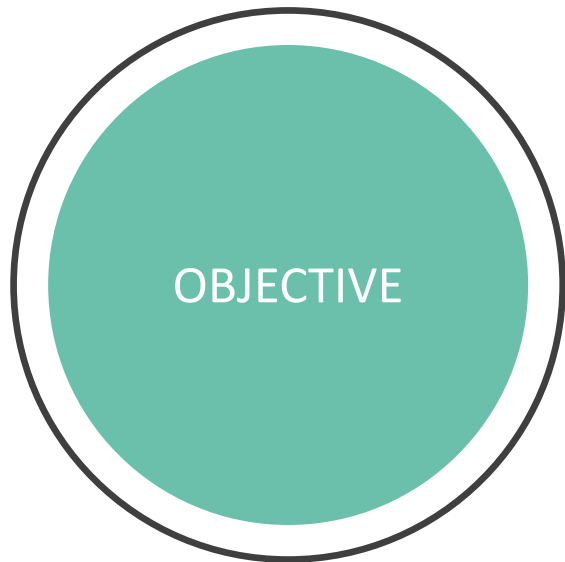


# **Executive Intelligence Security Services**

*Discovering Your Risk from an Adversarial Perspective*





1. Provide the kind of security intelligence that enhances protection for executives.
1. Provide the capability to understand relevant targets from an adversary perspective, paired with valuations of critical digital-cyber and physical risk vectors.
1. Proactively identify potential security threats and vulnerabilities, discover emerging threats, and prioritize risk through valuation. Clients can better protect themselves and their organizations.

## **Purpose**

Deliver a professional service that helps client be proactive, prioritize resources, and understand adversaries through a quantified method and risk framework for improved security resilience.

# The Threat Environment

Executives have become easy targets for threat actors evident from a significant increase in both criminal and nation-state operations that are zeroing in on executives as the initial point of attack.

---

Attackers lever publicly available information to learn about their target of choice and discover vulnerabilities to plan and carry out an attack. Reasons for these attack vary depending on motivating factors such financial reward, ideological, espionage or even physical harm.

---

Here are just five methods among many that threat actors use to target executives.

---

Data broker profiles:	Data broker profiles are risky for executives because they contain privileged information which hackers can leverage. Such as home IP addresses, passwords and financial information stored in the Dark Web and and confidential information about their family, relatives, and neighbors.
Home network and devices:	An executive's home network and connected devices are a perfect target for hackers because it is usually not set up securely and as a result becomes a vector to exploit.
Personal accounts:	One compromised Gmail or LinkedIn account can quickly snowball into several hijacked accounts, potentially leading to a full corporate breach.
Document extortion:	Threat actors expose any sensitive document, file or written correspondence that would be embarrassing to the executive if publicly exposed. The most common extortion materials are legal documents, tax records, medical files and personal photos.
Family members:	An executive's children and spouse are often less physically protected and less cyber-aware, which makes them an easier target for exploitation and extortion.

---

# Open-Source Intelligence Enhances Executive Protection

Importance: OSINT allows organizations to identify risks, continuously monitor for emerging hazards, and validate identified threats. Additionally, OSINT can also identify information threat actors might use to attack an executive or their organization.

How its leveraged: OSINT can be leveraged for many physical security applications from investigations and executive protection to crisis response and travel security.

**Executive Protection:** OSINT represents an essential tool for security details when conducting an initial threat assessment. Continuously monitoring open sources could also reveal new risks to a principal, such as stalkers, doxxings, misinformation, and violent threats.

**Crisis Response:** Continuously monitoring open sources can alert security teams of an emergency situation or potential threat. Further intelligence gleaned from public data could prove essential when planning a response or coordinating proactive security efforts.

**Loss Prevention:** Criminals are experts at exploiting technology to conduct their operations. Monitoring open sources can allow asset protection teams to learn about new tactics, upcoming attack campaigns, or particular products thieves like to counterfeit (and where they distribute them online).

