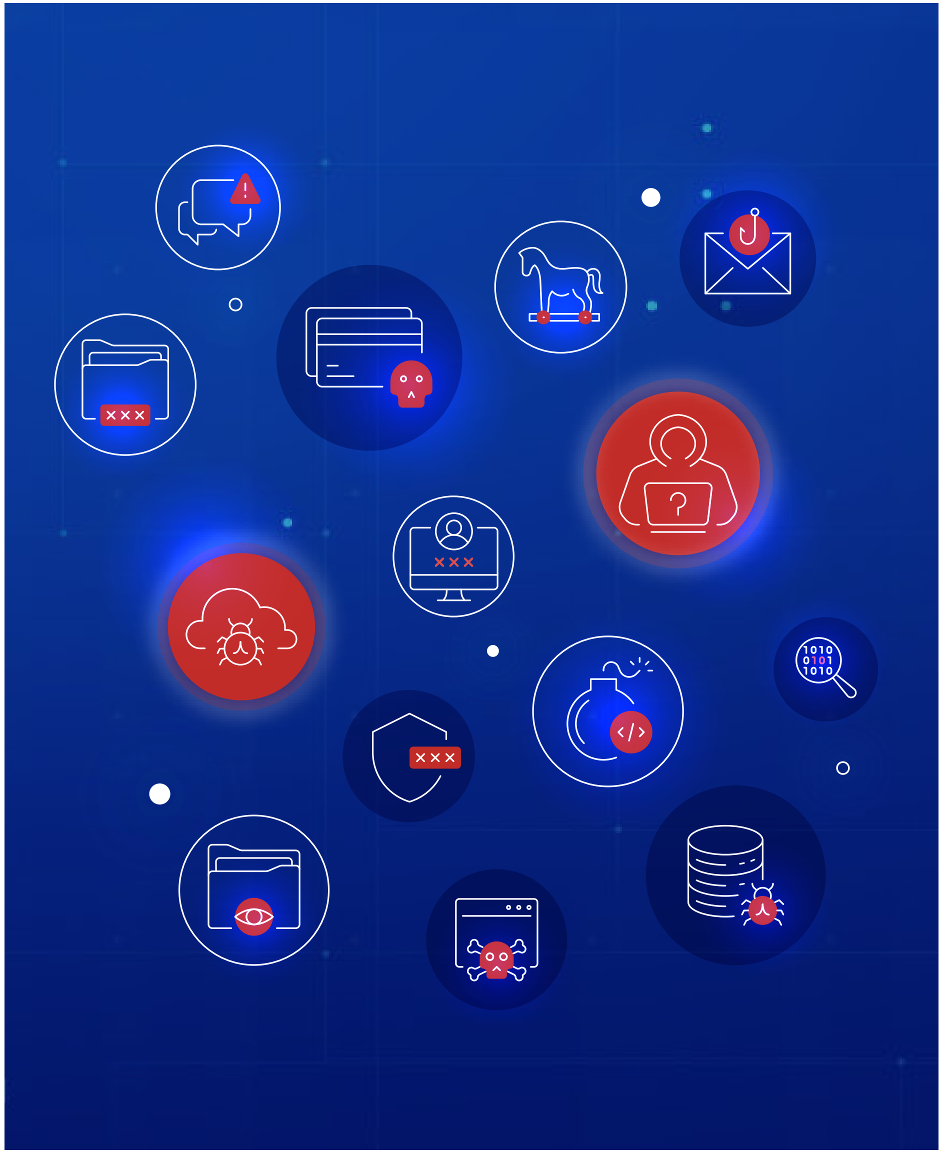
Businesses must keep a close eye on their security posture as the threat surface grows. Information fragmentation can create security blind spots, making it harder for teams to detect, prevent and respond to security threats. Mutating software, APT, insider threats and cloud-based computing service vulnerabilities are more than antivirus software can handle.

The 2022 Global Report on Insider Threats highlights a concerning trend of a 44% increase in insider threat incidents over the past two years. The Ponemon Institute's research reveals that the cost of data breaches has also risen by 2.6%, with the average cost increasing from USD 4.24 million in 2021 to USD 4.35 million in 2022.

In this volatile landscape, threat management is an important preventive measure that ensures data integrity. Threat management systems also enhance the collaboration between people, processes and technologies, giving organisations the best chance to detect threats sooner and respond more quickly.

