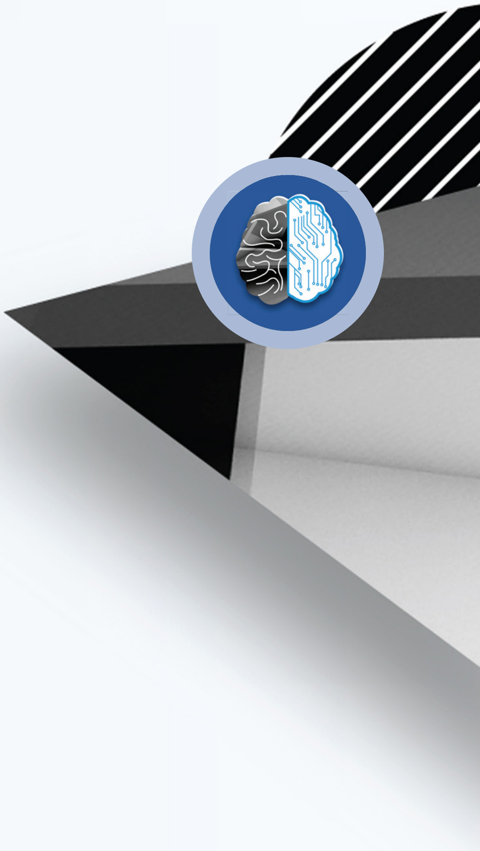
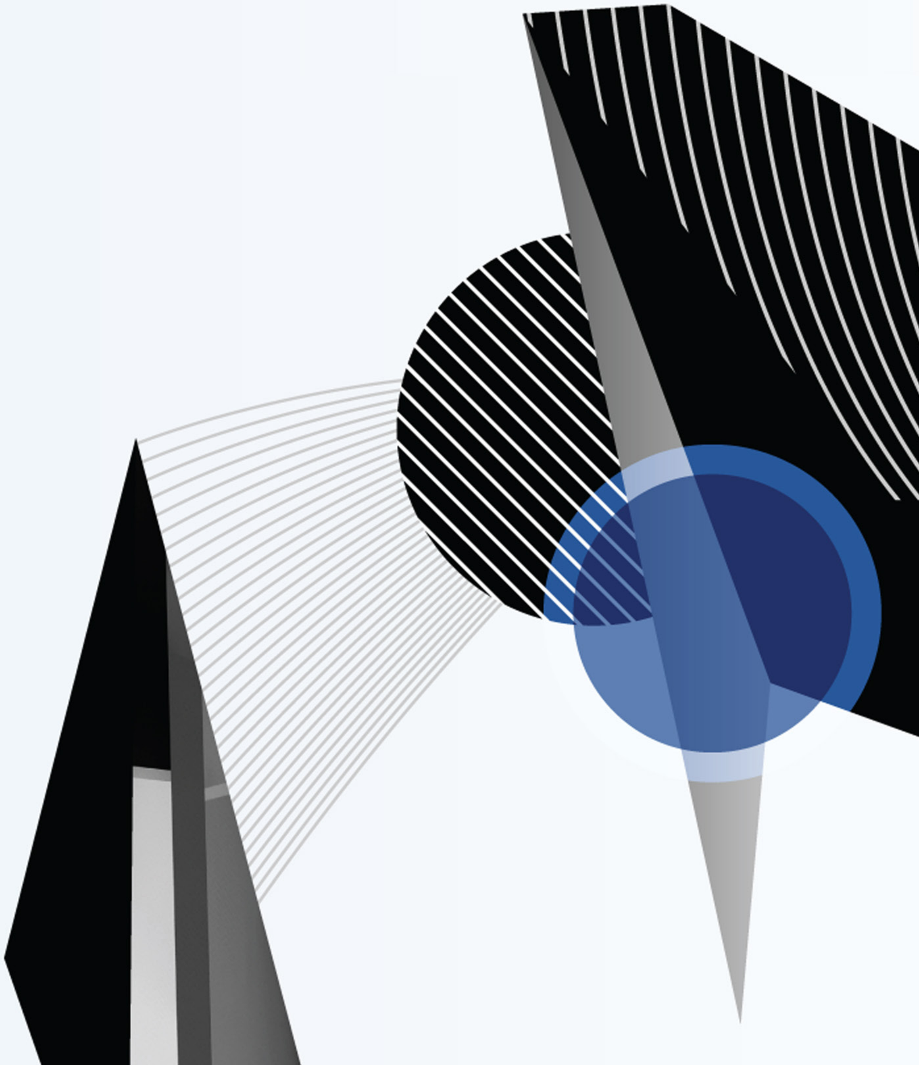
WHITE PAPER