**Data Leak Detection:** From time to time, company insiders may publish photos or information online that exposes the organization to new risks. For example, a single post on social media could accidentally expose the location of a VIP or reveal confidential company data. Continuous monitoring of open channels can allow security teams to spot and address these incidents before they become serious security risks.

**Event Security:** Open-source intelligence protects executives by enhancing protection at venues, prevent information leaks, and keep events running smoothly..

**Asset Monitoring:** OSINT helps to proactively identify operational vulnerabilities that could lead to disruptions or threats. For example, this might include suspected reconnaissance or vulnerabilities that certain threat actors target.

**Travel Security:** Teams can obtain real-time updates of global travel advisories by monitoring threat intelligence feeds, conducting research about location. Analysts can advise clients with a certain level of confidence sense of what's happening on the ground and what to expect.

**Investigations:** In our new and growing digital age, OSINT has become an increasingly common skill set for investigators. It now represents an essential tool when investigating fraud, theft, or other types of crimes.

## Customized Services

Tailored by design to support executives and high valued individuals.

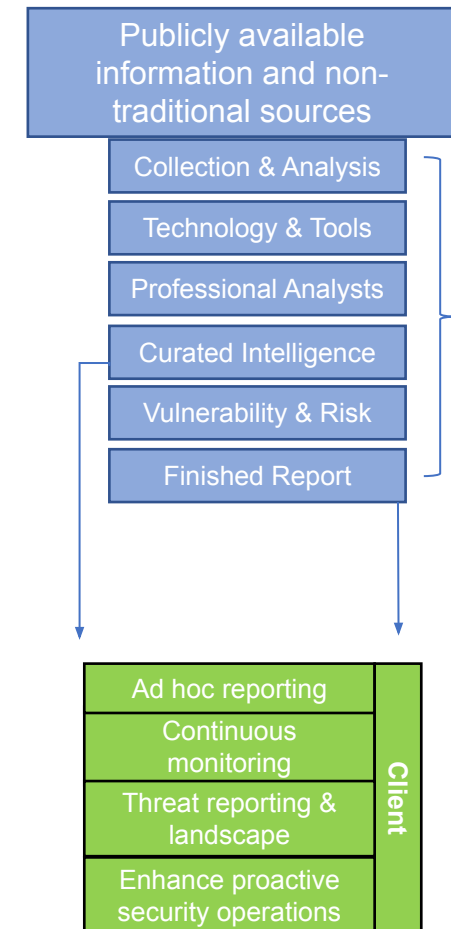
- ✓ Situational awareness and threat reporting
- ✓ Supports executive travel planning and security
- ✓ Personal brand detection and notification
- ✓ Investigative services
- ✓ Continuous threat monitoring
- ✓ Ad hoc request for new intelligence requirements
- ✓ Enhance security, protection, and privacy

## Approach

We scope and define client's intelligence requirements and formulate a customized approach for relevant intelligence gathering, analysis, and reporting.

- Personal intelligence collection, monitoring, and security reporting
- Access surface and dark web content to conduct risk and vulnerability assessments specific to client intelligence requirements
- Provide relevant and up-to-date intelligence on threat actors and adversaries most likely to exploit or act against a client's interest
- Help clients understand geopolitical trends and potential security risks to their personnel or organizations
- Conduct intelligence gathering on individuals to discover potential physical security risk, imminent harm or suspected criminal activity
- Conduct Technical OSINT for cyber vulnerabilities and risk assessments in the client's mission space, research on cyber threat actors, their TTPs, and indicators of compromise

**Our experts conduct thorough intelligence assessments utilizing Open-Source Intelligence (OSINT) research and analysis. We help our clients prioritize and understand their vulnerabilities and risks with intelligence informed, actionable risk evaluation findings and develop long-term resiliency strategies.**



# Digital Adversary Threat Assessment-Quantification (DATA-Q)

- DATA-Q includes Intelligence Community analytic standards for tradecraft in threat assessment and confidence reporting to ensure the solution is focused on end-user needs.
- DATA-Q is a tailorable, scalable, and repeatable threat assessment framework that delivers quantified prioritized risk intelligence to inform executives and decision makers of risk posture.