The cost per incident has increased by more than a third to

$15.38 million



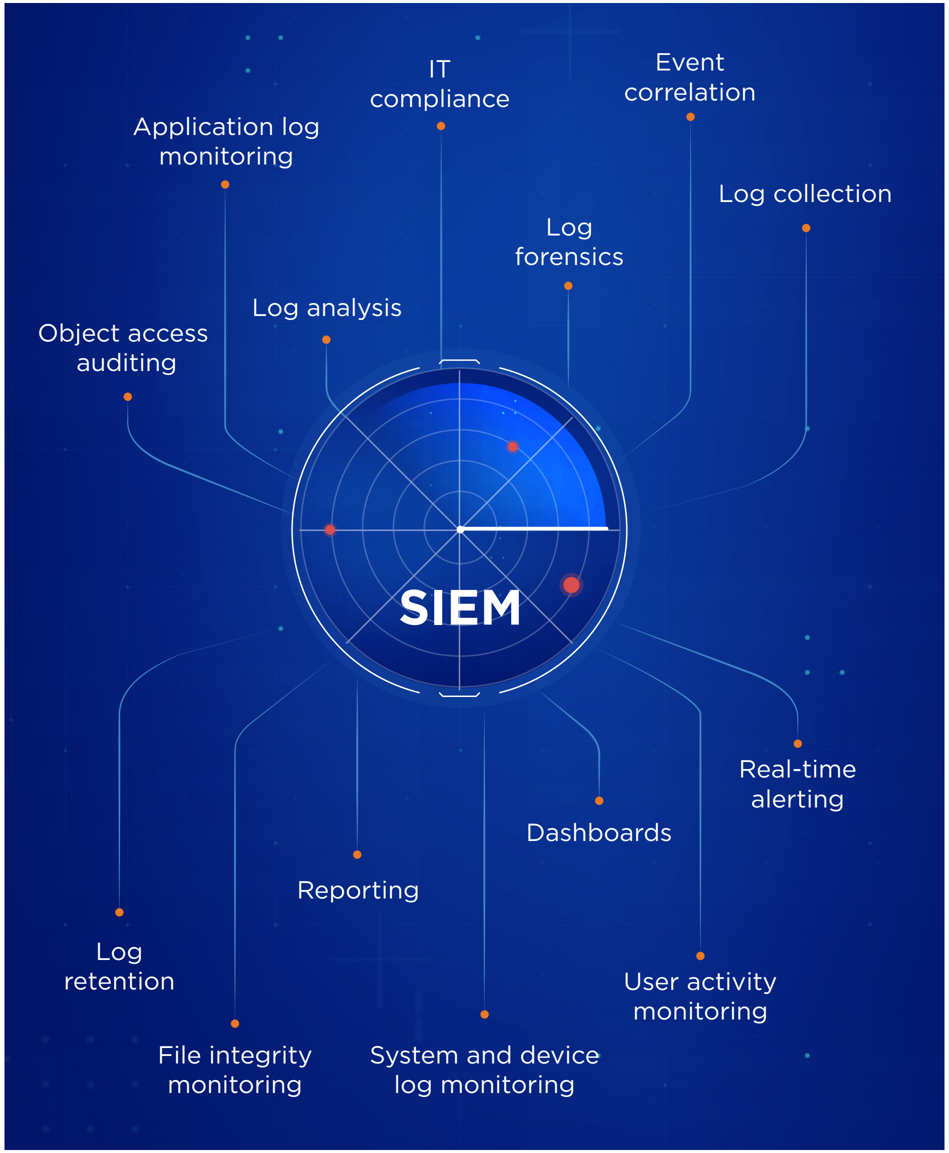
Best practices for threat management

Best practices for threat management

Modernised SIEM

While the traditional approach to SIEM monitoring was simplistic and obsolete, managed security services and large organisations today tend to adopt a platform-based strategy built around their security analytics core engine. Next-generation SIEM models ingest log and flow data and use threat models to determine the threats.

A modernised SIEM system can include real-time alerting, incident analysis and integration with other security tools and platforms. It can find and warn about possible threats in real-time, so organisations can act quickly to reduce the risk. Further, integrating with other security tools and platforms, such as UEBA (User and Entity Behavior Analytics), Threat Intelligence and SOAR (Security Orchestration, Automation and Response), provides organisations with a more complete and integrated view of their security posture.



