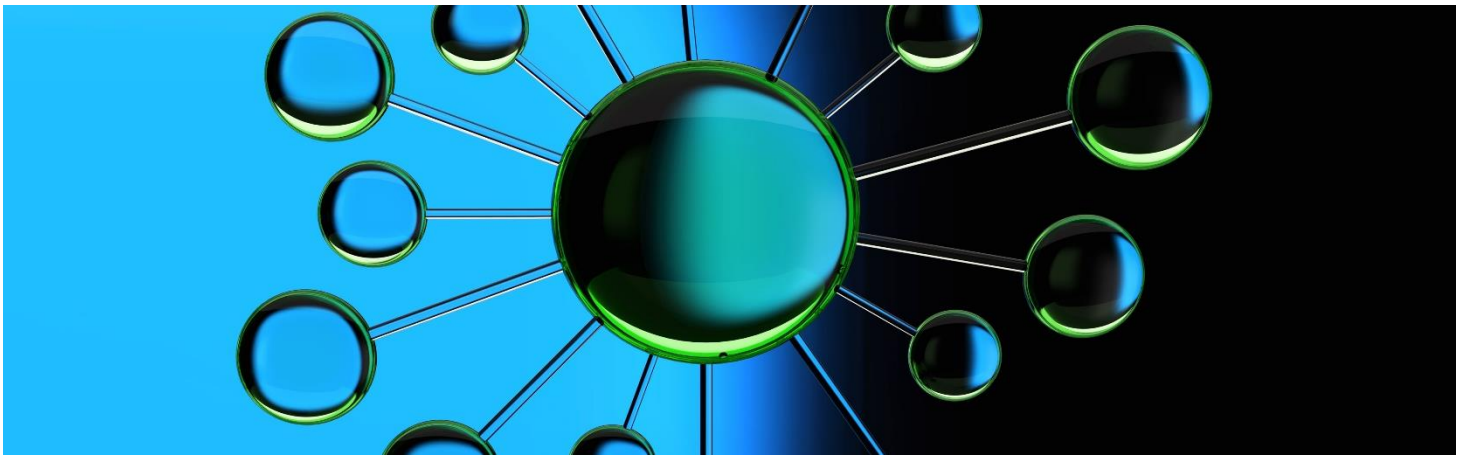
Deloitte.



Managed Threat Services
Establishing adaptive cyber vigilance

Staff shortages, the need to cut costs, and a desire to shift capital expenditures to operating expenses are a few of the issues that lead many organizations to hire managed security service providers. But today's cyber threat management challenges require more than a different way to source the same old approach to security monitoring.

Deloitte Advisory offers new, purpose-built Managed Risk Services that help organizations adopt the vigilance needed to get ahead of today's threats—and future threats. *Our Managed Threat Services (MTS) help organizations thrive by supporting their ability to pivot more rapidly in response to threats, gain greater predictive threat visibility, and focus resources on areas of greatest impact in managing business risk.*

Fight real fires

Device-centric managed services reflect an older IT-focused security monitoring model that lags behind today's reality. Anyone in security operations knows the problem too well. Cyber threats morph faster than blacklists can capture. The ecosystem of cybercrime tools and services empowers not just data theft, but campaigns bent on disruption and destruction. Business innovation creates a steady stream of new risks and vulnerabilities. And the IT environment spreads in scope: more users, more endpoints, more devices, more technologies, more applications—generating terabytes of data and millions of alerts. There is no assurance that the few alerts that can be investigated are the ones that matter.

The daily fire drill of security operations can be self-perpetuating. What commonly gets short-shrifted is the design, tuning, and development of new use cases and the adoption of next-generation capabilities that could help create fewer, smarter alerts.

The fire drill also perpetuates a dangerously internal focus. Cyber teams need panoramic threat visibility. Especially as the well-being of any one organization is increasingly dependent on the cyber-health of many third parties beyond its control, having a broad view of the threat horizon is especially important for anticipating who, why, and how a third party might be targeted.

MTS does more than help you manage your current approach more cost-effectively. While MTS can help you reduce costs and increase efficiency, our mission is to help your organization achieve your next generation of cyber vigilance capabilities so you can better detect the real "fires" that may threaten your business.

Big data, white gloves

Because of the volume and complexity of data to be analyzed, it is not possible to detect threats without advanced automation and analytics. But neither can monitoring be a purely mechanized function; the program must be tightly aligned to the particular characteristics and risk profile of each organization, and requires tailored use case development and tuning, and targeted threat research. MTS is both a big data cyber analytics platform and a multi-disciplinary team of cyber professionals who provide tailored "white glove" services.

Advanced technology platform. Client logs are collected and analyzed in real time via a cloud-based log management, correlation and analytics platform that replaces your on-premise security information and event management (SIEM) and log management technologies, and automates incident handling and remediation. Minimal footprint is required on the client site to support collection and forwarding of event and log data. A client portal provides a single pane of glass for tracking alerts, incidents, remediation and development activity, and for self-service compliance reporting.

Tailored service. Program managers, data scientists, threat researchers, SIEM developers, and incident analysts team to provide regularly scheduled and as-needed services, including:

- Monthly and quarterly threat briefings that produce a co-generated security maturity model for each client to guide ongoing use case tuning and development

Broad capabilities through an integrated service platform

Security Monitoring and Log Management

- 24x7x365 security monitoring
- Compliance reporting
- Log management and retention
- Alerting and ticketing
- Integrated orchestration and workflow

Threat Intelligence and Analysis

- Integrated, industry-specific threat data feeds
- Options for custom threat research services

Network Behavior Monitoring

- Detection of evasive network-level threats
- Application-level monitoring
- Layer 7 anomaly detection

Risk Analytics

- Vulnerability business risk analysis
- Exposed surface-of-attack analysis
- Critical systems vulnerability and risk scoring

Integrated Orchestration and Workflow

- Workflow integration for automated gathering and presentation of evidence and context associated with a threat
- Orchestration of SOC and IT OPS incident response: automated response and remediation actions.