## **Prioritize and Visualize Digital-Cyber and Physical Risks Posture**

DATA-Q provides an intelligence-based foundation for prioritizing personal security resources, adopting digital-cyber and security modernization solutions while providing executives the information necessary to make corrective decisions and maintain resilient operations.

## **Digital-Cyber reconnaissance and OSINT analytics service**

Together, digital-cyber reconnaissance and OSINT analysis can provide a comprehensive view of the digital-cyber threat landscape and help Clients mitigate potential cyber and physical threats.

## **Adversary threat**

Discover and identify known threat actors to recognize potential motivations, tactics, and targets. This can help Clients understand the types of threats they are likely to face and develop effective countermeasures.

## **Threat actor hunting**

Identify and categorize threats and adversaries that may pose a risk to Clients or other high-profile individuals.

## **Operational support and improvements**

Proactively identify potential security threats and vulnerabilities, discover emerging threats, and prioritize risk through valuation. Clients can better protect themselves and their organizations.

- Vulnerability and threat assessment
- Threat surface illumination
- Risk based consequence and quantified scoring
- Enhanced value of personal protection services
- Establish risk common operating picture

**Adversary focused risk quantification for improved security resilience.**



# DIGITAL ADVERSARY THREAT ASSESSMENT-QUANTIFICATION (DATA-Q)



## A METHODOLOGY BASED ON AN ADVERSARIAL RISK PERSPECTIVE

Threat identification and characterization identifies adversaries most likely to exploit risks in the client's mission space or personal life with empirical best fit capabilities.



## LIKELIHOOD AND IMPACT

Measures risk impact translated into quantifiable variables consistent with standards of evaluation from the Intelligence Community and Cyber Industry best practices.



## CONFIDENCE REPORTING AND RESILIENCY STRATEGY

Transparent reporting consistent with Intelligence Community Analytic Standards, supports RFI, and continuous monitoring for indicator updates as conditions change or new information becomes available.



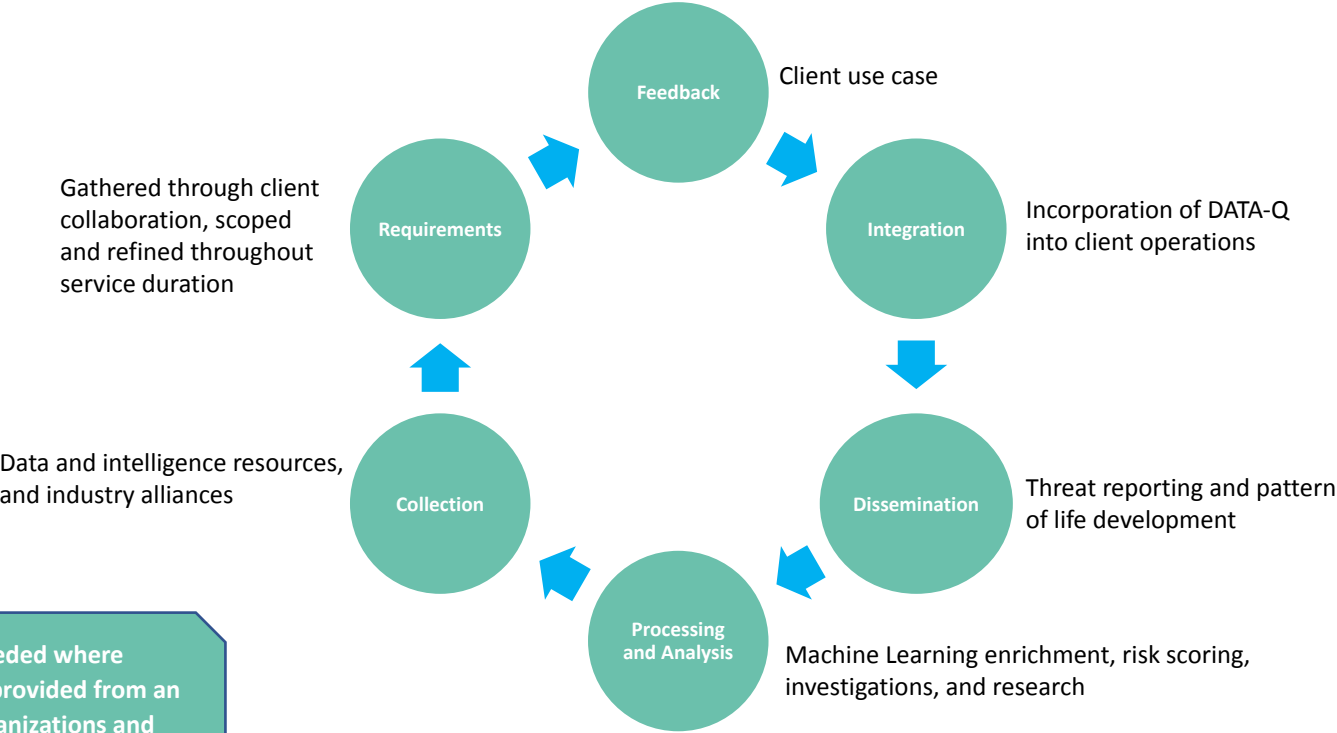
# Digital adversary Threat Assessment-Quantification (DATA-Q)

