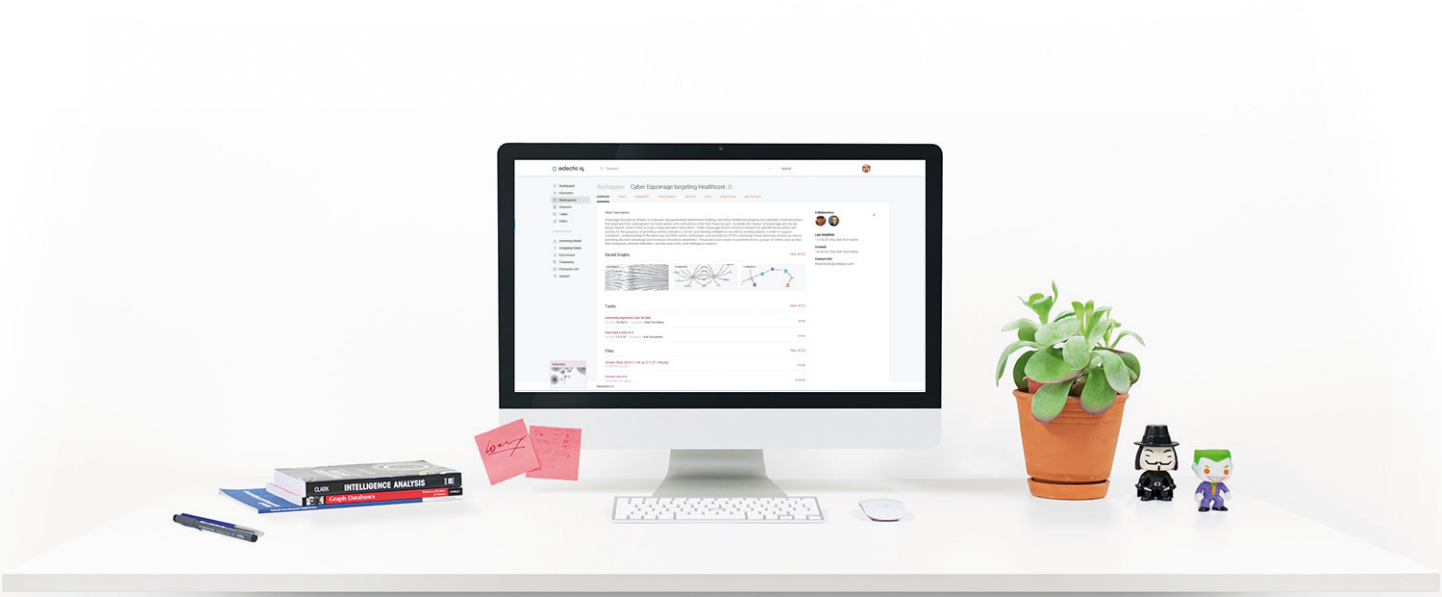
WHITE PAPER

Applying the Threat Intelligence Maturity Model to your organization

EclecticIQ's Threat Intelligence Maturity Model gives organizations a way to assess their capabilities in eight distinct areas essential to Cyber Threat Intelligence, enabling organizations to reduce uncertainty and risk throughout their operations



Contents

Abstract 3

What is Threat Intelligence? 4

A Model for Assessing Current and Desired Maturity for Threat Intelligence 6

Maturity Model 8

Using the Maturity Model 10

Best Practices in Building an Enterprise Threat Intelligence Capability 11

About EclecticIQ 16

Abstract

Enterprises and governments have become aware of cyber threats and have prioritized the business need for a threat intelligence practice capable of aligning action to the threat reality. With the growing diversity of threat intelligence products offered in the market, the emerging challenge is deciding where to start and how to guide investment decisions in people, process and technology.

Forrester Research reports that 77% of large enterprises consider establishing or improving their cyber threat intelligence (CTI) capabilities a high or critical priority.[1]

This paper provides a framework to assess the maturity of threat intelligence efforts and guide future investments.