FireEye

Intelligence First

How threat intelligence enriches security consulting services



Introduction

Organizations of all sizes are facing ever-evolving cyber threats as they struggle with limited budgets, a shortage of skilled security professionals and increasing regulatory disclosure requirements. Today's sophisticated attackers often hide within the noise of numerous alerts generated by security products.

To identify and combat these threats, security teams must master the workings of a myriad security products and understand how attackers think and operate. Timely, relevant and actionable threat intelligence enables risk-based decision making to effectively and efficiently protect the business. The right intelligence can transform cyber security into a competitive advantage and help organizations outmaneuver attackers.

Business and security leaders are reacting by turning to cyber security consulting services to help evaluate and mature their current program, manage risk and build scalable sustainable security programs. Choosing the right service provider from among thousands of vendors, including traditional management consulting firms, niche companies and consultants specializing in cyber security can be challenging.

Security-conscious organizations are best served by service providers that work intimately with and stay abreast of the constantly changing cyber landscape.

Limitations of traditional cyber security consulting

The traditional (non intelligence-led) approach to cyber security consulting services is based on general best practices, generic standards and industry groupings. It relies on open-source intelligence for insights into attacker tactics, techniques and procedures (TTPs). While useful, these approaches may not factor in the realities of today's modern threat landscape.

Consultants using a traditional approach are prone to gaps in their analysis. These may include the inability to stay abreast of changes in threat actor TTPs, leading to ineffective recommendations or inefficient remediation efforts—often resulting in an environment that is more prone to repeated compromises by similar attack groups.

Some consultants rely heavily on publicly available open source attack information. Relying too much on open source information has consequences. When considering open source intelligence, you must carefully evaluate the information's timeliness, quality and relevance to your organization. The level of effort required to consume, validate, and apply publicly shared indicators to existing organizational processes can make it very difficult to use relevant data and detect security events in real-time.

An organization's risk profile and internal risk tolerance play a significant role when determining the appropriate level of security needed. Understanding management's acceptable level of cyber risk informs which critical business assets must be protected to avoid material business disruption. Knowledge gaps in the organization's specific threat landscape and executive-level security expectations can lead to generic recommendations that often result in ineffective vulnerability management.

Without the benefit of timely, relevant threat intelligence, security consultants can only offer support informed by compliance requirements, best practices and industry standards which are not adapted to the latest attacker TTPs and tailored to the organization based on threat profile and risk tolerance.

Role of Intelligence in Consulting

Security consulting

Effective cyber security consulting improves the overall security posture of an organization before, during and after an incident occurs. It requires an in-depth knowledge of threat actor TTPs, along with an understanding of attacker motivations. This intelligence provides consultants with valuable information on how attack groups gain access to target environments, as well as their intent and methods of operation, answering questions such as:

- What threats are relevant and why?
- What are the potential business or operational impacts of specific cyber attack scenarios?
- What assets are these threats targeting?
- What tools, software and systems do these attackers use?
- Which vulnerabilities are exploited based on the tools, software and systems used?
- What does an organization's prioritization of security controls look like?
- How should an organization prevent, detect or respond to these threats?
- How can an organization focus on and prioritize threats that pose the greatest risk?

