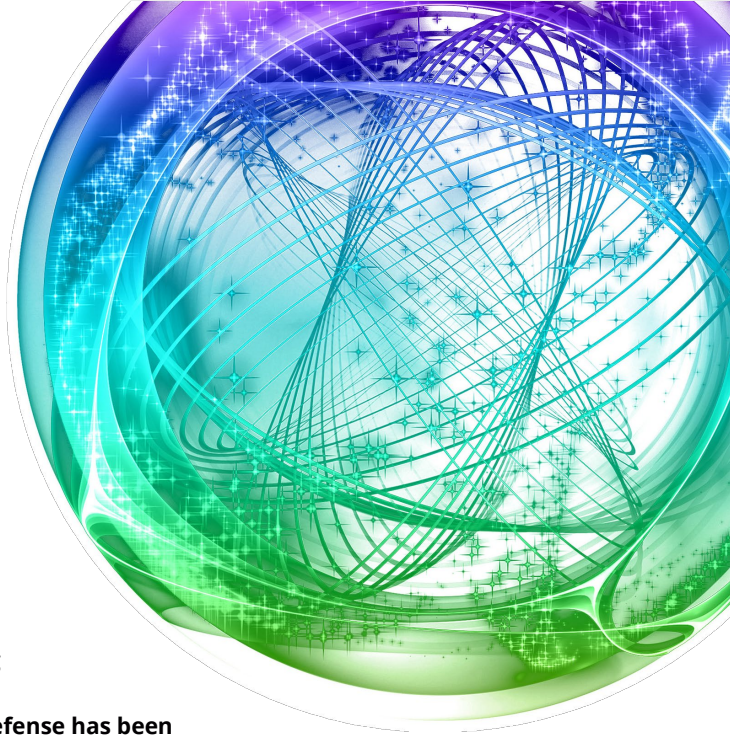
Deloitte.
counter-cybercrime.

Dynamic Adversary Intelligence

Deloitte.



Dynamic Adversary Intelligence

Cyber intelligence managed service

Successful cyber attacks aimed at financial, information, and operating infrastructure continue unabated despite enterprises deploying robust cybersecurity products and services. While playing aggressive defense has been the strategy of choice historically, many institutions now realize that defense is an insufficient approach. Investigative and anti-fraud teams need to be able to identify adversary technical and organizational infrastructure to facilitate recovery, takedowns, and arrests associated with ransomware, cryptocurrency, and other types of financial cyber-attacks. Deloitte Risk & Financial Advisory's (Advisory) Dynamic Adversary Intelligence (DAI) managed service is designed to help public and private sector organizations to bring a much more broad suite of tools to the existential battle for information security and business resiliency.

Achieve visibility of malicious actor's identity, tactics, techniques, and procedures

Understand the adversary: Achieve a broad perspective of the enemy/crime group/gang, their illicit support networks, how they operate, and what they are likely to attack next.

Identify the adversary: Prepare for technology disruption scenarios (including cyber incidents) with emphasis on security governance, strategic risk management, and supporting policies to effectively monitor and measure risk.

Achieve visibility of attacker operations: DAI does not require the deployment of any sensors or internal data sources, which facilitates expanded hunting into cloud and global attacker infrastructure. The Deloitte Advisory DAI team starts delivering actionable data on day one.

Increase resiliency of your business: Lower both the frequency of financial cyber-attacks and the cost of preventing them.

Reduce ransomware attacks: Focus on the future with deep understanding of the ransomware ecosystem to deter and deflect ransomware attacks.

Reduce fraud: Identify the behaviors of fraud and the organization behind it and thwart the criminal actions before it becomes fraud.

How Deloitte Advisory can help

Deloitte Advisory can help clients design, build, and operate dynamic, business-aligned security programs wherever they may be in their cyber journey. Deloitte Advisory's adversary intelligence capabilities and solutions help clients achieve peace of mind by fostering adaptability, confidence, and resilience to help them stay focused on driving better business outcomes.

Dynamic Adversary Intelligence Advantages

Play offense Provides actionable data (domains, IPs, company names, email addresses, etc.) to block, investigate, and serve legal process.	**Become a hard target** Raise the adversary's cost of reconnaissance and attack to the to the point that it becomes uneconomic to pursue.
Hybrid operations Complement enterprise cybersecurity team with the large Deloitte cohort of Master Operator/Hunter trained teams.	**Required tools and skills** Utilizes public and private data sources, leading analysis tools, and trade craft.
Enhanced threat visibility DAI focuses on the logical, persona, and physical layers of the adversary's infrastructure.	**Custom analytics** Enhance existing threat intelligence feeds faster, more efficiently, and at a scale

We utilize an intelligence-driven transformation approach to help you stop cybercrime:

- Improve **cyber resiliency** and **operations maturity**
- DAI requires **no sensors** and operates completely passively, blocking the adversary's visibility into the investigative process.
- **Learn and adapt** from internal and external intelligence to predict and prevent future attacks

The Deloitte Difference

We understand our clients' challenges and have a breadth of knowledge across risk domains. Utilizing the Deloitte cyber technology and data stack allows for lower operations cost. Our adversary and threat intelligence solutions are continuously enriched, helping some of the largest enterprise and government clients respond to threats. We bring these experiences together with our strong backgrounds in national security, intelligence, investigative, offensive and defensive cyber operations, and tactics and tool development.

Get in touch

For more information, please contact:

Curt Aubley
Managing Director
Detect & Respond Leader
Deloitte & Touche LLP
caubley@deloitte.com

Jennifer Vitalbo
Managing Director
Government Public Services
Deloitte & Touche LLP
jvitalbo@deloitte.com

Steve Mahar
Managing Director
Sales Leader
Deloitte Services LP
smahar@deloitte.com

Patrick O'Brien
Managing Director
Government Public Services
Deloitte Transactions and Business Analytics LLP
patobrien@deloitte.com