Effective threat intelligence has to align the information needs of stakeholders with the reality of the threat landscape, while remaining within ever-present business constraints on resources and budgets. In this environment, the critical elements of success are to build for clear internal needs, to align with key stakeholders, and to build people, process and technology that is fit for purpose.

1) Forrester Research, "The State of the Cyberthreat Intelligence Market," by Rick Holland, June 23, 2015

What is Threat Intelligence?

At its core, intelligence is about reducing uncertainty. When uncertainty involves conflict around business objectives, intelligence serves to decrease business risks. Cyber intelligence reduces uncertainty in dealing with threats such as electronic crime, hacktivism, terrorism and espionage.

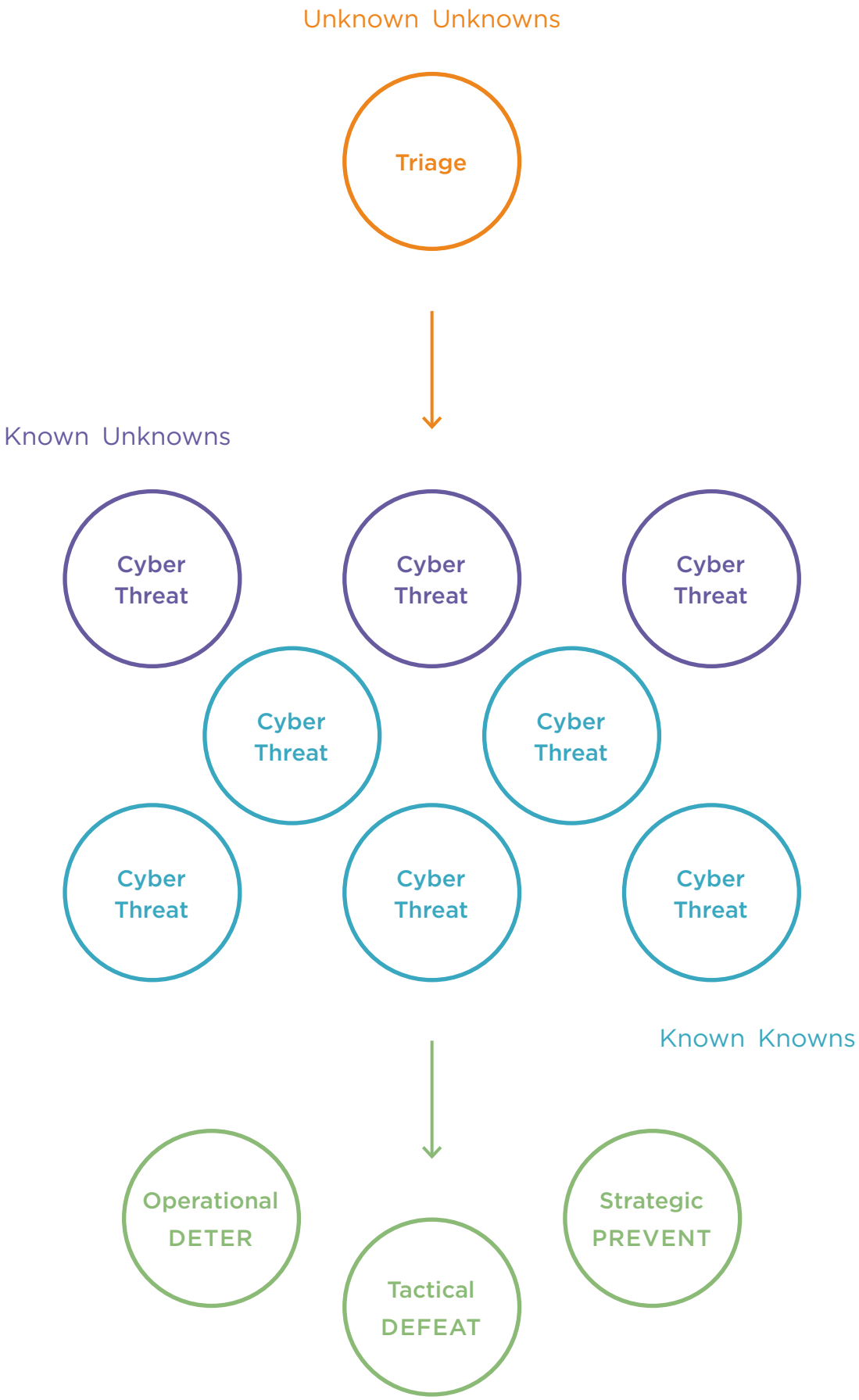
Reducing this uncertainty, and therefore managing these cyber risks, requires information that cyber adversaries prefer to conceal. Intelligence analysts need to uncover this concealed information using direct and indirect means of collecting and analyzing available information. Intelligence analysts proceed by establishing facts and then developing precise, reliable, and valid inferences for use in decision making. The resulting conclusions and predictions are extremely useful in operational planning for security operations, incident response, vulnerability management, risk management and board-level decision making.

