Deloitte.

CRAY THE SUPERCOMPUTER COMPANY

Cyber Reconnaissance and Analytics

Inverting the detection lens to preempt cyberthreats

The cyberthreat battle is often described as asymmetric: while defenders are compelled to plug every security gap in their complex, changing environments, the attacker only needs to take one successful action to achieve their "win." Deloitte Advisory's Cyber Reconnaissance and Analytics (Cyber Recon), powered by Cray, helps level the battlefield. *By revealing what your organization looks like to an adversary, and improving your ability to detect suspicious activity already occurring, Cyber Recon helps you take preemptive action to address potential weaknesses and proactively diagnose these behaviors to derail attack campaigns, many of which may already be "in progress" or part of a multi-staged attack.*

Changing the cyber intelligence paradigm

The alarming increase in the frequency and scale of cyber incidents is fueled partly by the ingenuity and persistence of cybercriminals themselves; however, the companies and organizations they target often provide fertile ground. The quest for operational improvement and innovation—whether through cloud services, mobile technology, Big Data, smart devices or other means of organization transformation—have led to explosive volumes of data, geometrically more points of entry, and therefore significantly more vulnerabilities, both in terms of size and complexity.

As leaders have become more aware that "bad guys" will get in—that perfect security defenses in the hyper-extended organization are highly unlikely—more resources are being allocated for cyber monitoring to improve threat detection. However, yesterday's monitoring is not by itself a match for today's cyberthreats. The typical detection program is designed to monitor as many of the organization's assets as possible, and to trigger alerts when known malware or cyberthreat indicators are identified in an effort to "patch" that specific vulnerability.

Some use advanced correlation logic to detect policy violations or subtle deviations in transaction processes. These are important foundations for a wide range of security operations functions, but they limit the ability to detect cyberthreats because they search for what was known about threats yesterday, rely on

pre-conceived attack scenarios to identify events, and generate petabytes of data faster than can be analyzed.

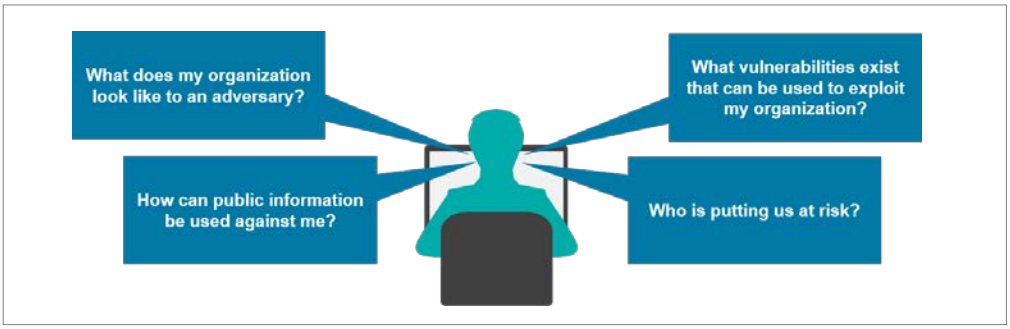
Only leveraging these approaches can lead to blind spots in the cyberthreat armor—and the inability to detect new types of attacks ("zero-days") or ones that are designed specifically to target your organization. Drowning in data and alerts, security operations teams may be unable to discern which issues require priority attention. Amidst the "noise" in the environment, malicious activity may easily find safe cover and go undetected for days, if not months—possibly until it's too late for an offensive response.

Thwarting the attack cycle

Cyber Recon services leverage vast amounts of data to provide a high-resolution "picture" of the client environment from the outside looking in. A person or group wanting to cause harm may first probe the organization, looking for system vulnerabilities and weak links. With these "holes" identified, various tools and malware are designed and implanted to enable their exploits.

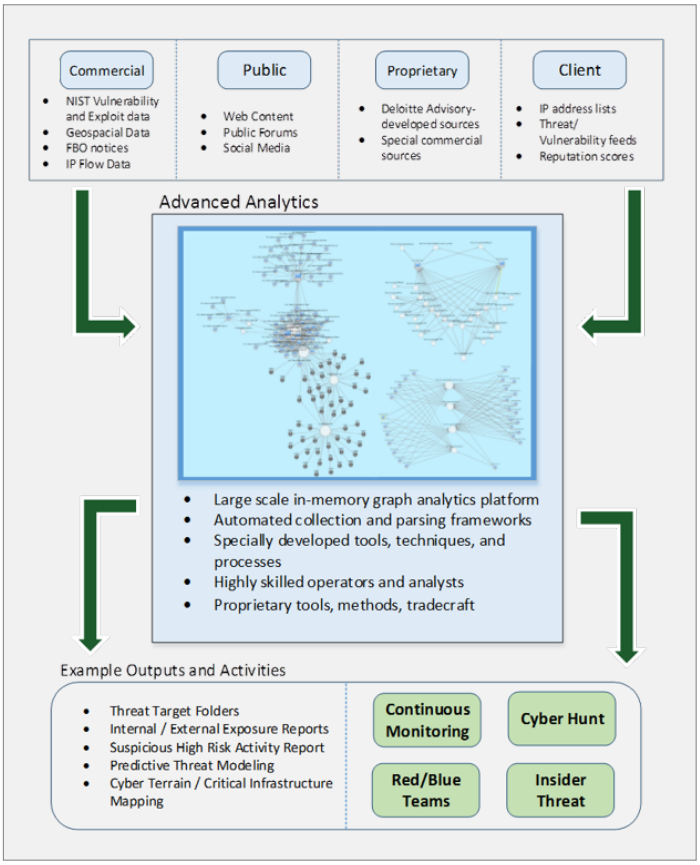
Cyber Recon creates visualizations of the organization's attack surface from the attacker's perspective so resources can be focused on addressing the vectors and vulnerabilities that the attacker can see, or taking other appropriate preemptive action. The ability to generate actionable cyberthreat insights in a complex environment requires three core elements:

