Deloitte.

Managed Threat Services

June 2018

Risk Advisory

Contents

Dynamic and Evolving Threat Landscape

With proliferation of advanced technologies and shared environments, the threat landscape is rapidly changing and expanding. Besides, it is getting more complex to manage with increased adoption of cloud services and use mobile devices for corporate data and applications. As a result, the traditional approach to security is not sufficient to ensure information and asset security of organizations or manage threats. Many enterprises are cognizant of changing security demands. However, due to inadequate integration between technologies, lack of expertise, resources, intelligence, and a di erent core business focus, the cost and complexity of security operations increases. To ensure essential cyber security, along with new generation security controls, there is a need of holistic and advanced security threat management programme that is equipped with actionable intelligence and rapid response to shift security operations approach from reactive to predictive threat management.

Deloitte Managed Threat Services

Deloitte Managed Threat Services (MTS) provides customized threat detection, assessment, and response services to enterprises across industries. It follows a business-aligned risk-based approach in security monitoring and threat analysis that prioritizes security incidents and threats on the basis of business value of the targeted asset. Leveraging its global Cyber Intelligence Centre (CIC) network, Deloitte MTS provides proven threat management.

Deloitte MTS is based on information acquired from the client's business environment, threat landscape dynamics, global threat intelligence and knowledge base built over experience of providing various security services to multiple clients from diverse industry verticals.

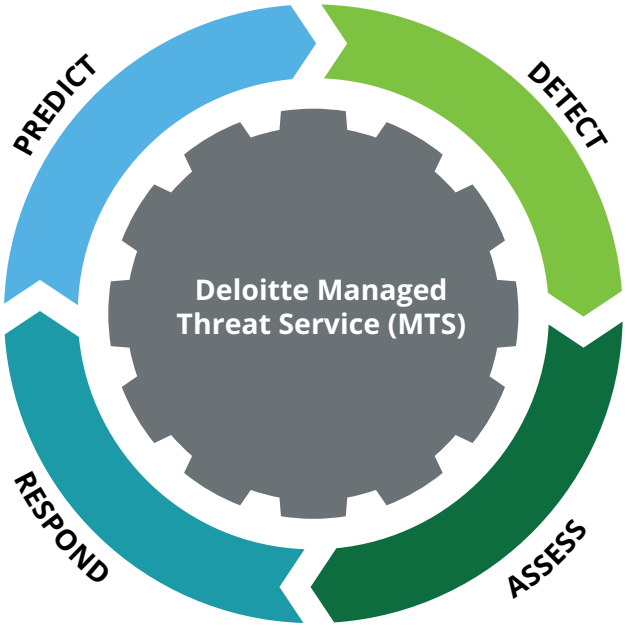
Our team has industry-recognized skills and certi cations. Going beyond the technical feeds, the team can contextualize the relevant threats, helping to determine the actual risk that a threat poses to an enterprise business, its clients and other stakeholders.

Threat Management Challenges

- **Changing Threat Landscape**
  With increased usage of smart devices and Internet of Things, the threat vectors and actors scope has increased signi antly.
- **Responding and Managing Threats**
  Distinguishing between real threats and false positives followed by e ective procedure to respond to quali ed incidents is experienced as a big challenge by enterprises.
- **Building Infrastructure and Providing Expertise**
  It's challenging for enterprises to build and maintain infrastructure, intelligence, and expertise outside of their core business.
- **Expanding IT Boundaries**
  With enterprises moving to cloud, IaaS, PaaS and SaaS, it's really difficult to be vigilant over threats coming from these environments.
- **Managing Technology Silos**
  Multiple traditional security controls are in place; however, they are not integrated to derive any actionable intelligence.
- **Managing Insider Threat**
  Unauthorized access to data and misuse of information by authorized users has always been a challenge.
- **Extracting Actionable Intelligence**
  Business environments are generating high volumes of data daily. It's cumbersome to manage and derive actionable intelligence from such a high volume.
- **Consolidating View of Threat Activity**
  With security incidents impacting top management layer, it's essential to have a dashboard that clearly depicts security posture and relevant details from top management to operations executive level.
- **Managing Compliance**
  Di erent security regulations mandate enterprises to speci c architecture and present di erent reports.
- **Monitoring Proactively**
  Proactively predict security threats that may be targeted for your organization instead of only reacting to the post security incidents.