> *"Intelligence is regularly defined as information that can be acted upon to change outcomes."*
>
> *— CPNI.gov.uk*

Cyber threat intelligence follows the methods of traditional intelligence to focus on operational, tactical and strategic responses to cyber threats.

A common method to describe the process of threat intelligence is the management of "knowns" and "unknowns." The most dangerous are the "unknown unknown" threats that we do not know about, nor understand. Accordingly, the first step of intelligence is to discover the existence of threats – the "known unknowns" – and subsequently work to understand them better as "known knowns", ensuring appropriate action on them. This continuous process of cyber threat identification, understanding, and action is a good high-level description of the process of threat intelligence.

On a practical level, intelligence informs an organization on how best to prevent, defer, or if necessary, defeat a full range of changing adversarial capabilities and activities that constitute cyber threats. An intelligence organization has to constantly evaluate the changing threat landscape in order to inform the organization on how to align against the threat in the most effective way given the available resources.


Unknown Unknowns
Triage
Known Unknowns
Cyber Threat
Cyber Threat
Cyber Threat
Cyber Threat
Cyber Threat
Cyber Threat
Cyber Threat
Cyber Threat
Known Knowns
Operational DETER
Tactical DEFEAT
Strategic PREVENT

A Model for Assessing Current and Desired Maturity for Threat Intelligence

EclecticIQ's maturity model is inspired by the great work of Robert M. Clark (author of "Intelligence Analysis: A Target-Centric Approach"), CPNI/CERT-UK's publications on threat intelligence, and iSIGHT Partners Threat Intelligence Maturity Model.

EclecticIQ's maturity model for organizational intelligence establishes a five-point assessment scale for measuring maturity for eight separate capabilities.

Overall, the model measures threat intelligence maturity in three broad areas:

1 Alignment with business and threat reality

Measures how well investments in threat intelligence strike a balance between business needs, resource constraints and the threat landscape. Relevant capabilities in the maturity model:

- **Stakeholder Management**
- **Requirements Management**
- **Awareness**

2 Ability to understand

Measures how well analytic capabilities allow threat intelligence teams to understand cyber threats according to the information needs of internal stakeholders. Key capabilities include qualifying technical indicators and strategically tracking key cyber threats facing the organization and similar entities. Relevant capabilities in the maturity model:

- **Source Management**
- **Analysis and Production**
- **Sharing**

3 Ability to control / action what is understood

Measures the ability of an organization to understand and control threats. Ensures action by security stakeholders responsible for aligning the organization's ability to defeat, deter and prevent cyber threats. Key capabilities include relevant technical indicators, instrumentation of detection and prevention systems, and involvement of business stakeholders on how the changing threat landscape drives appropriate investment and business decisions. Relevant capabilities in the maturity model:

