THREATCONNECT®

Deloitte.

GAINING SITUATIONAL AWARENESS Threat intelligence services to manage cyber risk

A FLOOD OF IRRELEVANT DATA OR TARGETED INSIGHTS?

To obtain intelligence that enables business decisions about managing cyber risk, organizations have historically hired dedicated teams to piece together multiple data sources and integrate with their diverse technologies. The most common challenges we hear from our clients are:

- On the scale of data, information, and intelligence, they have lots of threat intelligence data, but very little useful information. They **struggle to gain actionable intelligence** ahead of the threat.
- They **don't receive the answers** to their questions about the cyber threats that are relevant to their organization or industry.
- Their disparate teams, both internal as well as vendor-provided, don't "connect the dots" when identifying or responding to threats; **they don't share information or feedback**, and consequently, the implementation of controls either lags behind current threats, or their efforts are duplicative.

These challenges are not out of the ordinary and lead most internal cybersecurity teams to spend significant time solving operational issues or filtering out "the noise," instead of focusing on making the organization more secure. They are further compounded by:

- **Significant lag** between the initial discovery of a relevant threat, obtaining actionable information about that threat, and integration with enterprise cyber defense and visibility mechanisms.
- **Lack of efficient and secure mechanism** to collaborate and share actionable intelligence with peer teams and partners.
- Multiple and disparate platforms with different threat intelligence and **no single point of consolidation** to support consumption by disparate cyber operations, business, and information technology teams.
- **Lack of mechanism** to evaluate the quality and efficacy of the intelligence received in addressing business requirements.

LEVERAGING AUTOMATION TO REDUCE THE LAG BETWEEN DISCOVERY AND REMEDIATION

The solution to these problems has several essential components:

- Threat intelligence that aligns to specific requirements
- A technology platform that supports collaboration, sharing, and integration
- Professionals that execute the intelligence lifecycle based on defined procedures

Using ThreatConnect as a foundation, Deloitte offers two services to help organizations, which can be combined as needed, achieve this target state.

TIGHTLY INTEGRATED CYBER OPERATIONS SERVICES FOCUSED ON THREATS SPECIFIC TO YOUR ENVIRONMENT

Service Option 1: Subscription Services

For clients looking for a subscription service, Deloitte combines the strengths of a community-powered, industry-leading cybersecurity platform with integrated threat insights derived from a requirements-driven approach.

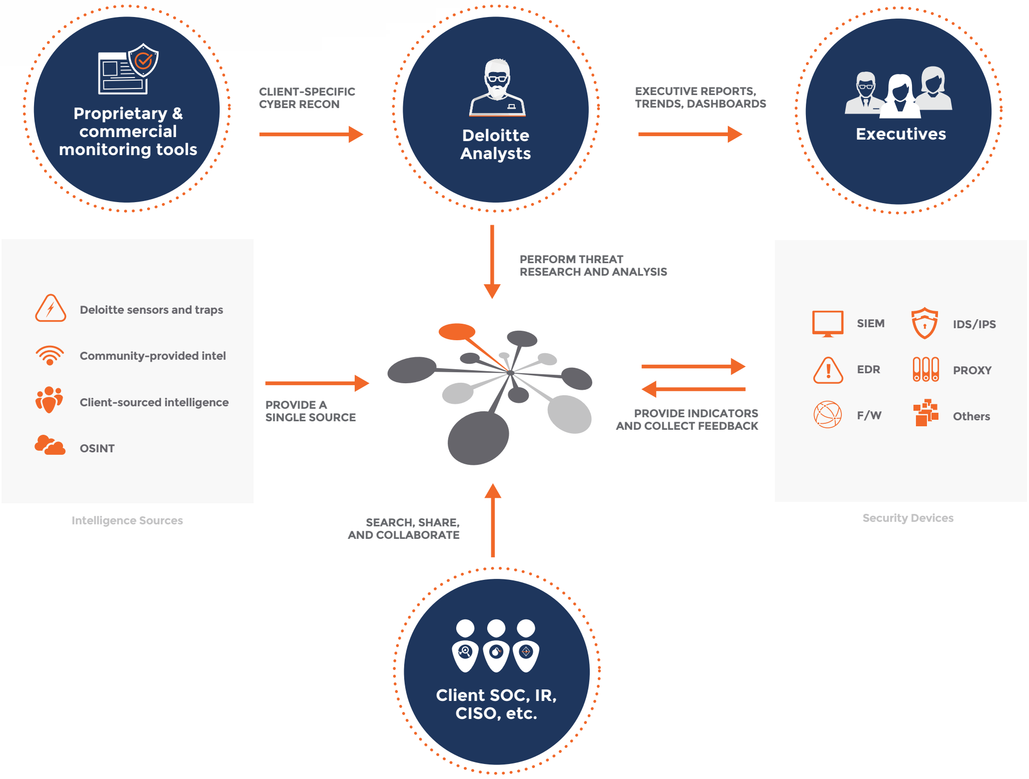
Features of the service include:

