MANDIANT

EBOOK

CONSIDERATIONS FOR EVOLVING INTELLIGENCE-LED SECURITY

Today's Threat Landscape Is Seemingly Limitless and Challenging

Foreign adversaries, cyber criminals and other malicious actors are conducting nonstop campaigns against organizations across every industry around the world. Whether they're motivated by multi-million-dollar ransom payoffs, disrupting critical infrastructure, exfiltrating sensitive assets or pure espionage, today's sophisticated adversary wields an array of attack tactics, techniques and procedures (TTPs) to penetrate organizational defenses.

To meet this growing challenge and minimize cyber risk, security leaders and technical teams need to know more about the specific adversaries they face, including: who they are, which regions, industries and crown jewels they are after, when and how they were detected, their motivation and the TTPs they adopt.

When teams understand the attackers targeting their organization and how they operate, programs that mitigate risk can be proactively developed and deployed to drive investments in people, processes and tools for effective business protection.

As teams evolve their security program to be led by threat intelligence and expert insights, and develop a more proactive security posture, they should consider a framework that includes:

- Assessment and identification of the transformative components needed to move to an intelligence-led approach
- A systematic approach for transformation
- Basic and advanced components of cyber threat intelligence (CTI)

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

Value of an Intelligence-Led Security Strategy

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

Value is demonstrated by:

Refined cyber security strategy

- Identifying the most relevant and impactful threats targeting your 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 your organization's security program
- Aligning resources against the most likely threats and actor capabilities

Increased 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 hunt for attackers targeting the organization and identifying their intent, techniques, and tools to improve security defenses

Accelerated responsiveness

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

In organizations with a mature CTI program, an intelligence-led approach can also help develop sustainability practices by meeting business demands and quantifying the return on security investments.

Common Roadblocks on the Intelligence-Led Journey

Becoming an intelligence-led organization affects the intelligence lifecycle and significantly impacts not just the enterprise but also the people and processes that are critical to successful business and security operations.

The enterprise

Enterprises can use CTI to counter and defeat cyber adversaries: 85% of organizations already consume CTI and the remaining 15% plan to embrace it,[1] while global security decision-makers now subscribe to an average of 7.5 commercial threat intelligence services.[2]

However, in many observed cases the intelligence program requirements are undefined or unmanaged, with only 43% of enterprises having documented their CTI requirements.[3] Neglecting proper planning and documentation diminishes an organization's ability to craft an end-state strategy for intelligence and justify return on investment. Additionally, business-critical assets are often improperly mapped to threats, leading to incorrect investment guidance.

Further issues involve overlapping intelligence collection and processing services and heavy reliance on low-fidelity and outdated sources such as threat feeds. These are not only inefficient and wasteful—they also produce reports that contain after-the-fact information that magnifies poor threat detection and security risks.

Disjointed dissemination of intelligence across the organization and the lack of feedback to the fast-paced security environment are also often overlooked. For example, 66.5% of organizations disseminate CTI through email, presentations and spreadsheets.[4] This can tremendously degrade the interest of intelligence consumers and blur their perspective on the value intelligence offers the organization, ultimately resulting in unmet expectations.

1. SANS (January 18, 2021). 2021 SANS Cyber Threat Intelligence (CTI) Survey.
2. Forrester (March 23, 20210). The Forrester Wave: External Threat Intelligence Services, Q1 2021.
3. SANS (January 18, 2021). 2021 SANS Cyber Threat Intelligence (CTI) Survey.
4. Ibid.

The Human Aspect of Transitioning to Intelligence-Led Security

No matter how good their intelligence, organizations still need proper staffing, expertise and resources to implement a defensive strategy.

Behind the stack, analysts collect and process overwhelming volumes of unreliable information at unprecedented rates. CISOs and security practitioners are familiar with the 24/7 struggle to make sense of all the alerts. SOCs can only look at a small fraction of their alerts.[5] There's simply too much noise in cyberspace for even the savviest security practitioners to decipher on their own.

5. Mandiant (May 2020). Mandiant Security Effectiveness Report 2020.

A Framework for Intelligence-Led Security

Integrating a CTI program into existing systems and processes can be a complex undertaking, but adopting a robust framework delivers many technical and strategic wins for both your enterprise and your personnel.

Hundreds of organizations over the years have directly experienced the compounding benefits of implementing a CTI framework into their cyber security strategy. Underpinned by a process lifecycle and integrated into the technology stack, this framework helps organizations show repeatable and measurable results for fine-tuning security investments and achieving sustainable security success.

While properly implemented and actionable CTI empowers organizations to stack the odds against today's increasingly sophisticated adversaries, organizations must fully invest in the process to succeed. This requires technical skills, effective planning, management, analytic tradecraft, communication and collaboration across the entire organization.