Best practices for threat management

Preventive layer

In terms of security posture validation, several businesses today engage in preventative technology. A preventive layer in threat management is a set of measures or controls that are put in place to prevent or mitigate potential security threats before they occur. These measures can be proactive, such as implementing security controls to protect against known vulnerabilities or reactive, such as establishing processes for responding to new or emerging threats.

Threat management preventative layers -

- Firewalls, intrusion detection and prevention systems, and other network security control to prevent unauthorised access and network-based threats.
- Multi-factor authentication and least privilege access to help secure systems and data.
- Secure coding and vulnerability testing to avoid vulnerabilities and exploits in custom-developed or third-party applications.
- Encrypting and controlling sensitive data to prevent unauthorised access and data loss.
- Training staff to recognise and report dangers, averting social engineering attacks like phishing.
- Regularly installing security patches and updates to systems and apps to prevent vulnerabilities from being exploited.
- Business continuity and disaster recovery planning to reduce disruptions and help firms recover faster.

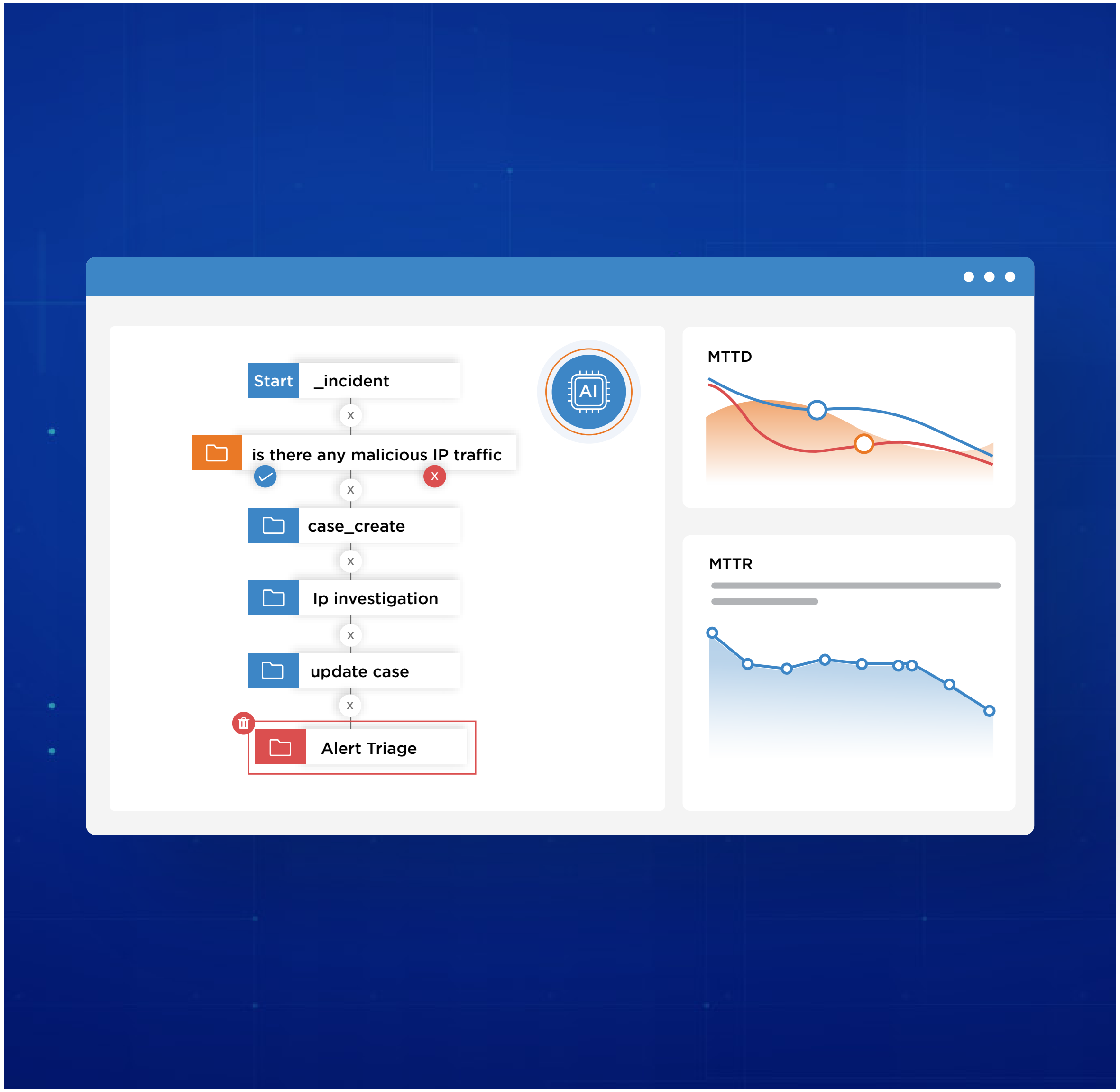
Firewalls, intrusion detection and prevention systems
Multi-factor authentication
Secure coding and vulnerability testing
Encrypting and controlling sensitive data
Training staff
Regularly installing security patches and updates
Business continuity and disaster recovery planning