- Intelligence based on industry and client-specific Prioritized Intelligence Requirements (PIRs) that derive threat insights relevant to a client's business. Powered by ThreatConnect, Deloitte's services **filter out the noise** to help your team focus on what matters.
- A cybersecurity platform that comes **packed with intelligence** drawn from multiple, vetted, open and proprietary sources that are constantly updated. This data is continuously enriched with contextual data from commercial sources, community shared intelligence, and Deloitte's internal threat research.

The cybersecurity platform allows clients to:

- **Share intel and collaborate** with various stakeholders during the normal course of business, including the assigned security operations analysts, information technology operations, and public or closed peer communities.
- Enable **automated delivery** of high-fidelity machine-readable observables to your security information and event management (SIEM) technology and other threat defense tools–reducing the lag between discovery, visibility, and remediation.
- Compare the **effectiveness and quality of intelligence** data by automatically collecting feedback from integrated technologies that provide visibility into matched observables or false positives.
- Ingest additional intelligence sources into the same cybersecurity platform (in addition to the Deloitte supported feeds) resulting in a **single aggregated and normalized source** for threat intelligence.

Threat Intelligence Subscription Services



Proprietary & commercial monitoring tools
CLIENT-SPECIFIC CYBER RECON
Deloitte Analysts
EXECUTIVE REPORTS, TRENDS, DASHBOARDS
Executives
PERFORM THREAT RESEARCH AND ANALYSIS
Deloitte sensors and traps
Community-provided intel
Client-sourced intelligence
OSINT
Intelligence Sources
PROVIDE A SINGLE SOURCE
PROVIDE INDICATORS AND COLLECT FEEDBACK
SIEM
IDS/IPS
EDR
PROXY
F/W
Others
Security Devices
SEARCH, SHARE, AND COLLABORATE
Client SOC, IR, CISO, etc.

Reducing the lag between discovery and response

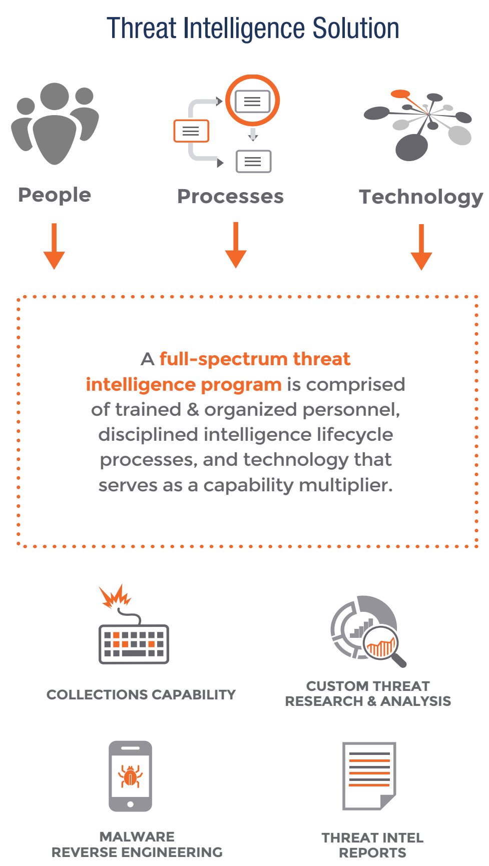
Service Option 2: Advisory Services

TO BUILD OR MATURE AN EXISTING INTELLIGENCE PROGRAM

For clients looking to build or mature their internal intelligence capability, Deloitte can assist with establishing or integrating ThreatConnect into new or existing threat management and security operations functions to help clients:

- Establish an **initial operational intelligence framework** through the definition of requirements, creation of procedures, and integration of ThreatConnect.
- **Mature their existing intelligence programs** through the integration of ThreatConnect to create a single platform for collaboration, sharing, and analysis.
- Build and operationalize a **mature threat intelligence capability using ThreatConnect**, including definition of requirements, creation of a collections capability (internal or through vendor selection), development of operating procedures, and training for development of finished intelligence products.