1) Amassing the range of data needed to create a comprehensive view;
2) High-performance computing to process it;
3) People who understand the threat and organization risk landscape to design the most useful analytic queries and efficiently act on the output.



Essential questions Cyber Recon can address

Offering overview



Data sources can include a wide range of publicly available global, social, and commercial data sets, and proprietary information from both the client environment and provided through Deloitte Advisory's shared cyber operations environment.

High-performance analytics platform through Cray's Urika®-GX system provides:

- Hardware that can accommodate massive amounts of data in memory
- Software that can flexibly link data from multiple sources, supporting data analysis including both Hadoop® and Spark™ workloads, and ad-hoc queries on massive unstructured data for which Cray's Graph Engine database is ideally suited
- The speed needed to return reliable results in minutes or seconds

Deloitte Advisory analytic and data scientists leverage advanced algorithms to supplement your red and blue teams as needed to design queries that extract insights relevant to each client's business risk landscape. Deloitte Advisory brings industry-specific knowledge of business risk and threat trends, current threat research, and active field-level engagement with a wide range of large, complex organizations.

Examples of Deloitte Advisory/Cray Cyber Reconnaissance Results

- **DISCOVERED** 1,000+ exploits that could be leveraged to gain entry into client organizations
- **IDENTIFIED** 250+ companies in various organizational networks beaconing to the same Internet Relay Chat (IRC) servers, indicating malicious activity
- **UNCOVERED** privileged targets, including critical personnel and infrastructure
- **LOCATED** servers hosting malicious activity and suspicious traffic to web providers hosting illegal activities
- **FOUND** potential entry points for spear-phishing using social content from an online resume

Why choose Deloitte Advisory's Cyber Recon services?

See what matters. Help security operations teams cut through data overload to zero-in on exploitable threats or vulnerabilities from an attacker's perspective, and support enriched cyber risk reporting to executives.

Disrupt or detect earlier in the cyberattack cycle. Help security teams identify seemingly innocuous tools, but which may signal initial stages of attack activity that may evade traditional monitoring activity.

Scale detection without a performance "hit." Because it uses passive data collection, Cyber Recon requires no agents or sensors, creates no extra network traffic, and introduces no infrastructure management tasks—so security teams can stay focused on their core cyber risk mitigation functions.

Achieve results faster. Cyber analytic solutions are widely touted, but achieving real results can be slow and painstaking. Standing up the computing and data integration capabilities takes time. Even more challenging, many organizations lack the diverse skills needed to design organization-aware queries and interpret the output. Deloitte Advisory's services, built on Cray's industry-leading analytics platform, provide a turn-key foundation and specialized analytics professionals who help tailor powerful automation to your business risk environment—to find the threats that matter to your organization.

Take action today! Request a briefing.

Deloitte Advisory Contacts

Deborah Golden
Principal | Deloitte Advisory
Deloitte & Touche LLP
debgolden@deloitte.com

Adnan Amjad
Principal | Deloitte Advisory
Deloitte & Touche LLP
aamjad@deloitte.com

Gordon Hannah
Principal | Deloitte Advisory
Deloitte & Touche LLP
ghannah@deloitte.com

Cray Contacts

Nitin Mittal
Director | Partner Relations
Cray Inc.
nmittal@cray.com

Tim Barr
Segment Leader | Cybersecurity
Cray Inc.
tbarr@cray.com

Chris Hegarty
Senior Manager| Analytics
Cray Inc.
chegarty@cray.com

About Deloitte

About Cray

Supercomputing leader Cray builds innovative systems and solutions enabling researchers in any discipline to meet existing and future simulation and analytics challenges. Leveraging 40 years of experience developing and servicing the world's most advanced supercomputers, Cray brings you a comprehensive portfolio of high performance computing (HPC), storage and data analytics solutions delivering unrivaled performance, efficiency and scalability. With a solution for every budget and need, Cray makes it easy to take advantage of HPC advancements.