Based on intelligence community best practices and over 15 years of helping customers consume and apply intelligence across government and commercial settings, Mandiant has identified the essential elements and commonalities that set the gold standard for an actionable intelligence framework. The framework not only guides your organization on its journey to an intelligence-led security posture that evolves with the threat landscape, but also evolves with the maturity of your organization's security staff, enterprise technology and processes.

The Building Blocks of a Framework for Intelligence-Led Security

GROUP 1

Establishing Foundations

A sustainable intelligence capability is dependent on a defined cyber threat profile, comprehensive intelligence, consumer analysis and established intelligence requirements.

Cyber threat profile

Threats an organization is facing, including threats to be prioritized.

- Environmental business and operational knowledge
- Threats, vulnerabilities and exposure

Stakeholder analysis

Personnel who need and use threat intelligence within the business.

- Consumer roles
- CTI appetite (desired format and frequency of content)
- Consumption use cases

Intelligence requirements

Characteristics that translate to greater stakeholder value

- Criteria categorization and prioritization
- Source and methods
- Intent and expected actions

GROUP 2

Implementing Practices

Buildout of the processes needed to support CTI use throughout an organization is an ongoing effort and critical to a sustainable intelligence-led cyber security strategy.

CTI lifecycle management

- **Data acquisition strategy.** Collecting and processing data can overwhelm SOC analysts and other security professionals, so a solid strategy can minimize future issues.
- **Analytic framework.** Analysts need this roadmap to make sense of data and safely steer the organization to success.
- **Analyst tradecraft and expertise.** The heart of any CTI program is the people behind the data. Investments in analyst training can put you well on your way to a successful intelligence-led security program.

Technology and integration

The use of application programming interfaces (APIs) or other methods to implement and integrate the right CTI with security technology can help analysts focus on threats that are relevant to the organization. Intelligence integration opportunities include:

- Threat intelligence platform
- Security information event management (SIEM)

GROUP 3

Realizing Capabilities

Implementation of best practices and processes empowers threat intelligence teams to fully realize CTI capabilities and move from a reactive to a proactive threat detection stance. Intelligence-led capabilities drive several courses of action across the enterprise, including:

- Analytic/tactical support to security operations
- Community of interest (COI) information sharing
- Threat trending and predictive analytics
- Proactive threat detection
- Repeatable and effective threat communications
- Strategic decision support

Prioritizing and strategically building an intelligence framework helps align intelligence capabilities and business needs.

Phases of Intelligence-Led Security Transformation

Business transformation usually requires a phased approach to ensure organizational alignment and methodical implementation. Mandiant experts recommend four phases to transition to an intelligence-led security operation: an assessment of the current capabilities, identification of business requirements, implementation of systems and operationalization of systems.

Phase 1. Assessment

Gain an understanding of the current threats facing your organization, its important intelligence consumers and ways that threat intelligence can support those consumers over time. Examine capability gaps across people, processes and tools, while providing robust recommendations along with a strategic program improvement roadmap.

- How intelligence currently supports the organization
- What capabilities the organization should have to meet its CTI goals
- How threats (internal and external) are mapped to the organization's critical assets
- How the strategic roadmap guides investment priorities across people, process and technology

Phase 2. Design

Analyze Phase 1 results to align organizational directives with the Mandiant CTI framework. Document intelligence integration points across cyber defense teams and create organization-specific communication workflows. Quantify resourcing needs including skill sets, roles and responsibilities linked to your customized service catalog.

- CTI use cases, such as business decision support, hunt missions and attack surface
- CTI products and services such as threat alert, threat advisory and briefings to meet identified use cases and the needs of specific stakeholder roles such as strategic (CISO), operational (incident responders) and tactical (SOC personnel)
- CTI standard operating procedures (SOPs) outlining the steps analysts will perform

Phase 3. Enhancement

Align CTI strategy with processes, procedures and threat landscape. Rolling the program out in stages will make implementation manageable. Opportunities for improvement can be recorded after reviewing each stage.

- The effective implementation of the Intelligence Lifecycle
- An identification of the inherent cyber risk present in the organization