Deloitte's experience with companies of varying maturity provides for an approach that can be adapted to your needs, regardless of where you are on the spectrum and whether you have an intelligence capability today or are starting from scratch.



Threat Intelligence Solution

A **full-spectrum threat intelligence program** is comprised of trained & organized personnel, disciplined intelligence lifecycle processes, and technology that serves as a capability multiplier.

COLLECTIONS CAPABILITY
CUSTOM THREAT RESEARCH & ANALYSIS
MALWARE REVERSE ENGINEERING
THREAT INTEL REPORTS

Deloitte's diverse advisory intelligence team comes from law enforcement, federal defense agencies, and commercial intelligence backgrounds, and have experience with a wide variety of industries and environments.

Solution Advantages

- Unite people, processes, and technologies behind a cohesive, intelligence-driven defense against threats
- Automate aggregation, normalization, enrichment, and distribution of intelligence via ThreatConnect
- Pivot from one data point to another, uncover patterns, and gain a full picture of your adversaries' tools, tactics, and procedures (TTPs)
- Contribute to and draw from trusted communities to build a shared knowledge resource of common threat actors and tactics

WHY CHOOSE DELOITTE'S THREAT INTELLIGENCE SERVICES POWERED BY THREATCONNECT

Together, our combined offerings help clients build an intelligence-driven threat defense:

- Delivers strategic, operational, and tactical intelligence to all major stakeholders that can provide **a single reference source to facilitate decisions** by different teams based on same information.
- **Leverages automation** to embed threat intelligence into security operations.
- Provides an **enterprise-wide view of threats to your organization** and how they are being mitigated, and a means of measuring the effectiveness of the intel we provide.
- Uses defined workflows to **reduce the time from threat discovery** and identification to response.
- Makes it easier to tune intelligence data based on feedback from peers, and data from your own environment, thus completing the intelligence lifecycle.

Deloitte.

Secure.Vigilant.Resilient.™
Deloitte's approach to managing cyber risk.

To grow, streamline, and innovate, many organizations have difficulty keeping pace with the evolution of cyberthreats. The traditional discipline of IT security, isolated from a more comprehensive risk-based approach, is not likely to offer adequate protection. Through the lens of what's most important from a business risk standpoint, organizations must invest in cost-justified security controls to protect their most important assets, and focus equal or greater effort on gaining more insight into threats, and responding more effectively to reduce their impact. Deloitte works with clients design, build and operate Secure.Vigilant.Resilient. cyber risk programs that can help them become more confident in their ability to reap the value of their 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.

Take action today! Request a briefing.
For more information visit **www.deloitte.com/us/cyberrisk** or contact Keith Brogan at **kbrogan@deloitte.com**.

ThreatConnect Contacts

Michael Mullins | **Vice President, Strategic Alliance, MSSP & Channel Partner Sales**
mmullins@threatconnect.com | 703.727.6019

Lincoln Turner | **Director, Strategic Alliances and MSSPs**
lturner@threatconnect.com | 214.763.0218

Gene Barlow | **Solutions Architect**
gbarlow@threatconnect.com | 303.912.9575

ABOUT THREATCONNECT

ThreatConnect, Inc.® unites cybersecurity people, processes and technologies behind a cohesive intelligence-driven defense. Built for security teams at all maturity levels, the ThreatConnect platform enables organizations to benefit from their collective knowledge and talents; develop security processes; and leverage their existing technologies to identify, protect and respond to threats in a measurable way. More than 1,200 companies and agencies worldwide use ThreatConnect to maximize the value of their security technology investments, combat the fragmentation of their security organizations, and enhance their infrastructure with relevant threat intelligence. To register for a free ThreatConnect account or learn more, visit www.threatconnect.com.

ABOUT DELOITTE

This document contains general information only and Deloitte is not, by means of this document, rendering accounting, business, financial, investment, legal, tax or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this document. As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.