Cyber Risk Management

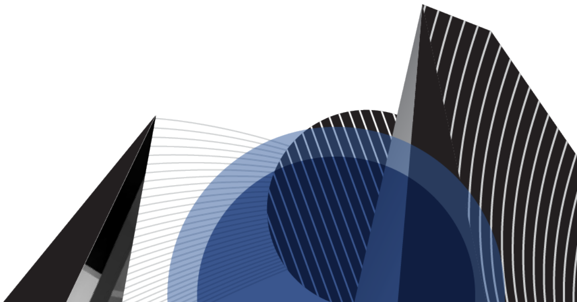
Effective management of cyber security risk requires a forward-looking perspective. There is significant value in gaining such perspective- executive decision-making can radically improve once leaders gain a deep understanding of the "top risks" facing their organization. A level of uncertainty regarding future risk will always exist, but advanced risk management techniques can significantly help reduce such uncertainty and improve decision making. Advanced risk management requires organizations to consider multiple future risk scenarios and focus on questions such as:

- What classes of threats should we prioritize based on the nature of our attack surface?
- What is the frequency of business impact due to such threats?
- What is the magnitude of business impact due to such threats? Including impacts that increase expenses or liabilities and those that decrease revenue or asset values.
- How do our current countermeasure activities align to these classes of threats?
- What are the strategic options for investing in new countermeasures against such threats?
- What is the return on investment for risk-reducing capacity of new countermeasures?

Cloud Platform Consulting

The adoption of cloud platforms is increasing across all industries, though many organizations are concerned about cloud-related threats and challenges. Addressing these concerns requires knowledge of the latest threat actor TTPs. Understanding how cyber attackers target cloud environments allows organizations to answer questions such as:

- What threats are specific to cloud services?
- What tactics are used to compromise cloud infrastructure?
- What is the right strategy for cloud security?
- How does a security team prevent, detect and respond against cloud services?
- What gaps exists in the current security program for cloud adoption?



Selecting a Service Provider

Compliance versus security needs

Cyber security regulations have evolved over the years, creating a baseline of safeguards for enterprises and their customers. For some organizations, maintaining a clean bill of compliance health is their primary objective. Failing to comply with compliance standards can trigger complex audits and steep financial penalties. While compliance provides a modicum of security, limiting security to minimum compliance requirements proves inadequate for organizations in high risk industries, organizations with more complex operations and for those who recognize cyber security as a strategic imperative.

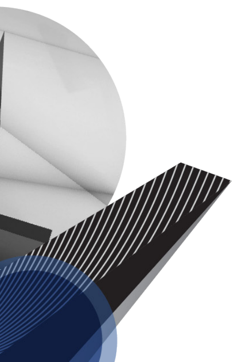
Meeting minimum compliance standards does not guarantee effective security processes. Many organizations who are compliant suffer devastating breaches. They have learned that to suitably protect themselves, compliance is just a starting point. A intelligence-led, resilient cyber security program is vital.

Resilient security focuses on minimizing cyber risks rather than "checking all the boxes" to meet compliance requirements. Proper cyber security proactively implements controls to protect an organization's assets from relentless threat actors. The security landscape is changing daily, unlike regulations which remain fairly static for years. This is why an effective, intelligence-led security program is essential for keeping pace with the current and emerging threat landscape.

To develop a successful security partnership, choose a service provider that can help you identify and focus on your organization's primary needs.

An intelligence-led approach

Threat intelligence provides unique, comprehensive information surrounding active and evolving threats, with insight into adversary TTPs. Selecting a vendor with a frontline view of what industry- and business-specific threat actors are targeting, along with the tools they are likely to use, is critical when maturing a cyber security program.



There are three main sources of intelligence—adversary, victim and machine. Combined, they provide a holistic view of the threat landscape that includes visibility into adversary behaviors and motivations, an understanding of how security measures are bypassed and a view into malicious campaigns as they unfold.

- **Adversary Intelligence:** Understand who the adversaries are, what they're after, and the risks they pose to an organization.
- **Machine Intelligence:** Visibility into attacker telemetry and proliferation, and visibility into emerging campaigns.
- **Victim Intelligence:** Learn what the attackers were after, where an organization's security controls failed, and how those attackers continually evolve their TTPs.

