MANDIANT®

EBOOK

CONSIDERATIONS FOR EVOLVING TO INTELLIGENCE-LED SECURITY

Introduction

Today's attack landscape is seemingly limitless.

Cyber criminals are activating campaigns in every country around the world, using a multitude of attack techniques. To successfully reduce cyber risk, security teams need to know more about the specific attackers targeting their organization, including who they are, the regions and industries they target, when they were sighted, their motivation and the tactics, techniques and procedures they adopt. This is the promise of cyber threat intelligence (CTI).

When teams know the attackers targeting their organization and how they operate, programs to mitigate risk can be proactively developed, driving investments in tools to effectively protect their business.

This ebook discusses what teams should consider as they evolve their security program to an intelligence-led capability, helps assess the value of a more proactive posture and provides a framework for implementation incorporating:

- The phases of transformation to an intelligence-led approach to security
- How to assess and identify the key components required for transformation
- The basic components of CTI capability
- The advanced components of CTI capability

To successfully reduce cyber risk, security teams need to know more about the specific attackers targeting their organization

The Challenges of Compliance-Based Security

Some organizations rely on compliance-based security to manage their cyber risk. This approach, with its formulaic or one-size-fits-all method, does not take into consideration the many complexities and points of differentiation among organizations and the industries within which they operate. When using compliance-based security, organizations are likely to end up with:

- **Unfocused data-collection strategy:** The organization cannot collect relevant intelligence because they don't know their attackers.
- **No defined mission or mission statement:** Without a purpose, the team cannot be effective.
- **No understanding of business needs:** They cannot identify useful tools and strategies for adequate protection
- **No analytic requirements:** The organization is not aware of what or whom they should be tracking.

As a result, security teams will end up with a reactive security posture, not knowing which threats to prioritize, lacking business focus and making it difficult to quantify the security program and its value.

Value of an Intelligence-Led Security Strategy

Intelligence-led cyber security transforms a reactive security posture into a proactive one, allowing security teams to raise threat awareness and mitigate breach impacts. Decisions are based on deep analysis, corroboration and technical insight. They include expert predictions and the effective management of stakeholder expectations.

Intelligence-led security adds value by:

Refining cyber security strategy

- Identifying the most relevant and impactful threats targeting an organization—not just on a day-to-day basis, but also during periods of change, such as mergers and acquisitions or business expansion.
- Influencing investment by aligning business risk with an organization's security program
- Aligning resources against the most likely threats and actor capabilities

Increasing operational efficiency

- Providing early warnings and enabling automated responses to the threats that matter most
- Supporting the patch management lifecycle and empowering teams to patch vulnerabilities that pose the biggest risk to an organization
- Enabling teams to proactively search for attackers targeting their organization and identifying their intent, techniques and tools to help improve security defenses

Accelerating responsiveness

- Providing the detail and intelligence behind a security incident
- Helping teams to prioritize their response to alerts

These attributes are commonplace in environments that are truly intelligence-led. In organizations where a CTI program has matured, an intelligence-led approach can also help establish a sustainable program, meeting business demands and quantifying the return on security investments.

Phases of Intelligence-Led Security Transformation

Transformation in any business usually requires a phased approach to ensure the changes meet an organization's needs and are implemented methodically. Mandiant experts recommend four phases to transform a business into an intelligence led security operation, including an assessment of the current capabilities, identifying business requirements, implementing systems and operationalizing systems.

Phase 1. Assessment
Gain an understanding of the current threats facing your organization; who the key stakeholders are and how threat intelligence can support those stakeholders over time. Examine CTI gaps and their remedies and identify how CTI could benefit the wider cyber security team.

Phase 2. Design
During the design phase, build out recommendations for a CTI program aligned to both organizational processes and the CTI process lifecycle. Document integration endpoints for the entire cyber defense team and create organization-specific communication workflows.

Phase 3. Enhancement
Develop skills and experience within your CTI team which can be especially useful when they lack a traditional cyber intelligence background. This phase not only strengthens the team's capabilities, but also promotes the consumption, application and benefits of threat intelligence to stakeholders throughout the organization.

