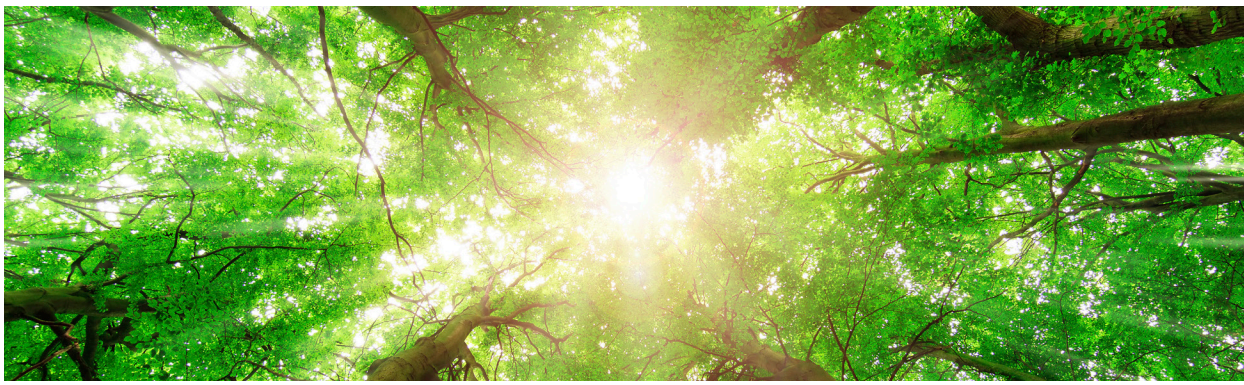
Deloitte.

For more information about our Cyber Risk Services please go to www.deloitte.com/us/cyberriskservices

Information to insight: Threat Intelligence & Analytics for business risk mitigation



Threat Intelligence is an organizational capability, not a data set.

Your organization probably uses many monitoring tools and consumes many sources of threat data, but do these technologies really provide the intelligence – the useful insights – you need to preempt or respond quickly to serious cyber incidents?

Deloitte's Advisory's Threat Intelligence & Analytics (TIA) services can help you improve your visibility on potentially high-impact threats and help your organization establish a more comprehensive cyber intelligence program to manage the cyber dimensions of business risk.

Today's sophisticated cyber adversaries exploit the unprecedented complexity of modern business environments. Determining when your most valued business operations and assets are under attack is more difficult than ever. It's not a purely technology effort, nor is it solely the domain of security analysts. It requires continuous awareness of threats on the horizon, and the ability to distill vast amounts of data into practical insights to empower efficient action by both business and technical teams.

Detect what matters – to you.

Security teams in large organizations may detect thousands of "bad" IP addresses, file hashes, domain names, or other threat indicators per day. Analysts sift through mountains of data, trying to determine which incidents might escalate into business crises. This data overload inhibits efficient threat detection – and it's also yesterday's data. Although threat feeds and signature-based detection tools may be important elements of a monitoring foundation, by their nature, they struggle to incorporate business context and simply can't keep up with how threats are evolving now.

When it's increasingly impossible to detect every infiltration, a business risk approach is more important than ever. Although there are threat trends common across industry sectors, many organizations have concerns specific to their operations. With guidance from senior leaders on which cyber risks are most critical, and with an understanding of the cyber threat tactics and methods, security teams can sharpen their focus on high-priority threats by instrumenting monitoring capabilities that prioritize alerts, and leveraging a balanced combination of automated threat data and tailored, hands-on threat research and analysis. It also helps inform the preventative control state that protect critical assets.

The whole organization needs to be threat-intelligent.

The security operations team is usually at the center of collecting and interpreting threat information, but a vigilant organization efficiently provides threat insights to a wide range of others, including IT architects and engineers, application developers, system administrators, employees, customers and partners, risk managers and senior executives. As the threat landscape changes, strong collaboration is needed to equip leaders to guide the cyber risk program, integrate threat awareness into innovation initiatives, adjust security controls, and educate people on the front lines of your operation to help defend the organization.

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.

Deloitte Advisory's Threat Intelligence & Analytics (TIA) Service

Through a range of advisory and managed services, **our professionals create a high-touch, tailored engagement** to advance organizational threat intelligence capabilities. Our TIA services consist of two categories of components that work in tandem to provide strategic and operational support to a client's threat intelligence program.

Advisory Intelligence

Deloitte Advisory works closely with clients on site to help them assess, enhance, and implement intelligence capabilities to reduce business-relevant cyber risks.

Threat Analysis & Research

Annual subscription service that provides client-specific threat insights and analysis delivered through a unified cyber portal. Our analysts deliver timely accurate, relevant, and predictive intelligence reports to help clients mitigate business risk.

Engagements are led by specialists with deep knowledge of applicable regulations, law enforcement and cyber intelligence, informed by Deloitte Advisory's broad experience across many industry sectors. Our approach has been refined through many effective engagements with multi-national companies, government entities, regulatory bodies, and industry groups, incorporating methods from industry, government, military and academic research. Our years of working closely with client security operations teams and on Deloitte Advisory's Managed Threat Services engagements demonstrates our ability to effectively operationalize intelligence.

To discuss your business or cyber risk challenges and solutions options, please contact your Deloitte Advisory engagement professional or contact:

Ed Powers
Deloitte Advisory National Managing Partner
Cyber Risk Services
Deloitte & Touche LLP
epowers@deloitte.com

Adnan Amjad
Deloitte Advisory Partner
Cyber Risk Services
Deloitte & Touche LLP
aamjad@deloitte.com

Keith Brogan
Deloitte Advisory Senior Manager
Cyber Risk Services
Deloitte & Touche LLP
kbrogan@deloitte.com