Connected World.
Connected Experiences.

Tech Mahindra

SenTindra
Next-gen integrated SOC by Tech Mahindra

Tech Mahindra’s mechanism to effectively detect & remediate known / upcoming threat vectors / Zero Day

78% of CISOs have 16 or more tools in their cybersecurity vendor portfolio; 12% have 46 or more*

80% of IT organizations said they plan to consolidate vendors over the next three years.*

State of art Multi Tenant global security operation which can also be leveraged for shared service offering by leveraging Microsoft Sentinel.

Provide next gen integrated SOC to TechM Customers by leveraging TIP, UEBA, NBAD, Vulnerability Integration and SOAR capabilities for automated remediations

To implement industry specific use cases to address legal and regulatory compliance requirements & providing a mechanism to effectively detect & remediate upcoming threat vectors / Zero Day

Source
***Gartner Identifies Top Security and Risk Management Trends for 2021**

Tech Mahindra

CHALLENGES

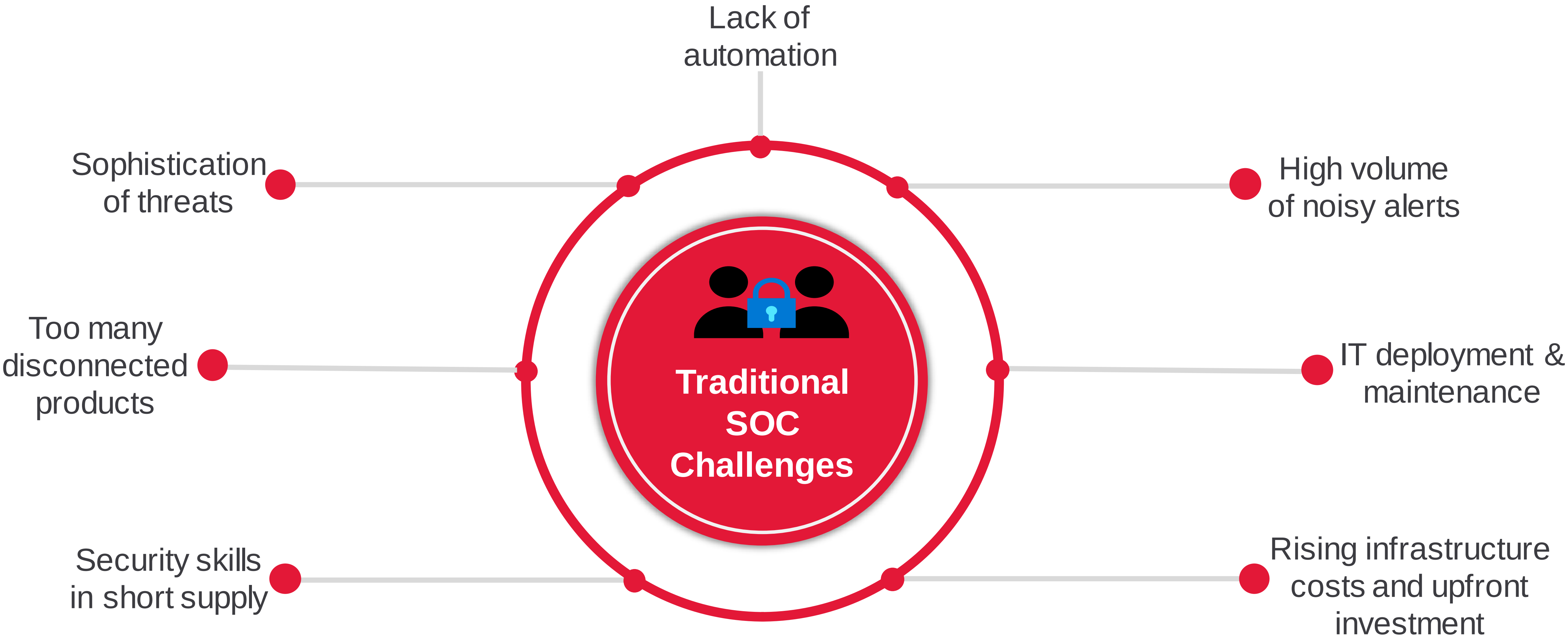
- Security tools running in a silo
- Stitching together a holistic approach from network, endpoint, application and data security along with risk and compliance is a mammoth task
- Inadequate visibility to pattern based and behavior-based anomalies.
- Lack of single pane of glass to view to summarize security events
- Actionable information on high-risk events for early attack detection
- Absence of next-generation solution along with overall monitoring of Security posture

IDEAL SOLUTION

- Adoption of Cybersecurity holistic approach by deploying the correct controls whey they are needed the most
- Having fewer security solutions can make it easier to properly configure them and respond to alerts, improving your security risk posture
- Next generation of AI and automation helps leverage the large-scale intelligence available in the cloud and make it work for you.