Phase 4. Operationalization
Align CTI strategy with processes and procedures. Rolling the program out in stages will make implementation manageable and opportunities for improvements can be recorded after reviewing each stage.

A Framework for Intelligence-Led Security

Introducing a CTI program can be a complex undertaking. Adopting a framework ensures solid foundations are implemented, upon which an organization can introduce the technology and processes to support their needs as they mature. With many years of experience working on the frontlines of incident response, Mandiant experts have developed a trusted and proven framework to guide an organization on their journey.

Building Blocks of a Framework for Intelligence-Led Security

Establishing Foundations

Organizational Threat Profile

- Environmental Business and Operational Knowledge
- Threats, Vulnerabilities and Exposure

Stakeholder Analysis

- Consumer Roles
- CTI Appetite (desired format/ frequency content)
- Consumption Use Cases

Intelligence Requirements

- Criteria Categorization and Prioritization
- Source and Methods
- Intent and Expected Actions

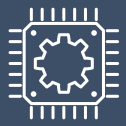
Implementing Practices

Manage CTI Lifecycle

- Collection and Processing
- Analyst Tradecraft/ Expertise
- Analytic Framework
- Production Standards

Technology Integration

- TIP
- CMS
- SIEM Integration
- Big Data
- Supporting Analytic Toolsets



Realizing Capabilities

CTI Operations

- Analytic/Tactical Support to Security Operations
- COI Info Sharing
- Threat Trending and Predictive Analytics
- Proactive Threat Detection
- Repeatable and Effective Threat Communications
- Strategic Decision Support

Maturity

Building Blocks of a Framework for Intelligence-Led Security (cont.)

Establishing Foundations

The building blocks in the first stage should create an enduring cyber intelligence organization that can determine:

- Threats an organization is facing, including threats to be prioritized
- Stakeholders who will need and use threat intelligence within the business
- Intelligence requirements that will best serve the stakeholders

Foundational elements are critical to a successful CTI program. Neglecting foundational blocks can complicate the alignment of intelligence capabilities to business needs when organizations must focus on advance blocks as they mature.

Implementing Practices

This stage focuses on building the processes necessary to support the use of CTI throughout an organization, and includes:

- Training analysts who will be running the CTI capability program
- Determining the data acquisition strategy
- Implementing the right tools and technology.

Realizing Capabilities

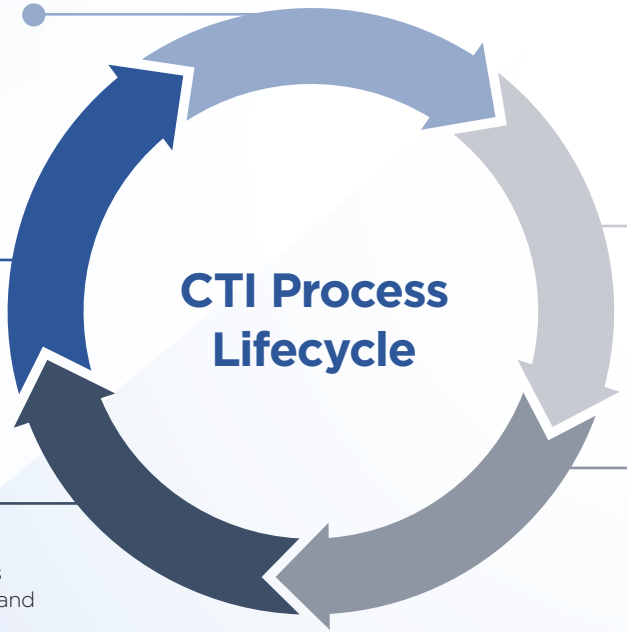
The final stage realizes CTI capability, implementing a day-to-day workflow of processes identified in stage two. This allows a threat intelligence team to shift from a reactive to a proactive threat detection stance.