- **Dissemination**
- **Integration**

Maturity Model

Capability	Stage 1	Stage 2
Stakeholder Management	Little to no awareness of what threat intelligence is and what business capability is responsible for it	Threat intelligence sometimes makes it to stakeholders, rarely considered and acted upon
Requirements Management	No requirements, or requirements not based on stakeholder input	General understanding of stakeholder needs through informal or irregular touch-points
Awareness	No awareness of threats	Some awareness of commonly (and publicly) discussed threats
Source Management/Collection • open-sources • commercials • communities	• None or ad-hoc	• Irregular decision making on source acquisition • Mostly open- or sources of unknown reputation
Analysis and Production	No analysis, intelligence from sources is dissemination or integrated directly	**Qualification** Intelligence received is enriched and qualified using automatic or manual methods
Dissemination	intelligence is disseminated directly from sources	Disseminated intelligence has ample context and confidence statements to understand relevance to receiving stakeholder
Integration	Intelligence from sources is not integrated into security controls and workflow systems	Intelligence indicators are irregularly integrated into security controls and workflow controls
Sharing	No sharing	Sharing with individuals at similar organizations

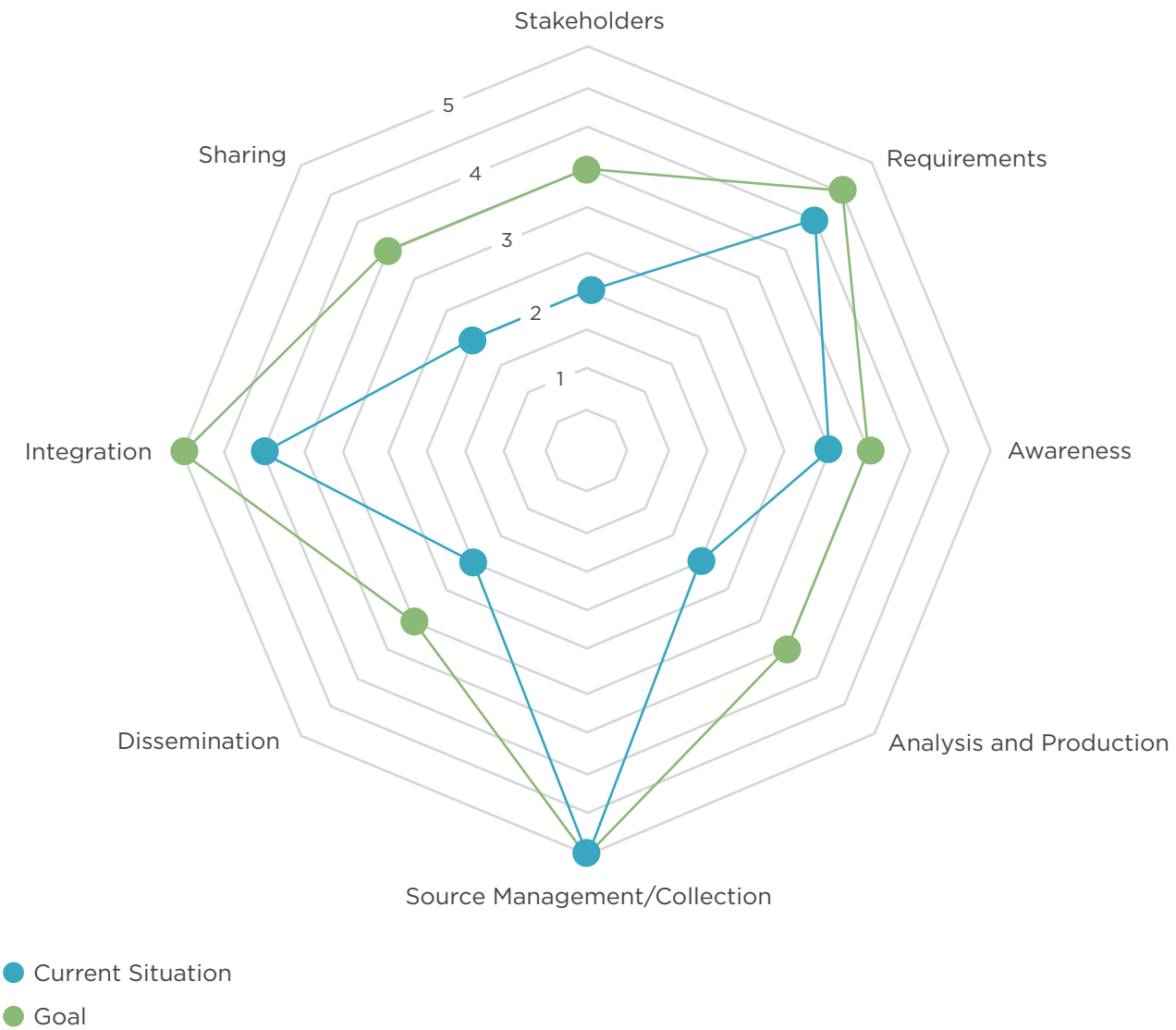
Stage 3	Stage 4	Stage 5
Threat intelligence regularly sent to stakeholders and consistently considered and acted upon	Threat intelligence consumed as a standard input and regularly used in decision making around cyber related issues	Threat intelligence consumed as a standard input, with advice actively sought on major decisions
Regular and established touch-points to understand stakeholder needs	Regular and established touch-points to understand stakeholder needs, with ad-hoc feedback on received intelligence	Regular and established touch-points to understand stakeholder needs, with regular, ongoing feedback on received intelligence
Some awareness of threats, including trends in threat actor capabilities and motivations	Deeper insight into trends of common threats, and good understanding of actor capabilities, motivations and persistence	Awareness of most relevant threats, including un-common and targeted threats, including actor capabilities, motivations and persistence