Highlights of Deloitte MTS

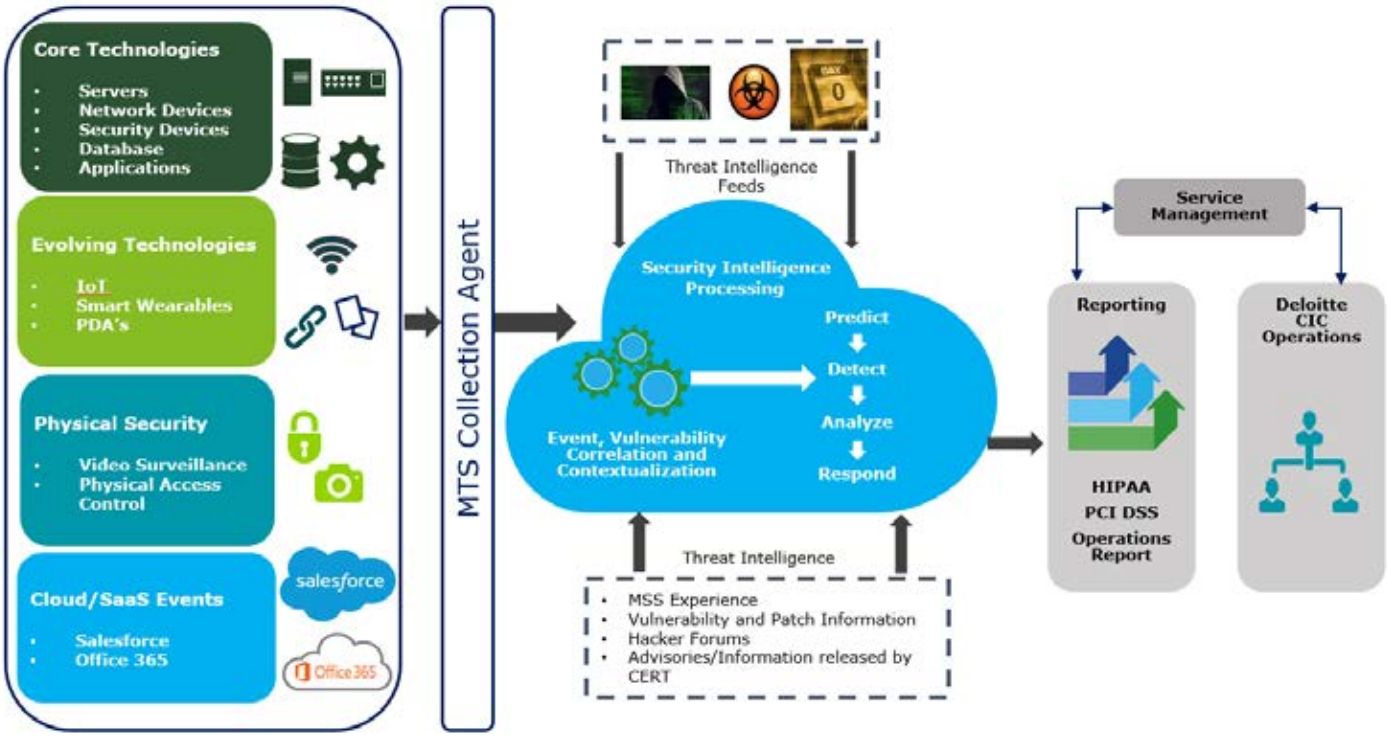
- Context aware security intelligence platform of Deloitte CIC
- Enables actionable threat intelligence to predict security threats
- Zero-day threats, malware, and reputation feeds for proactive prevention actions
- 24x7x365 security monitoring and threat detection through proven use case based framework
- User Behavior Monitoring to alert in case of anomaly in user action
- Context Aware Service contributing to prioritize security incidents and gauging their impact on your IP, assets, and information.
- In-depth assessment of potential and quali ed security incidents by skilled security experts
- Incident and threat response as per agreed procedure and stipulated Service Level Agreements (SLAs)
- Assistance in containment of impacted asset, remediation, and restoration