**DIGITAL ADVERSARY THREAT ASSESSMENT-QUANTIFICATION (DATA-Q)** is an advanced digital-cyber risk quantification methodology that involves cyber tradecraft and open-source intelligence (OSINT) collection, curation, analysis, risk prioritization, and threat relevant reporting. Tailored toward client specific, VIP and executive personnel risk analysis for visibility, threat trends, and reporting.

**The differentiator of the DATA-Q capability comes from the real-world, data-driven decision-making support for clients. Incorporating discovery from the adversary perspective clients are given relevant risk, real-world adversaries, and threat actors aligned to exploitation of identified risk.**

DATA-Q
Experienced team of intelligence and cyber professionals with multi-disciplinary skillsets
Evidence based reporting through OSINT collection and analysis
Digital adversarial threat assessments derived from open, deep, and dark web sources to identify and mitigate risk to VIPs and organizational operations
DATA-Q quantifies risks in the logical and digital-cyber realms from an adversarial point-of view

## DATA-Q Intelligence Life Cycle



Service/Deliverables
A comprehensive methodology based on an adversarial risk perspective
Data science and Machine Learning, human analysis, and Intelligence-grade reporting
Measures risk impact translated into quantifiable variables
Transparent reporting consistent with Intelligence Community Analytic Standards

**Value + Impact= Delivery**

Discover vulnerabilities and risks that are public, available, and exploited by threat actors

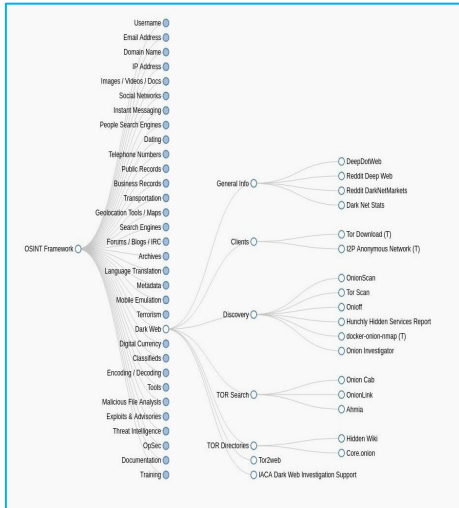
Clients can look through the eyes of an attacker and discover and understand Vulnerabilities and threats.