Advanced Cyber Hunting

- Definition and refinement of hypotheses, tactics, techniques, and procedure (TTPs), based on exploration of new intelligence and analytics
- Identification of advanced persistent threats (APTs) leveraging both human and machine analytics

User and Endpoint Behavior Monitoring

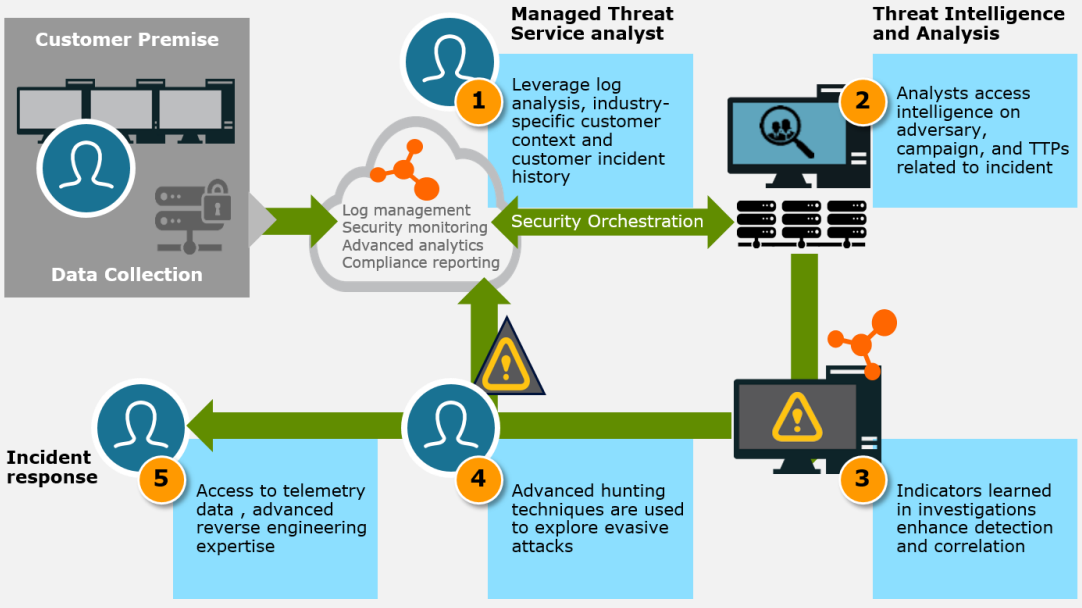
- Real-time endpoint visibility
- Endpoint active response
- System- and user-based behavioral and anomaly detection
- Investigation workflow automation
- Integrated endpoint data

- Design and development of context-rich monitoring use cases to support the prioritization of alerts and remediation
- Assignment of an industry-focused analyst who gains resident knowledge of each client's security environment and business challenges.
- Integrated cyber hunting services to scan for active threats based on hypotheses that are developed and tested leveraging a wide range of threat intelligence and awareness of each client's discernable patterns of threat activity.

Choose your starting line

Whatever level of maturity they're starting from—and whatever level they ultimately aspire to—by engaging MTS, our clients are better able to reduce burden on their in-house teams, prioritize remediation activity, and migrate to an analytics-based platform that can adjust and flex as their business needs evolve and as the digital landscape grows more complex.

Multiple disciplines turn threat intelligence into actionable insights



Logs are analyzed to identify patterns that provide insight on potential threats to a customer's environment integrated. Log analysis is integrate with exploration and hunting by skilled practitioners, leveraging intelligence on adversary TTPs from Deloitte Advisory's Threat Intelligence and Analysis teams, telemetry data and malware samples from forensic analysis, and indicators gained through Deloitte Advisory Incident Response Services.

Why choose Deloitte Advisory's Managed Threat Services?

- **Achieve the basics faster** with our library of use case accelerators and knowledge of industry standards and leading practices.
- **Make faster strides toward advanced threat management** by leveraging our pre-built, cloud-based analytics infrastructure.
- **Shorten the incident handling cycle** through automated orchestration and workflow.
- **Broaden threat visibility** through multifaceted approach to custom and industry-focused research.
- **Alleviate talent shortages** by reducing the labor associated with on-premise SIEM and log management, and by relying on the advanced skills of our specialists.
- **Prioritize remediation activity** more effectively through contextualized, risk-focused incident identification.

Visit us on the web at
www.deloitte.com/us/cyberrisk

Request a briefing!

Deloitte Risk and Financial Advisory Contacts

Adnan Amjad
Partner
Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
aamjad@deloitte.com

Kent Cinquegrana
Managing Director
Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
kcinquegrana@deloitte.com

Vikram Kunchala
Managing Director
Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
vkunchala@deloitte.com

Secure.Vigilant.Resilient.™

To grow, streamline, and innovate, many organizations have difficulty keeping pace with the evolution of cyber threats. The traditional discipline of IT security, isolated from a more comprehensive risk-based approach, may no longer be enough to protect you. Through the lens of what's most important to your organization, you must invest in cost-justified security controls to protect your most important assets, and focus equal or greater effort on gaining more insight into threats, and responding more effectively to reduce their impact. A *Secure.Vigilant.Resilient.* cyber risk program can help you become more confident in your ability to reap the value of your strategic investments.

BEING SECURE means having risk focused defenses around what matters most to your mission.

BEING VIGILANT means having threat awareness to know when a compromise has occurred or may be imminent.

BEING RESILIENT means having the ability to regain ground when an incident does occur.