Tx Managed Cybersecurity Testing & Monitoring Practice

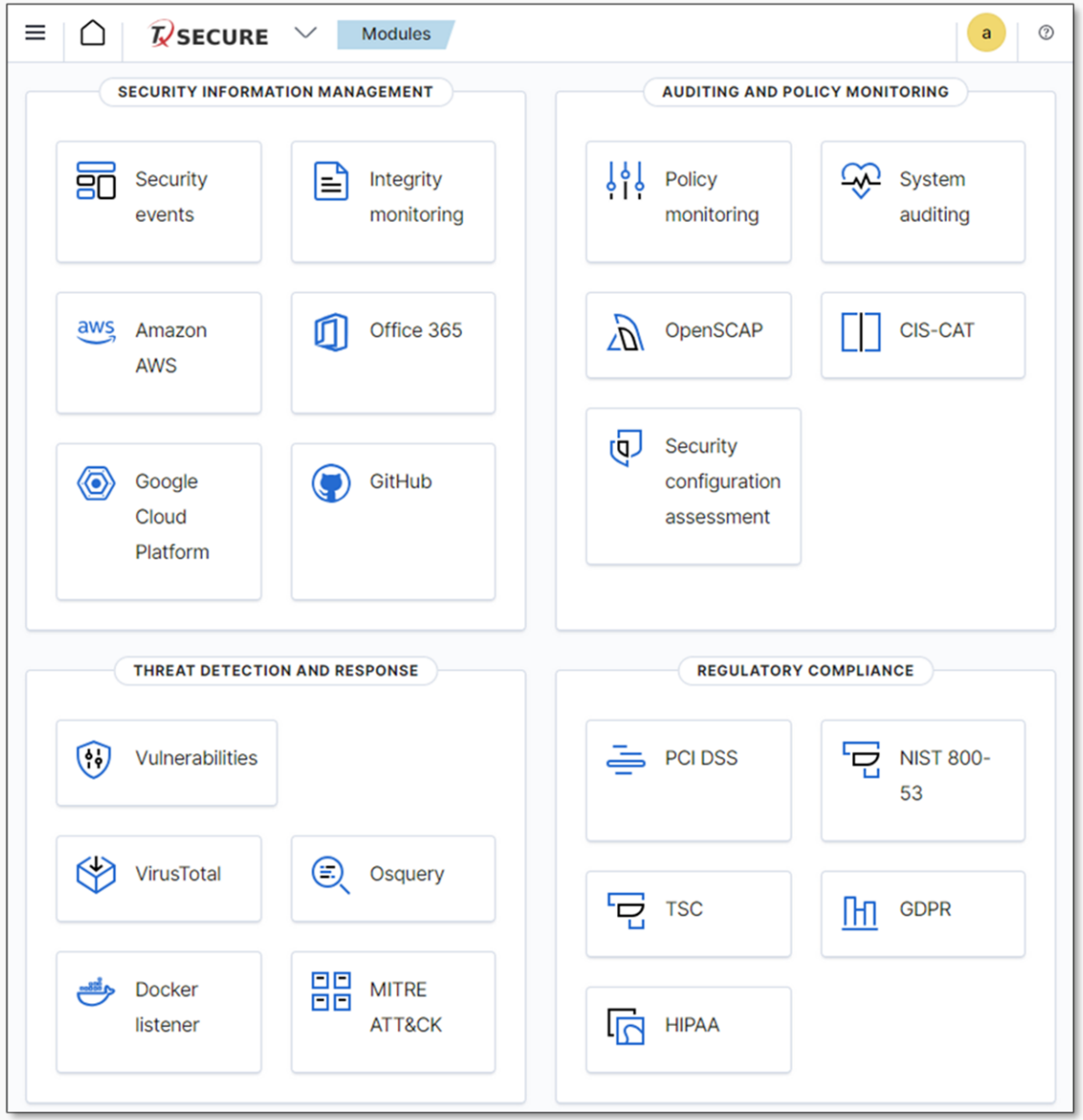
WWW.TESTINGXPERTS.COM

Continuous Security and Compliance Monitoring

Tx-SECURE: An Overview

TX SECURE

- A powerful Security Operations platform covering SIEM, Compliance Monitoring, Threat Intelligence etc. that provides advanced security analytics and threat detection capabilities.
- It offers comprehensive monitoring, analysis, and AI-powered threat content enrichment for a wide range of security-related data across your entire infrastructure.
- Tx-Secure seamlessly integrates with various data sources, **including endpoints, servers, cloud environments, containers** etc. to provide a centralised view of your security posture.
- Its robust rules engine and machine learning algorithms enable real-time detection of known and unknown threats, empowering your security team to respond quickly and effectively.



Features of Tx-Secure

Real-time Threat Detection

- Tx-SECURE’s advanced analytics and correlation rules quickly identify and alert on suspicious activities, enabling rapid response to potential threats.

Compliance Monitoring

- Tx-SECURE monitors systems, servers as well as cloud environments ensuring continuous compliance with industry standards like CIS Benchmarks, PCI-DSS, NIST 800-53 etc.

Vulnerability Management

- Tx-SECURE’s offers built-in capabilities for end-to-end Vulnerability Management across endpoints, servers and cloud instances.

Network Intrusion Detection

- Tx-SECURE monitors network traffic to and from endpoints, servers to detect intrusion attempts by detecting commonly used attack methodologies.

File Integrity Monitoring

- Tx-SECURE tracks and alerts on changes to critical system files and configurations, helping to detect and prevent unauthorised modifications.

Comprehensive Visibility

- Tx-SECURE collects and aggregates security data from across your entire infrastructure, providing a centralised, unified view of your security posture.

Malware Detection

- Tx-SECURE uses Virustotal API to detect malware in endpoints and servers in real-time.

Log Management and Analysis

- Tx-SECURE's powerful log management capabilities enable in-depth investigation and forensic analysis to uncover the root causes of security incidents.

Tx Cyber Security Services Portfolio: Tx-SECURE

Planning Stage

1 Requirement Gathering

2 Design Stage
- Attack Surface Analysis
- Threat Modelling

3 Identification Stage
- Asset Identification & Classification
- Monitoring Rules Definition
- Monitoring Policy Creation

Plan Document (Deliverable)
- Documenting Security Compliance Policies
- Specifying Applicable Policy For Each Asset Type.
- Identify And Assign Responsibility & Ownership For Each Asset Type

Tx-SECURE Continuous Security Compliance Monitoring Solution
A single window solution to monitor security compliance across all assets.

4 Continuous Compliance Monitoring Setup
- Implement Compliance Monitoring Policy in Tx-SECURE platform
- Install 'agents' on target systems/assets
- Configure connections between agents and Tx-SECURE Server.

5 Continuous Operation
- Monitor Security Events and report them on regular intervals.
- Continuous Monitoring of Compliance Deviations across all assets and asset groups.

6 Production Operation & Maintenance
- Continuous Operation and Policy Updation as per new identified threats.
- Continuous Reporting about the performance of the solution.
- Solution upgradation and patch management as required.

Implementation Stage

Security Consultant

Client Team


Thank you