• Regular decision making on source acquisition and re-alignment • Wider range of mostly reputable sources	• Established procures to acquire, evaluate and re-alignment sources • Many reputable, well-known sources with regular collection of unique analysis capabilities	• Established procures to acquire, evaluate and re-alignment sources • Large set of reputable sources, including well-known and niche sources, offering consistent supply of unique collection or analysis capabilities
IOC Management Technical indicators and observable components are nurtured with quality control	**Case Management** Established threshold criteria dictates when intelligence warrants ad-hoc, case-based and collaborative research in order to improve understanding of specific threats	**Threat Management** Threats are proactively and strategically managed from a central register; Continuous research is proactively performed to understand known threats
Disseminated intelligence is targeted for the specific stakeholder	Intelligence is created collaboratively with stakeholders in order to validate and test key hypotheses; Conclusions of intelligence are sent directly to the relevant stakeholders	Stakeholders have full control over the timing, delivery method and subject matter of intelligence reports, and receive targeted intelligence on relevant topics when necessary
Intelligence indicators are regularly integrated into security controls and workflow controls	Intelligence indicators are integrated into security controls and workflow controls with information about context, priority and specific course of action	Intelligence indicators are integrated into security controls and workflow controls with information about context, priority, specific course of action, as well as clear and easy-to-understand drill-down into analytics and intelligence of surrounding context
Sharing through semi-regular meetings with individuals and semi-sensitive groups	Ad-hoc sharing via institutional relationships or within sensitive, trusted groups	Regular sharing via institutional relationships or within sensitive, trusted groups