Best practices for threat management

Automated SecOps

Adding a security operations layer can help with threat management in several ways. First, it provides a central control point for security-related activities, allowing organisations to monitor and respond to threats more effectively. SecOps can also help monitor network traffic, identify and block malicious traffic and implement security controls to prevent or mitigate potential attacks. Secondly, a security operations layer helps the organisation better monitor its security posture. Finally, a security operations layer enables organisations to respond to and recover from security incidents more effectively. This involves having a well-defined incident response plan and the necessary tools and resources to remediate security breaches quickly.

The predefined SOPs and playbooks expedite remediation and reduce manual intervention through automation. Contextual data, combined with automation, reduces the Mean Time To Detect (MTTD) and Mean Time To Respond (MTTR). Detecting and responding to threats more quickly can significantly alleviate their impact on business.

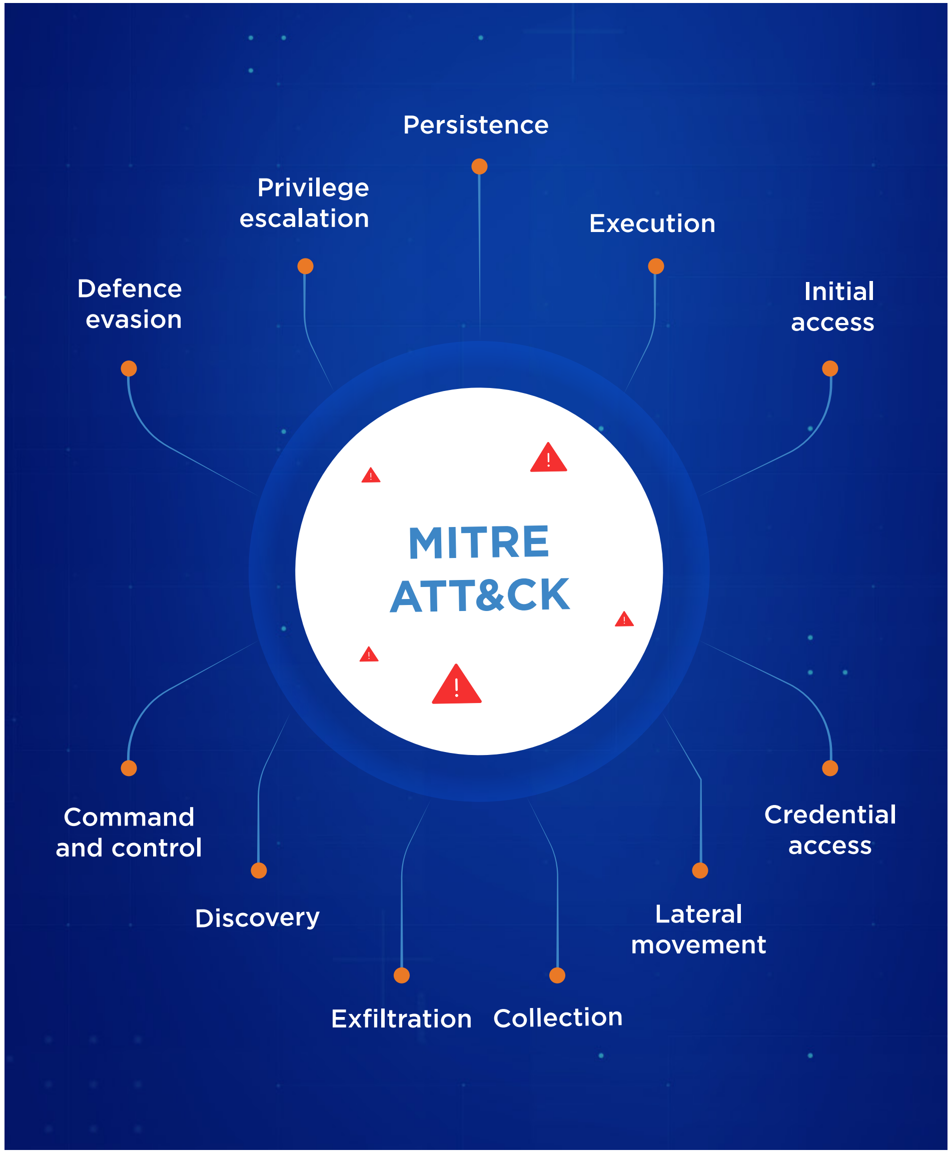


Best practices for threat management

Understanding initial access

Initial access is how an attacker gains access to a system or network and it can be achieved through a variety of methods, such as exploiting a vulnerability, using a stolen or weak password or using social engineering techniques to trick a user into divulging login credentials. Understanding initial access is important because it helps organisations identify the root cause of an attack and take the appropriate steps to prevent similar attacks from occurring in the future.

Customers evaluate security procedures using the popular MITRE framework. You can determine the security roadmap and investment choices by mapping the ingested logs against the MITRE attack architecture and highlighting their vulnerabilities. With this foreknowledge, organisations can verify phishing, anti-phishing and other technologies and train their staff on how to deal with unsolicited URLs. Over time, it also helps the companies understand how initial access is established and take corrective action to strengthen their security posture.