DESIERD OUTCOME

- End to end visibility to the entire landscape against NIST & CIS – helping to uplift the overall security posture
- Tech Mahindra's holistic approach of monitoring integrating all the security components which would enable immediate addressing of security threats and thereby giving clients a better Security Posture
- 30% enhancement in security posture with expert recommendation



Traditional SOC Challenges

Lack of automation

Sophistication of threats

High volume of noisy alerts

Too many disconnected products

IT deployment & maintenance

Security skills in short supply

Rising infrastructure costs and upfront investment

Human and Artificial Intelligence

Security Operations Team

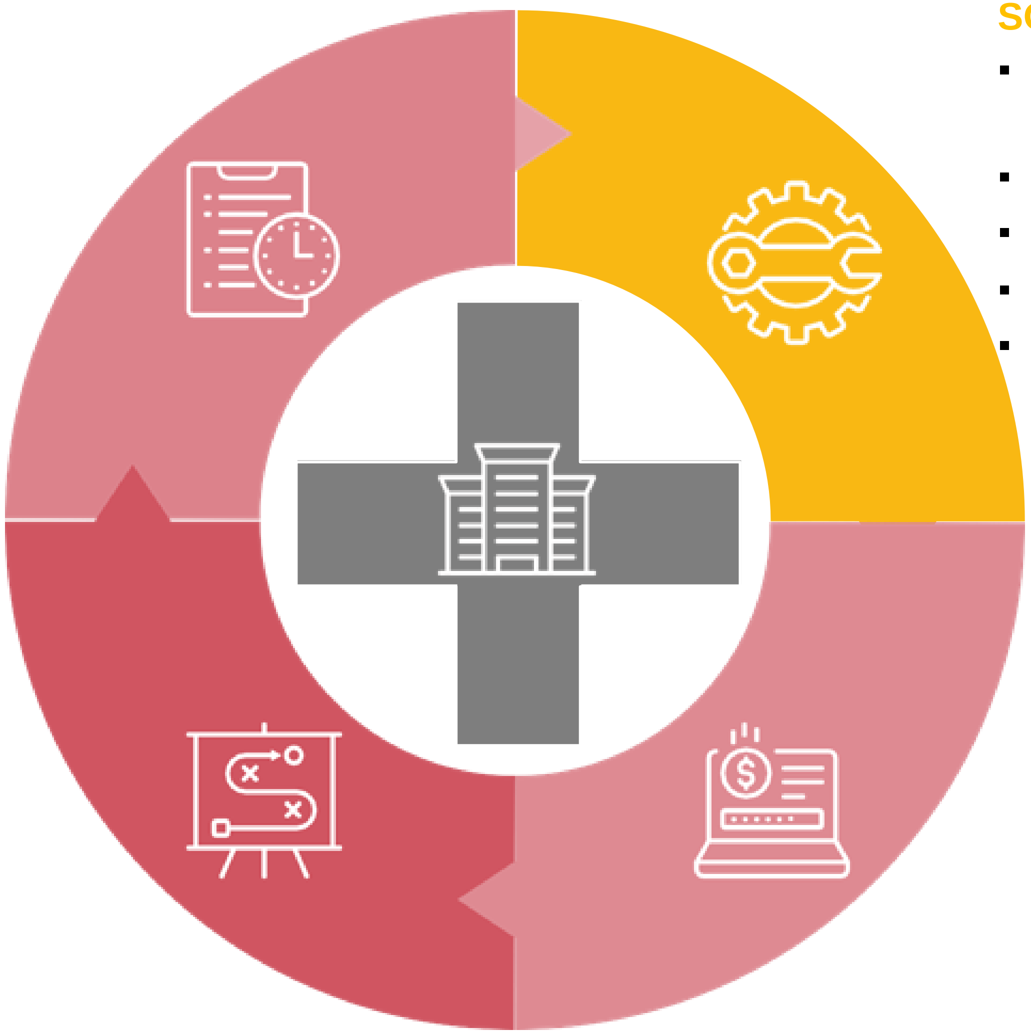
Cloud + Artificial Intelligence

AS IS STATE ASSESMENT

- Understanding IT environment, landscape and strategic initiatives, mandates and KPIs.
- Understanding Cyber Policies, Audit Policies, Standards, legal and regulatory requirements
- Understanding business layers, information systems, data technology (IT and Telcom) and Security

SOC Transformation

- Assessment calendar for 3 years.
- BAU report and timelines
- Implementation of all agreed corrective action towards identified gaps
- Sustenance Processes & Knowledge Transfer



SOC Framework Identification

- Based on the AS-IS state assessment findings, TechM team will plan the enterprise security monitoring framework with
- Business context
- Unified risk,
- Third party risk, compliances and
- Minimum baseline security monitoring standard for infra and application.

Managed Security

- Define processes and procedure for SOC + IR (incident response)
- Development of Content – Use cases, reports and dashboard
- Defining Run Books/Jupityr Notebook
- Implementing monitoring, notification and triage process
- Implement Incident escalation and incident response/reporting process
- Integration of Log sources (Target services)
- Integration with ticketing tool

Tech Mahindra's Azure Cloud Services

GET A DEMONSTRATION:

microsoftgtm@techmahindra.com

CALL FOR MORE INFORMATION:

+91-8826566066

ASK A QUESTION VIA EMAIL:

microsoftgtm@techmahindra.com

LEARN MORE:

https://www.techmahindra.com