Using the Maturity Model

Before creating a plan to build or improve threat intelligence for your organization, it is important to establish first, where you are today; and second, and where you want to be within the next 12 to 18 months as a reasonable starting point. Stakeholders need to agree on the level of maturity you want to achieve in your intelligence capabilities.

Based on our experience working with threat intelligence teams globally, we recommend aiming to raise maturity each year by not more than two points on the five-point scale for each capability. In order to ensure enough time to operate at an improved level, allow time to measure results, and then to re-align and plan accordingly.

Create a diagram that visualizes the current situation with respect to the desired state.



Best Practices in Building an Enterprise Threat Intelligence Capability

1 Build for stakeholders

Creating business value from threat intelligence relies on the ability to understand the information needs and requirements of key stakeholders in the organization. These stakeholders are ultimately responsible for the deterrence, defeat and prevention of cyber threats. Start by understanding who the key stakeholders are, how and at what cadence they prefer to consume intelligence, and what key intelligence requirements they need answered.

Stakeholders and their requirements typically include:

- **Executives and decision makers** need to understand how their organizations are exposed to key threats
- **IT Architects and other IT decision makers** need to stay up-to-date with their understanding of key threats to common IT security systems and concepts as to ensure alignment with the configuration of IT infrastructure with the reality of cyber threat in mind.
- **Security Operations Centers (SOCs)** require technical structured indicators and warning signals associated with key threats, usually as soon as they become available and in machine-readable structured formats.
- **Incident Response and Operations (IR) teams** often require ad-hoc, bespoke intelligence related to tools, modus operandi, associated campaigns, actor intent and attribution and other contexts of discovered technical indicators of compromise during forensics, both during and after notable IT security incidents.
- **Security controls administrators** require information about adversary tactics, tools and techniques in order to deter threats by adapting the configuration of controls.
- **Risk Management** requires a thorough understanding of the business risks associated with threats facing the organization, in order to assess the likelihood of uncertainty around key business objectives.
- **Business stakeholders** require regular updates on key threats and their potential impacts on business operations with their areas of responsibility.
- **Vulnerability Management teams** require written intelligence describing emerging high-impact IT system vulnerabilities and known exploitation vectors.
- **Anti-fraud teams** use information about cyber threats to detect and respond to potentially fraudulent activities on the organization's customer-facing platforms, such as e-banking or retail.

2 Drive urgency of organizational awareness of cyber threats

The potential application of threat intelligence spans across a wide range of operational, tactical and strategic issues that require both immediate action and long-term planning. Stakeholders have to be aware of the scope of threat intelligence, and how it can help them to control their exposures to the changing threat landscape. Successfully implementing a threat management capability requires buy-in by decision makers, and their appetite to investment will be proportional to how well internal stakeholders understand the value of threat intelligence.