Decision makers are given the ability to visualize and prioritize risks for mitigation and improve operational resiliency

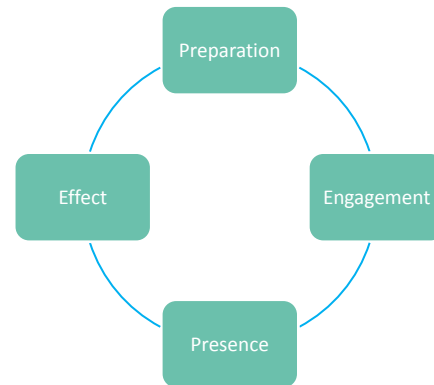


# DATA-Q Framework and Methodology

The OSINT framework simplifies the process for data collection, research, intelligence gathering, and reconnaissance.



## Adversarial Target Exploit Mapping



## Digital Discovery

Gather publicly accessible data for indicators of compromise and exposure.

Analyze data for information and gather intelligence.

Discover vulnerabilities, create digital profile, geospatial mapping, and pattern of life.

Monitor and expand threat surface of target-victim

Achieve offensive dominance, develop attack plan, create crisis situations, carry out attack.

Digital cyber vulnerability assessment

Threat surface illumination

Adversary risk quantification metrics

## CARVER Method (Matrix)

**CARVER involves the evaluation of six Impact Analysis Factors (IAF): 1) Criticality, 2) Accessibility, 3) Recuperability, 4) Vulnerability, 5), Effect, and 6) Recognizability**

**Each of the IAFs are assigned a severity score 1-10: From negligible/unknown (1-2), limited (3-4), serious (5-6), severe (7-8), and catastrophic (9-10).**

**Originally used by Special Operations Forces for targeting and mission planning and has since been adopted by numerous agencies to evaluate risk as an offensive targeting prioritization tool.**

DATA-Q's metrics scoring methodology for targeting and mission planning is the foundation for Attack Surface Illumination and risk prioritization.

Incorporates the adversary perspective by determining the impact of risk to a person or organization.

Scoring the adversary's assessment of risk to mission impact through six Impact Analysis Factors directly translates to defensive response prioritization.

Notable example of its use: Sabotage against Iranian nuclear program known as "STUXNET."



# Pricing

## EXAMPLE: Executive Package: Executive Intelligence Security Service

Service	Quantity	Rate	Monthly Total	Annual Total
Data-Q (optional discount service for annual customers)	60-120 hours.	2 FTEs		Capped at \$15,000 as part of package.  <i>Marked down from \$24,000</i>
Threat reporting & continuous monitoring	1	2 FTEs	\$15,000	\$180,000
Executive travel	1	1 FTE	-	-
Ad hoc request (covers any additional line of service offered at discount rate).	Scoped at 40 hours. Client receives year- round ad hoc reporting for the price of one.	1 to 2 FTEs depending on scope	-	\$8,000
Total				<b>\$203,000</b>

*All services are billed at a rate of \$200 per hour for Clients not enrolled in annual package deals.*

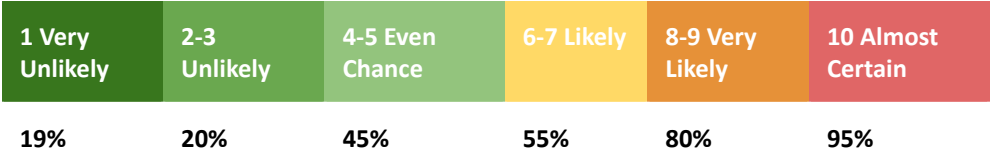
# CARVER Method Risk Quantification



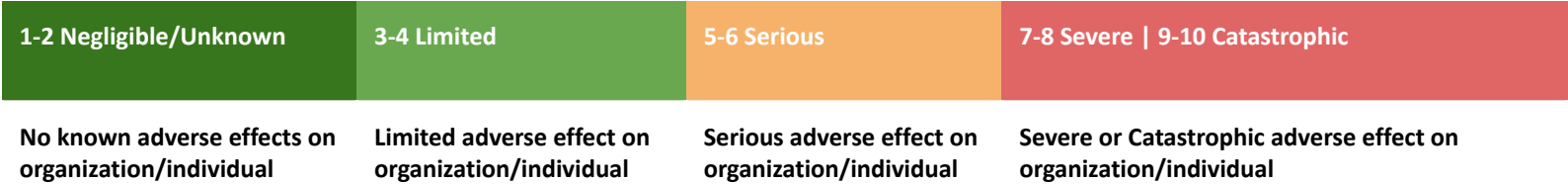
Rating	Description
High	High confidence in rating, strong basis for key considerations.
Medium	Reasonably confident in rating, some basis for considerations.
Low	Low confidence in rating or confidence could not be rated due to significant gaps.