Best practices for threat management

Predictive approach

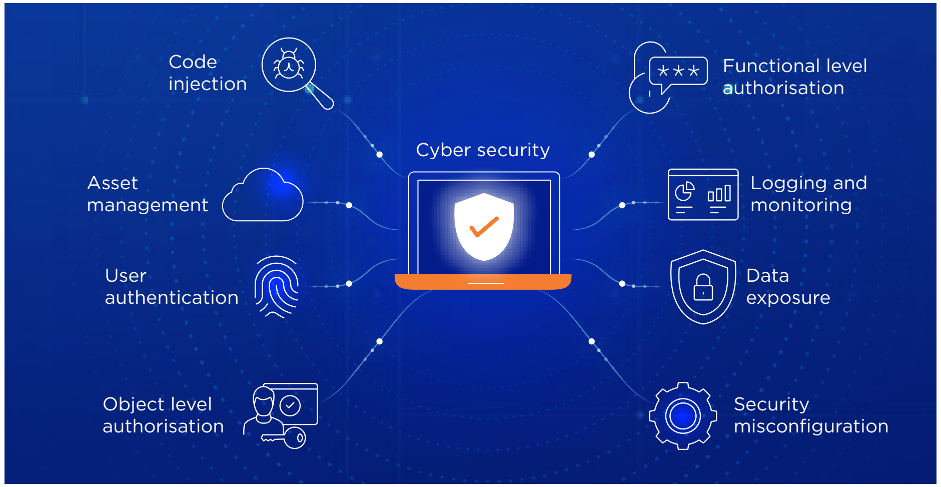
A predictive approach to threat management involves using data and analytics to anticipate and proactively mitigate potential security threats before they occur by leveraging AI and ML. You can analyse patterns and trends in data, identify potential threats and take preventive action.

A predictive approach allows an organisation to be proactive rather than reactive in its approach to security, allocate its resources more effectively and recover rapidly from security incidents. Overall, a predictive system is a best practice for threat management because it allows an organisation to protect its assets better and reduce the risk of security breaches.

Strengthening security controls

Weak security controls can be identified across an organisation's infrastructure, including at the data center, endpoint, work-from-anywhere infrastructure, and partner ecosystem. To improve communication with partners, organisations can add controls to their API framework or external system.

In today's evolving threat landscape, continuous review and improvement of security controls is crucial for staying ahead of potential threats and safeguarding systems and data. This can involve implementing strong access controls, firewalls, and network security measures, as well as regularly updating systems and applications.



Best practices for threat management

Simple onboarding

When it comes to threat management, the top goal is to simplify the customer's security monitoring requirements. A simplified onboarding process can help the customer. For example, an integrated threat management platform connecting to the customer's ecosystem beyond dedicated lanes and IP SEC-based tunnels would offer a more efficient and seamless user experience. Typically, organisations begin with their crown jewel apps and onboard associated infrastructure.