Role of intelligence by service type

Obtaining and understanding attacker methods, motivations and history enables security consultants to deliver thorough, rapid and effective services. Receiving current intelligence about TTPs is critical because threat actors continuously evolve their approach.

- **Incident Response Consulting Services:** Consultants apply frontline intelligence to investigate cyber breaches with speed, scale and efficiency. This knowledge enables organizations to protect critical assets by quickly identifying threat actor TTPs for focused incident scoping, containment and remediation efforts. In addition, it amplifies a security operations team's ability to perform in-depth alert investigations to assess, validate and prioritize potential future incidents.
- **Strategic and Transformational Consulting Services:** Consultants use cyber threat intelligence to properly frame engagements performed through proactive assessments and strategic functional improvements. Intelligence informs the plans, processes, workflows, controls and recommendations implemented for organizations. It bridges the technical and business divide that is typically inherent to security practices. Overall, intelligence is a helpful tool for justifying and procuring security investments.

- **Technical Consulting Services:** Consultants consider intelligence to thoughtfully scope technical engagements. Tactically-focused assessment services use this knowledge to address high-priority relevant threats, and to identify, respond to and help remediate activity within compromised networks. The absence of cyber threat intelligence in tactical engagements has led to historical cases of missed threat actor activity and repeated compromises by similar attackers.
- **Training Consulting Services:** Consultants employ frontline intelligence to develop and deliver security products, functional processes and training that improves security capabilities. Organizations can then assess and enhance their security operations training based on threat intelligence findings.

Questions to ask security providers

Selecting a cyber security consulting provider should be a business decision. The CISO should work closely with business leaders to determine vendor selection criteria and choose vendors that meet the organization's specific cyber risk management needs.

Vendors must be able to offer guidance before, during, and after an incident. Learning from past events and preparing for future incidents is a critical capability that helps reduce the frequency of future breaches and mitigate their impact on business operations, profitability, customer service and reputation.

Consider the security needs framework (Fig. 1) to level set where your organization's security capability focus areas are, and where they'll need to be moving forward. As a security program matures, it should follow a cycle that offers thorough capability assessments, process enhancement and functional transformation.

Selecting the right service provider can be challenging, considering the wide range of options available. To choose a vendor aligned to your organization's security needs, consider the following questions:

- Do you have a dedicated incident response or cyber defense operations team? What is their experience?
- How quickly can you provide remote support?
- What types of cyber threat intelligence resources do you have?
- How do you implement threat intelligence into your security services?
- How do you ensure attacker knowledge is current enough to combat an existing incident and effectively safeguard for the next?
- What type of service levels do you offer when looking at capability needs before, during and after an incident occurs?

You should establish a relationship with a security consulting provider that offers vast global intelligence resources. The vendor selection process can require budget shifts and potentially tough conversations about decision-making, but the right provider will improve your organization's overall protection. By learning about and openly discussing these cyber security needs and challenges, security teams can help create a competitive advantage for the enterprise through solid cyber security practices.

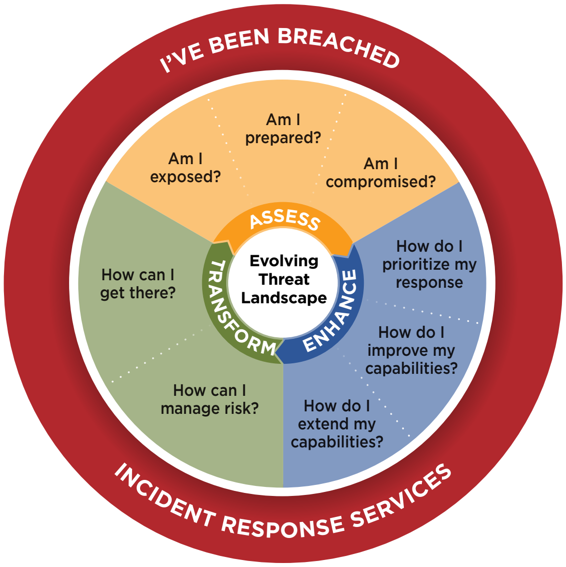

I'VE BEEN BREACHED
Am I prepared?
Am I exposed?
Am I compromised?
ASSESS
Evolving Threat Landscape
TRANSFORM
ENHANCE
How can I get there?
How do I prioritize my response
How do I improve my capabilities?
How can I manage risk?
How do I extend my capabilities?
INCIDENT RESPONSE SERVICES

Figure 1. Security needs framework.