Threat Management Lifecycle

Key features

- Integrates with Deloitt agship services
- Scans run-time application, enabling applications to protect themselves against attacks
- Supports on-premise as well as cloud environments
- Ensures exible deployment models
- Provides scalability in case of expanding business environment
- Includes defence-in-depth security architecture for CIC environment with privilege identity controls for all Deloitte CIC security experts
- Consolidates CIC dashboard for security posture view and reports repository
- Enables out-of-the-box and customized compliance reporting



Deloitte has adopted an intelligence-led approach to monitor and manage cyber risk—key to building cyber security and resilience. By identifying the relevant, current, and emerging threats to an enterprise, MTS can proactively identify and assist in mitigatation cyber attacks.

In MTS, collection agents integrate with data sources to collect, aggregate, and normalize the events. The source of information to MTS could be IT infrastructure, network/security devices, database, applications, mobile devices, user activity, machine learning, and processed events from another Security information and event management (SIEM) platform. The Security Intelligence Engine processes the relevant security events for correlation and threat intelligence execution. It also has numerous use cases created to alert and assess on the basis of data from information sources and threat intelligence feeds.

Deployment Options

Deloitte MTS allows exible deployment, with options ranging from as-a-service to dedicated security operations deployment. Deloitte assists the client enterprise to choose the deployment model that best ts their business needs. A brief summary of Deloitte MTS's di erent deployment is given below:

1. Managed Security Analytics (Multi-Tenant)

This deployment model is based completely on Deloitte people, process, and technology. It is a multi-tenant deployment model and thus highly cost-e ective with high intelligence sharing. There are di erent subscriptions available for this deployment; the enhanced subscriptions have more features, better SLAs and work integrated with Deloitte's othe agship services such as Vulnerability Management and Application Security Services. Please refer to the table below to understand features available with di erent levels of subscription:

Features	Basic	Premium[1]	Advanced[1]
Log Collection, Aggregation, and Normalization	✓	✓	✓
Log Retention	✓	✓	✓
Multi-Device Correlation Rules and Monitoring	✓	✓	✓
Deloitte CIC Threat Intelligence	✓	✓	✓
Near Real-Time Monitoring and Alerting	✓	✓	✓
Deloitte MTS Dashboard/Security Portal	✓	✓	✓
Vulnerability Correlation and Intelligence		✓	✓
Global Threat Intelligence		✓	✓
Context Aware Security Intelligence Monitoring		✓	✓
Customized Threat Intelligence and Advisory		✓	✓
Threat Emulation and Modelling			✓
User Behavior Analytics and Machine Learning			✓
Real-Time Application Scanning			✓

1. The additional features in Premium and Advanced subscriptions of MTS are subject to additional Deloitte services to be subscribed.

2. Managed SIEM

Deloitte MTS i exible to provide enhancement to existing investment made by enterprises or planning to invest in SIEM/ security monitoring frameworks. Deloitte can take over the implementation and management of client enterprise owned SIEM/security monitoring framework. In this model, Deloitte will extend its MTS services to manage security monitoring operations from Deloitte CIC and integrate additional capabilities and deep expertise.