When customers have adequate information about the security policies and procedures and any relevant security tools and technologies they will be using, the risk of unauthorised access or misuse is considerably reduced. Customers can be granted the appropriate level of access to the security tools and technologies they need.

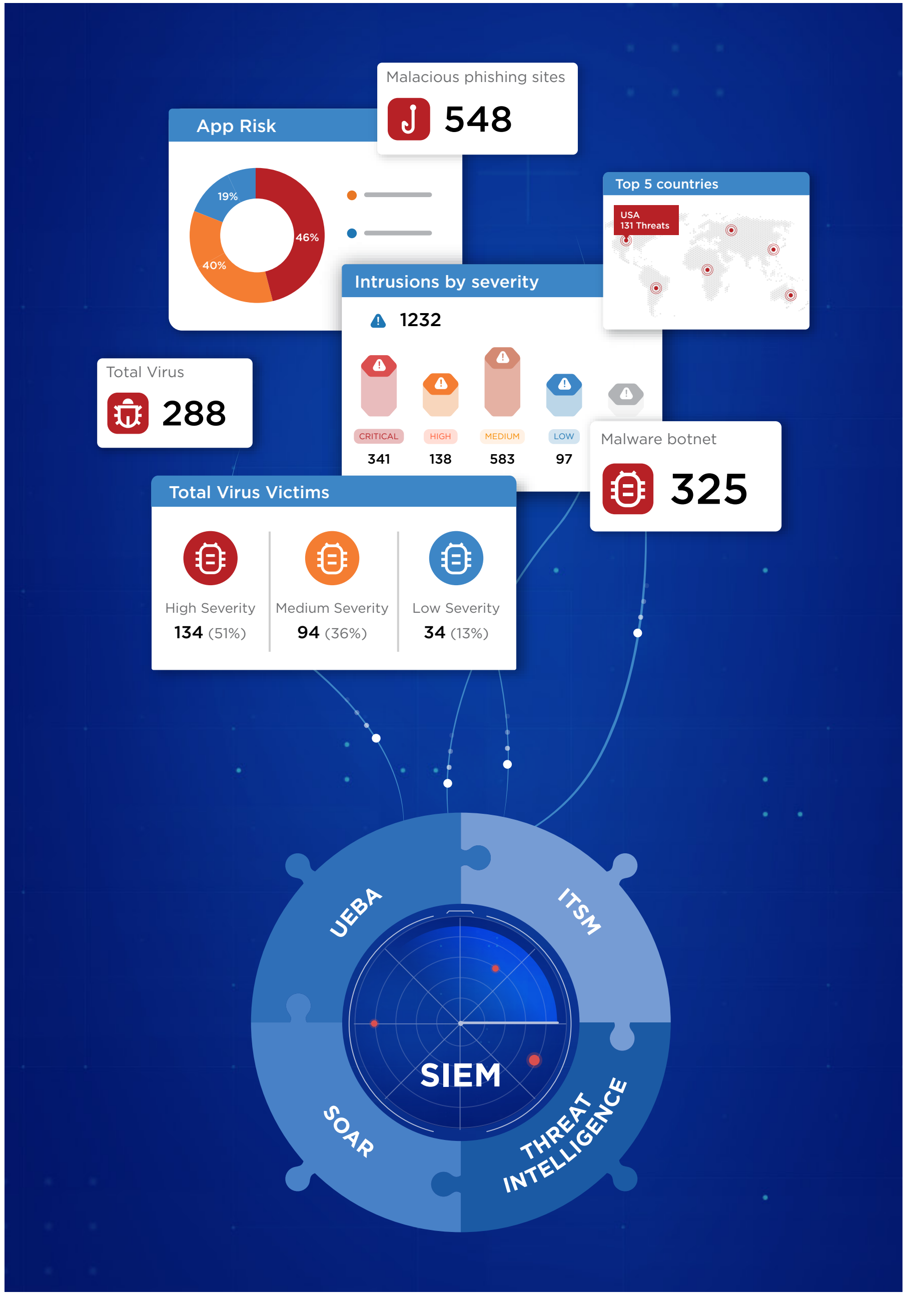
Stay up to date on latest threats with our threat advisory.

Unifying threat management with a platform-based approach

With security modernisation, traditional SIEM is not going to help. Hence, a platform-based approach is needed to provide a more collaborative and flexible approach to security operations. In addition, unifying threat management across the entire organisation enables cybersecurity and IT analysts to respond more quickly and effectively to potential cyberattacks and other incidents.