Criticality	Describes level of importance the target has and relative value to an attacker.
Accessibility	An assessment of the placement and expertise required for an attacker to reach an asset.
Recognizability	Measures an adversaries’ knowledge of a target
Vulnerability	An assessment of the capability of an attacker to achieve the desired effect against a target.
Effect	Measures advantages and disadvantages of a given action in terms of collateral impacts and public perception.
Recuperability	Determines impact of loss, the cost required to replace or repair following an attack or compromise in terms of time and resource expenditure.

Likelihood factors are scored individually from 1-10 based on assessed likelihood of an adversary attempting to exploit a target based on Criticality, Accessibility, Recognizability, Vulnerability.



Severity factors are scored individually from 1-10 based on assessment of the severity of mission consequence and the Effect of a successful attack and Recuperability of the target following an attack.



DATA-Q has established a clear and transparent method for evaluating and reporting confidence associated with assessment factors aligned with Intelligence Community tradecraft guidelines for sourcing and estimation: High Confidence (H), Moderate Confidence (M), or Low Confidence (L).

(See Intelligence Community Directive 203 Analytic Standards).

Risk prioritization is achieved through ranking risk vectors by the overall mission risk score—the sum of all likelihood and severity variables.

# DATA-Q Advanced Analytics

## Machine Deep Learning



Analyzes complex volume data structure in an optimized model to identify significant relationships and patterns that are risk associated.

## Neural Network Modeling



A neural network is composed of a vast number of highly interconnected processing elements (neurons). The network of neurons individually work together toward a purpose such as data classification and pattern recognition.

DATA-Q's advanced analytics places high emphasis on adversaries' capabilities and decision making. Our analytic models are designed for high-level focus on attackers' behaviors and intent enabling VIPs and organizations to implement proactive defenses based on their adversary's intents and capabilities.

Scalability

Integration

Efficiency

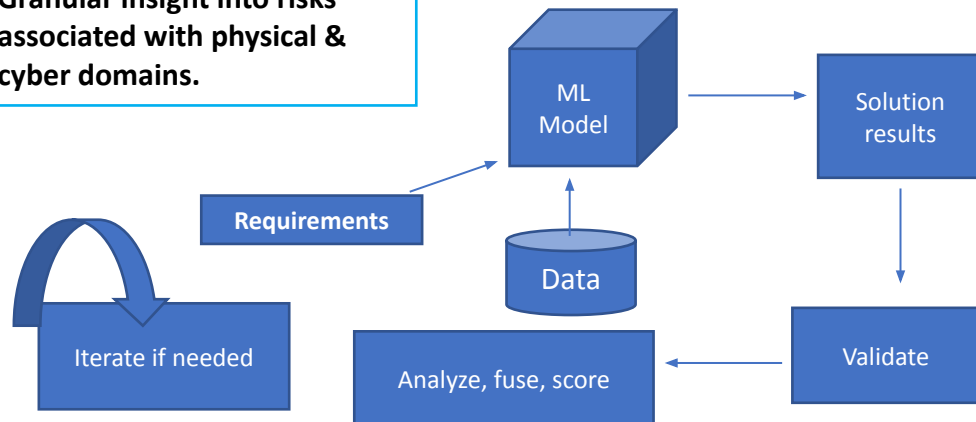
Identify

Indicators, capabilities

Predictive-Actionable

Human evaluated, recommendations

Granular insight into risks associated with physical & cyber domains.



Predictive risk analysis provides threat outcomes, visualizes threat surface, and provides threat specific insight to enhance strategic risk mitigation strategies.