Neglecting foundational blocks can complicate the alignment of intelligence capabilities to business needs

The Intelligence Lifecycle

When an intelligence-led capability has been operationalized, teams can adopt a CTI process lifecycle to guide them through the continuous flow of planning, data collection, analysis, production and review of both threat intelligence and the means by which it is gathered and applied throughout the business.

Using an organized CTI process ensures structured and consistent practices across the organization. To reap the full business and risk management benefits of this approach, the CTI process lifecycle and key program components should be handled at the executive level.



Planning and Requirements

- Define CTI core directives
- Identify and prioritize intelligence requirements
- Manage execution continuosly

Collections and Processing

- Decipher data aquisition strategy to fulfill requirements
- Normalize, de-duplicate and enrich raw data into consumable forms

Analysis

- Evaluate, analyze and interpret processed information against requirements
- Assess collection gaps

Production

- Produce timely, relevant and actionable intelligence products that align to stakeholder needs and satisfy requirements
- Document deficiencies

Dissemination and Feedback

- Deliver finished intelligence products to stakeholders with defined frequencies and methods
- Acquire and analyze stakeholder feedback

Support Through Intelligence Capability Development (ICD)

Mandiant Threat Intelligence has spent the last decade helping organizations from various industries effectively adopt and integrate CTI into their security operations.

These experiences have helped FireEye build and refine a set of services designed to systematically build best practices for the consumption, analysis and practical application of CTI.

ICD services from Mandiant Threat Intelligence range from engagements with a specific requirement to large-scale intelligence program implementations that help security teams:

- Find the baseline for existing intelligence capabilities and planning improvements
- Determine the cyber risk your organization faces, the intelligence you need to fight that risk and who will use it
- Map out your strategic, operational and tactical use cases for the application of intelligence
- Provide workshops to improve CTI capabilities and use CTI more effectively in day-to-day activities

Whether combined or delivered separately, ICD services support the development and maintenance of a comprehensive threat intelligence program.

> A set of services designed to systematically build best practices for the consumption, analysis and practical application of CTI

Access Unparalleled CTI with Mandiant Advantage

Mandiant Advantage provides organizations of all sizes with to-the-minute, relevant and easy to consume threat insights, accelerating decision making to reduce risk and improve an organization's security posture. Users access threat intelligence that goes beyond the capabilities of current open source SaaS platforms with insight derived from:

Breach Intelligence
Over the last 15+ years, Mandiant has built a reputation as the industry's premier Incident Responder, attending 800+ Incident Response engagements annually.

Operational Intelligence
The Mandiant Managed Defense team performs detection and response services for over 300 customers from four international Cyber Threat Operations Centers, ingesting 99m+ events and validating 21m+ alerts.

Adversary Intelligence
Mandiant Threat Intelligence deploy 200+ intelligence analysts and researchers located in 23 countries who collect up to 1 million malware samples per day from more than 70 different sources.

Machine Intelligence
Mandiant experts take advantage of FireEye technologies, which have approximately four million virtual guest images deployed globally in 102 countries, generating tens of millions of sandbox detonations per hour, confirming 50,000 - 70,000 malicious events per hour.

Conclusion

Intelligence-led cyber security is transformational for an organization. A proactive security team operating on to-the-minute intelligence is better equipped to protect their organization against threats because they are acutely aware of the specific threats they face.

Organizations need a proven framework for organizations to follow and develop a successful, sustainable CTI program. Ultimately, their teams will use various data feeds, briefings, investigations and prioritization recommendations to make strategic security and business decisions on a daily basis. But they first need to establish a strong foundation that ensures any investment in new intelligence capabilities is aligned with their organizational needs. Over time, a commitment to continuous security evolution combined with a conscious effort to incorporate CTI into business strategy will lead to a mature, intelligence-led cyber security practice.

To learn more about how to improve your security posture visit: **www.fireeye.com/intel.**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6500/877.FIREEYE (347.3393)
info@FireEye.com

About Mandiant Solutions
Mandiant Solutions brings together the world's leading threat intelligence and frontline expertise with continuous security validation to arm organizations with the tools needed to increase security effectiveness and reduce business risk.

MANDIANT®