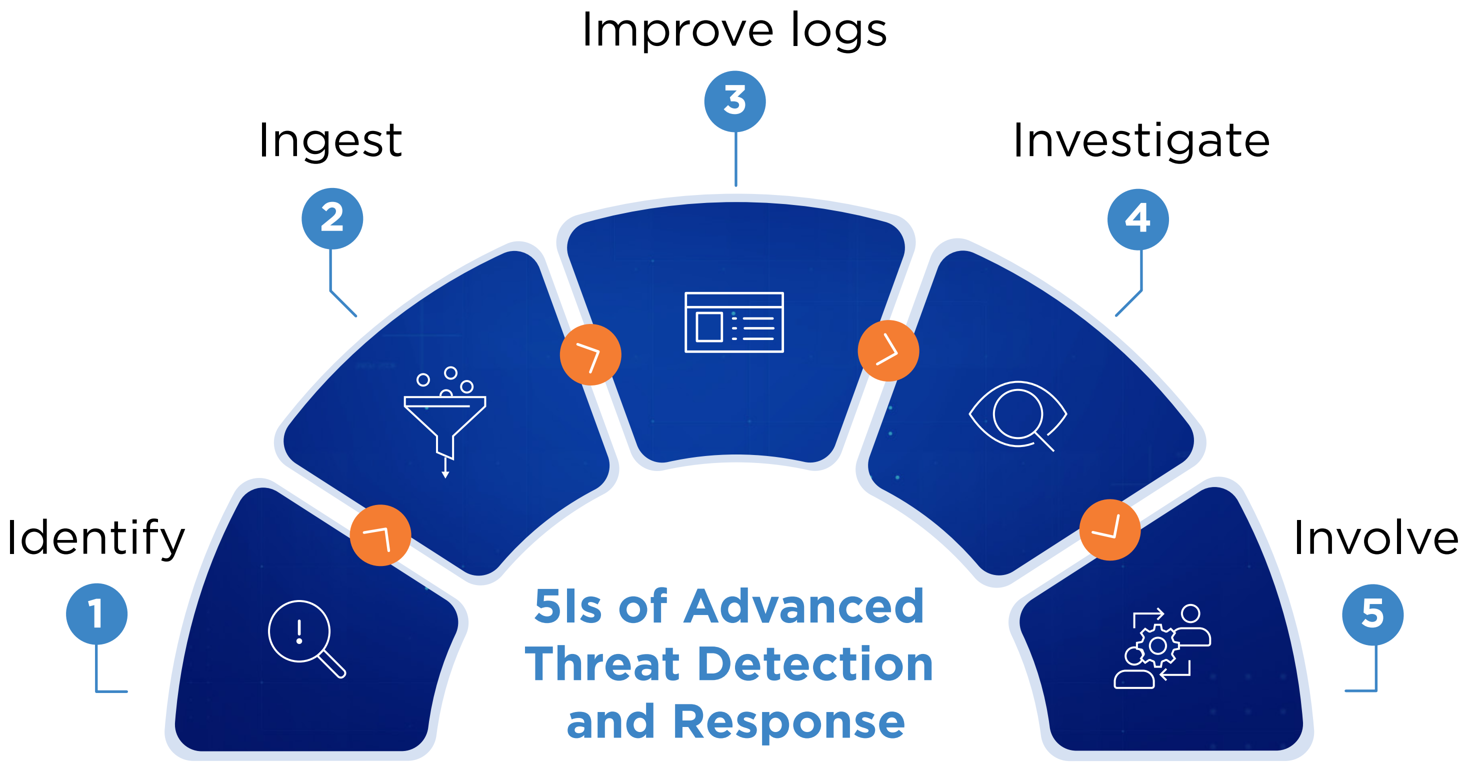
Minimising the impact of a cybersecurity incident requires a rapid incident response, which is only possible if an organisation has centralised visibility and control over its entire IT environment. As a result, a platform-based threat management solution can minimise the cost of security breaches with faster detection and response to ever-evolving threats.

Integrating SIEM (Security Information and Event Management) with other modules like UEBA (User and Entity Behavior Analytics), ITSM (Information Technology Service Management), Threat Intelligence and SOAR (Security Orchestration, Automation, and Response) can help unify threat management by making security more comprehensive and integrated. SIEM systems collect and analyse data from various sources, like network devices, servers and applications. Combining them with other modules helps organisations connect data from these different sources and get a complete picture of potential threats.