Phase 4. Operationalization

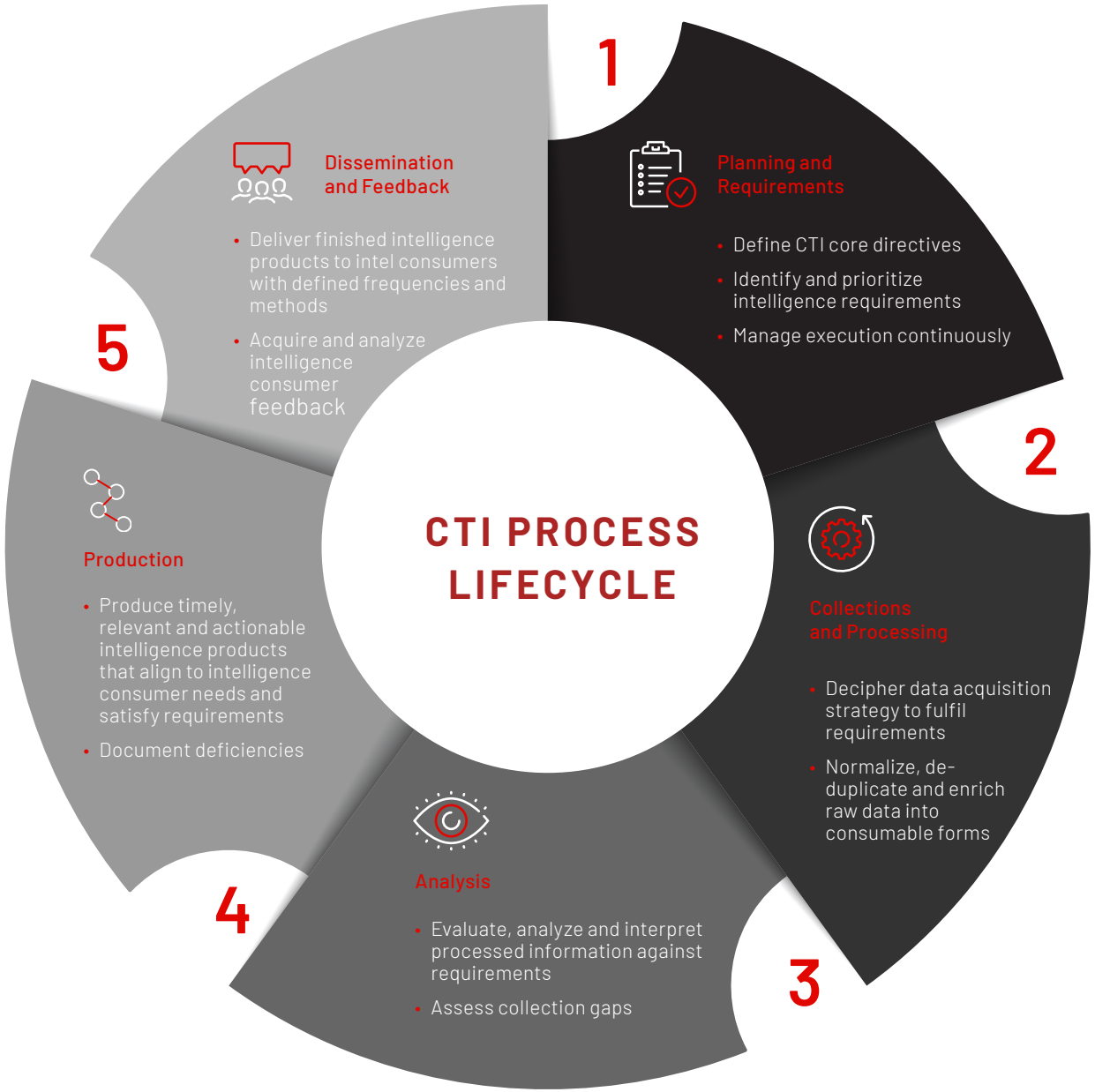
Develop skills and experience within a CTI team, especially useful for teams that lack a traditional cyber intelligence background. This phase not only strengthens the team's capabilities, but also promotes process refinement by amplifying intelligence consumption and application to intelligence consumers throughout the organization.

- Analyst skillsets that follow intelligence best practices
- Analyst knowledge that considers business and security priorities
- Optimally tuned process and procedures

End-State: Sustainable Intelligence Lifecycle

After an intelligence-led capability has been operationalized, your 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. It also creates opportunities to measure the success of the CTI capability. To reap the full business and risk management benefits of this approach, the CTI process lifecycle and essential program components should be supported at the executive level.



Business Benefit: Lower Cyber Risk

Risk that arises specifically from a cyber security related incident caused by cyber threats is categorized as cyber risk. It is a critical component to any enterprise risk management capability.

The ultimate goal of a CTI program is to help drive risk reduction activities across an enterprise. CTI is uniquely positioned to inform risk teams with the detailed threat information needed to thoroughly assess cyber risks within an organization. It can also outline solutions that can bring risk levels back in line with organizational risk tolerance levels. CTI gives risk practitioners the information they need to truly prioritize and respond to their most concerning cyber risks.

An effective CTI program should continuously and consistently provide quality inputs to enterprise risk models either through qualitative or quantitative measures regardless of the risk framework used. Framework examples include FAIR and NIST.

Conclusion

Intelligence-led cyber security can be 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 to follow a proven framework to develop a successful, sustainable CTI program. Their teams should 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 can lead to a mature, intelligence-led cyber security practice—which ultimately results in greater defensibility and minimizes risk.

Learn more at **www.mandiant.com/intelligence**

Mandiant
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant
Since 2004, Mandiant has been a trusted security leader to organizations that can't afford to fail. Today Mandiant delivers decades of frontline insights at scale through easy-to-deploy and consume SaaS solutions for provable and transformative cyber defense.

MANDIANT