The FireEye Mandiant Difference

FireEye Mandiant combines a practical approach to cyber security rooted in core fundamentals with industry leading cyber threat intelligence to deliver pragmatic, risk-based recommendations.

Since 2004, Mandiant experts have provided rapid incident response services to minimize the impact of compromise, along with security assessment, enhancement and transformation services that mitigate risk and strengthen overall security posture to outmaneuver cyber attackers—before, during and after an incident.

Mandiant professionals leverage combined adversary, machine and victim intelligence sources (Fig. 2) in their work.

- **Adversary Intelligence:** Over 160 intelligence analysts and researchers across 18 countries monitor worldwide threats, providing a view into the earliest stages of threat initiation. Our experts rigorously track and analyze the complex dynamics of global cyber threats to develop adversary context.
- **Machine Intelligence:** Over 16 million virtual analyses per hour from FireEye detection technology deployed around the world provides broad visibility into constant threat activity worldwide.
- **Victim Intelligence:** More than 300 incident responders in 20+ countries at the frontlines of the world's most consequential breaches, responding to known and never-before-seen cyber attacks. We track the actual TTPs used by attackers to infiltrate an organization.

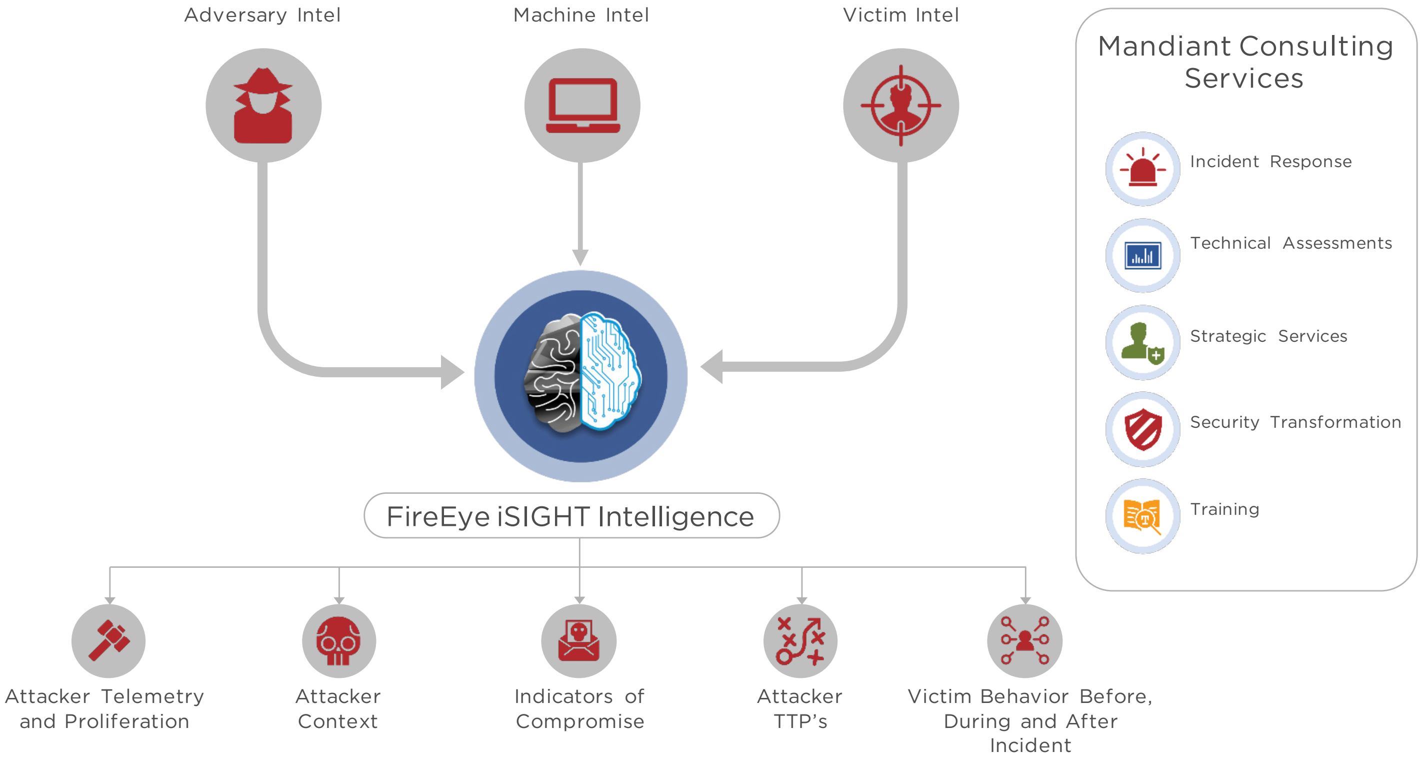


Figure 2. Ecosystem of FireEye intelligence sources.

Threat Intelligence Enriches Consulting Services

Limited budgets, strict regulations, and a shortage of skilled security staff make it increasingly difficult for organizations of all shapes and sizes to obtain a tight hold on cyber attackers amidst today's sophisitcated threat landscape.

Properly managing the innerworkings of security technology and understanding how an attacker may be thinking is a necessary, yet heavy task for any security department. To master these tasks and effectively protect an organization's critical assets, actionable threat intelligence is essential—though most often this cannot be achieved by an internal security team alone.

C-suite and security leaders alike are reacting by identifying cyber security consulting services that lead with threat intelligence to help evaluate and mature their current security posture, manage risk and build scalable sustainable programs that enable their team to continuously outmaneuver cyber attackers.