3. Managed Security Operations

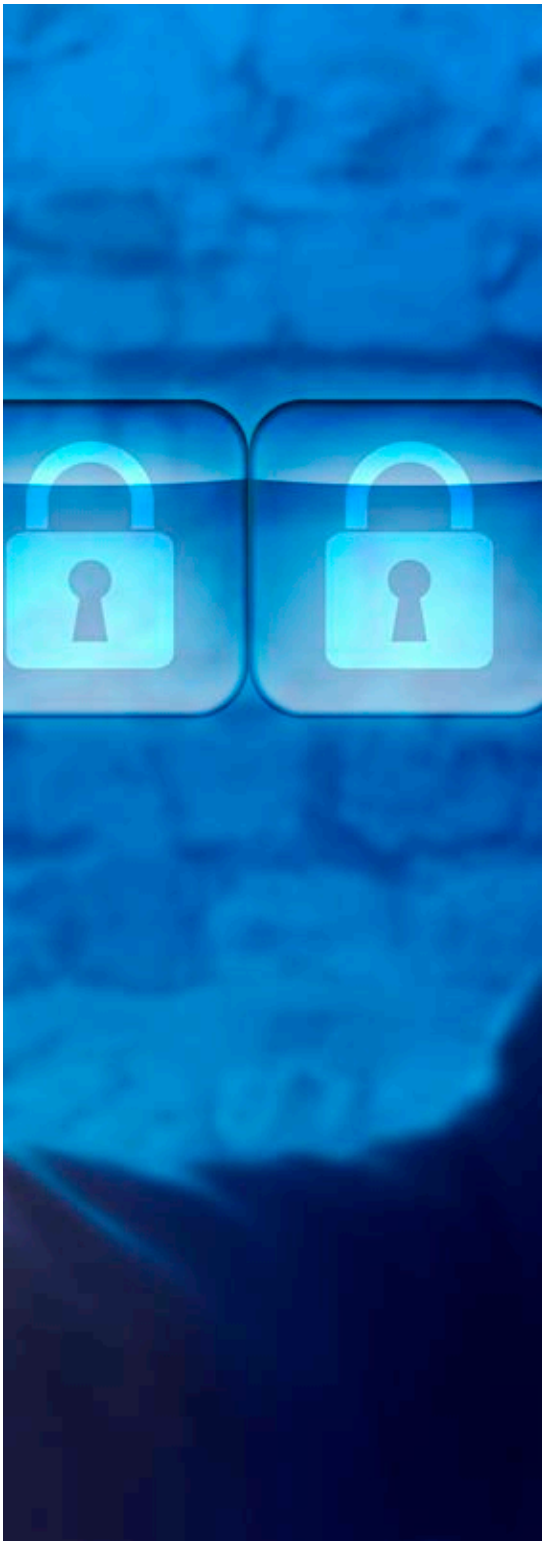
Due to security regulations, an internal security policy, or any other business reasons, enterprises may want to set up a dedicated security intelligence framework for their environment with all the associated people, process, and technology within their perimeter. Deloitte MTS i exible to extend its intelligence and expertise to operate from the client's network.

Deloitte Cyber Intelligence Centre (CIC)

Deloitte's Cyber Intelligence Centre has been developed to help client enterprises make more intelligent decisions. Working alongside organizations to contextualize the threat to their business, we focus their attention in the right place at the right time to spot the tell-tale signs of an attack before it turns into a crisis. CIC integrates technology with industry insight to provide round-the-clock client business-aligned security services. With 24x7 coverage, we monitor, assess, and manage threats speci c to your organization, enabling you to swiftly and e ectively mitigate risk and strengthen your cyber resilience.

CIC services ensure our clients are able to stay secure in a rapidly evolving threat landscape, while avoiding spiralling costs and investment requirements. Deloitte CIC follows industry best security and service delivery standards such as ISO 27001 and ITIL, respectively.

Deloitte CIC combines a number of security services together to provide our clients with a truly tailored service catalog, which enables them to fully understand their cyber risks and adopt proportionate responses in an increasingly digital, interconnected business environment. We do this by providing them with improved visibility of threats and assets, based on highly relevant intelligence that re ects their speci c business, market, and industry.



Related Services:

1. Managed Vulnerability Services:	Enable enterprise vulnerability management program with ease by enabling on-demand scans, reporting, and enabling vulnerability intelligence by integration with Threat Management Services
2. Managed Application Security:	Provides full life-cycle application security services ranging from on-demand assessment to real-time application security of the client's web-presence
3. Cyber Emergency Response:	Provides con dence that when a cyber attack takes place, Deloitte will help mitigate the impact on both technical and business front and stabilize operations to run business as usual; subscriptions-based services to enable clients sustain cyber emergencies
4. Cyber Attack Simulation:	Improves resiliency of environment through on-demand cyber-attack simulation and validate protection mechanism for enterprise environment

Key Contacts:

Rohit Mahajan
President - Risk Advisory
rmahajan@deloitte.com

Gaurav Shukla
Partner - Risk Advisory
shuklagaurav@deloitte.com

Anand Tiwari
Partner - Risk Advisory
anandtiwari@deloitte.com

Sandeep Kumar
Partner - Risk Advisory
kumarsandeep@deloitte.com

Deloitte.