A five-step approach to effective threat management

While there are various frameworks to deal with threat management, one of the most effective approaches is a five-pronged one: identifying threats, ingesting the logs, improving the quality of the records, investigating the red flags, and involving staff.



A five-step approach to effective threat management

Identify

Many businesses start their journey by integrating or enabling detection control for their infrastructure. Customers work alongside the MSSP to identify the "crown jewel" apps and the infrastructure around critical, business-sensitive applications. The next step is to turn on detection control for them. This step also includes identifying all the log source ecosystems to be integrated with the threat management platform.

Ingest

Most businesses find ingestion challenging as applications are dispersed across different locations. Once organisations identify the devices or user ecosystems that will provide the log data, they need to filter irrelevant logs at the source and ensure the threat management platform further processes only the meaningful logs critical to security. There are several advantages to doing this:

- Companies stand to pay less to cloud providers only for the valuable log traffic exiting the cloud.
- Secondly, the utilisation of threat management platforms is captured by the volume of logs received by the platform. Filtering of logs at the source ensures that the platform only receives meaningful security information for further processing.

Improve logs

Data improvement or enrichment adds value by assembling all the different elements. Contextual information helps you cut through the noise and develop a coherent outlook. Malicious logs from the company's internal infrastructure and the external world often lurk alongside meaningful ones. To get rid of these, enriching and improving the logs is essential. In addition, the industry feeds ingested into the platforms from the company's CTA infrastructure help improve the logs. The logs are then run through the complete set of correlation rules and numerous models. The outliers are identified using various data models and rules that process the ingested logs.

Enriching or improving log data improves observability and diagnosis, making the data more useful for search, analysis and other operational needs. You can enrich logs by connecting to various enrichment sources and then using them to define policies. The platform can also validate foreign IPs using commercial and open-source feeds. As a result, the analyst can decrease threat proliferation through swift preventive measures and isolate and target the endpoints that connect with possible attackers.

A five-step approach to effective threat management

Investigate

The analysis or investigation of logs is a preventative measure that uses additional information from the customer's infrastructure. Engineers use rules to drill down and analyse similar historical occurrences or patterns. As a result, the analyst can decrease threat proliferation through swift preventive measures and isolate and target the endpoints that connect with possible attackers. The investigation also helps qualify the assets and infrastructure logs communicating with the outside world. For instance, if some outliers are discovered on the cloud, engineers will apply rules to check if a similar pattern exists in other infrastructures, like on-premises data centers or AWS. Thus, we can proactively avert potential attacks. SOAR playbooks also assist SOC specialists in triaging and qualifying threats.

Involve

When a critical alert is found, the security service provider contacts the client's CSIRT team or incident manager to begin remediation. Multiple severity levels can be defined while onboarding a customer to the threat management platform as per their organisational security guidelines and the threat is then handled according to its severity and ticket priority. With a predefined SOP for remediation, that threat can be addressed efficiently. A SOAR-assisted security ecosystem ensures quick identification of the cyber risks related to the organisation, connecting back to the customer for remediation. Additionally, real-time feedback mechanisms, incident reporting and regular customer communication ensure proactive security monitoring and the implementation of preventive controls.

TATA COMMUNICATIONS

Explore Tata Communications' Managed Detection and Response (MDR) Solution

Tata Communications defends businesses against internal and external threats. As a CERT-In-empanelled, award-winning cyber security vendor, we prevent complex threats with 24/7 threat management, cloud security, governance risk and compliance management. In addition, our platform-based SOC services provide enhanced protection by identifying advanced threats and automating threat response. With Tata Communications MDR solution, get your SOC up and running in 2 weeks.

Request a free security consultation today

References:

1. Sumo Logic. "2020 State of SecOps and Automation Report | Sumo Logic," June 2020.
2. ITIJ. "Risk Managers - Are You Prepared for What's on the Horizon in 2023?" November 17, 2022.
4. Oltsik, Jon, and Bill Lundell. "The Life and Times of Cybersecurity Professionals 2021 Volume V." ESG Global, July 2021.
5. "Cost of a Data Breach 2022." Accessed December 19, 2022. https://www.ibm.com/reports/data-breach.
6. Proofpoint, "2022 Ponemon Cost of Insider Threats Global Report | Proofpoint US," January 31, 2020.
7. Deloitte. "Smart cyber: How AI can help manage cyber risk," 2019. Accessed January 2, 2023.