Organizations are best served by a provider who works on the frontlines of today's ever-evolving cyber landscape to collect timely and relevant adversary, machine and victim intelligence that ultimately elevates the preparation, investigation and remediation efforts of security teams worldwide.

Case Study

A large North American hospitality and entertainment company engaged FireEye Mandiant to help mature their security program and develop and improve cyber defense capabilities to proactively anticipate, detect and respond to targeted threats.

During the engagement, Mandiant consultants identified gaps in the processes used to identify and prioritize suspicious malware within the environment. The consultants found that the organization had difficulty using threat intelligence to triage malware. In one instance, the organization assumed that a particular malware family found within the environment, NETWIRE, was commoditized crimeware used to target organizations indiscriminately across industries. However, in this instance it was being used in targeted campaigns across the hospitality industry. Unaware of this, the organization ignored the potential impact of the malware.

Improvements in malware triage

Mandiant used adversary, victim and machine intelligence sources to uncover the campaign and provide related TTPs to show how the organization was at a heightened risk due to a targeted threat. The organization triaged the malware and prioritized investigation of future instances of this malware within their environment.

Improvements in ability to prevent, detect and respond to future threats: Mandiant also addressed systemic gaps in the customer's cyber defense processes. Our experts helped the organization consider and efficiently use intelligence via a threat profile. They were ultimately able to incorporate threat intelligence use cases into their security processes.

Summary

Without proper threat intelligence, risk assessment and processes required to identify the true nature of current threats, the customer might have responded incorrectly to the threat and been unable to adapt to their changing threat environment over time. Both factors could have resulted in significant business impact.

In this strategic consulting engagement, Mandiant used cyber threat intelligence (CTI) to help the organization better understand their risk, mitigate the associated threat and improve their ability to detect and respond in the future.

To learn more about FireEye, visit: **www.FireEye.com/services**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye, Inc.

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.