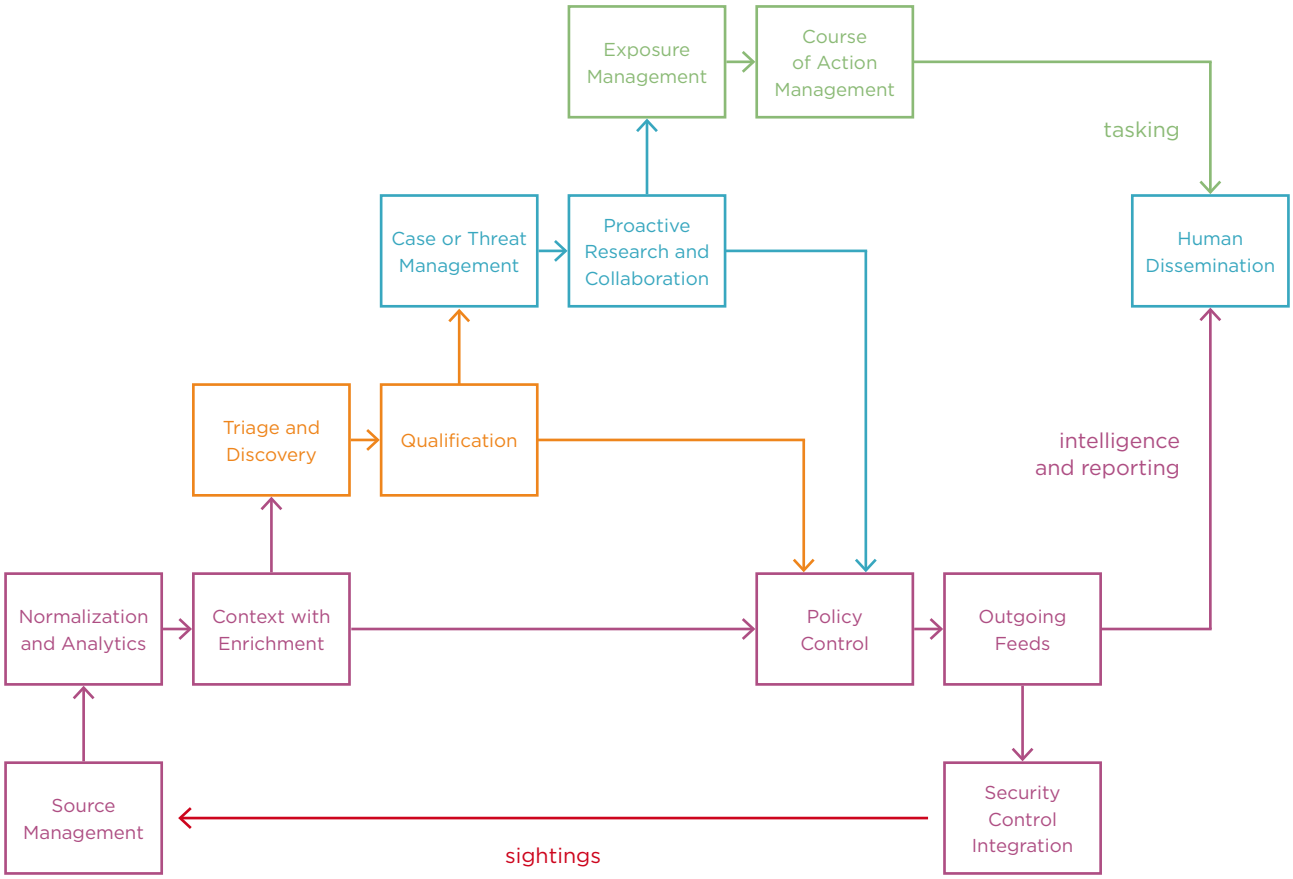
3 Achieve organizational buy-in

All stakeholders should be comfortable with the plan for threat intelligence, including a shared vision, timing for a phased roll-out, known constraints and measurable results expected. The key to any successful project is to cultivate an understanding of how much you want to accomplish, at what pace, in what steps and with what business constraints, whether in timing, resources or other factors. Make promises to the organization you can keep. Big or small.

4 Establish a Threat Management practice separately from IT Security

A Threat Management practice implements a threat intelligence process and to successfully plan, implement and operate such a practice requires specific intelligence competencies.

Threat intelligence is adjacent and related to IT Security, but it is a distinct competency with clear lines of demarcation. A separate Threat Management practice ensures the availability of the relevant competencies needed to architect, plan and implement threat intelligence processes and procedures, including the acquisition and analysis of threat intelligence feeds. The IT Security and Threat Management teams should work together as a well-balanced, cross-functional team during the roll-out of any changes to existing of new processes and procedures. Otherwise, they should have separated responsibilities.



5 Strengthen capabilities in Analysis and Production

In threat intelligence, analysis and production represent the key enablers in understanding cyber threat.

Threat intelligence best-practices for analysis and production can be established at several levels of maturity. An organization should strive to advance capabilities through each successive level.

- **Qualification** is the reactive process of ensuring that automated systems and threat analysts qualify intelligence received from sources to understand relevancy for the organization, determine confidence and proximity and define action.
- **IOC Management** further ensures that the related technical warning signals that indicate potential cyber threats in play against the organization, often called Indicators of Compromise (IOCs), Indicators of Attack (IOAs) or Observables, are of sufficient quality and fit for the detection, prevention and response capabilities of the organization.
- **Case Management** applies threshold criteria or relevancy criteria to intelligence received in order to uncover potentially valuable data points warranting further research and collaboration. This "cherry-picking" helps analysts to understand issues more deeply, potentially generating valuable and unique collection analysis. Furthermore, automated case management improves the ability of analysts to assess threats over a longer time horizon. Individual cases usually span over short or mid-term timeframes, which means that incoming intelligence is often not representative of broader trends or common threats. Case Management gives analysts a more comprehensive perspective by incorporating historical data into present analysis.
- **Threat Management** builds upon case management with proactive tracking and management of commonly-occurring categories of threats, campaigns, actors and other analytic topics and constructs. Using the extended dataset, an organization can constantly evaluate incoming intelligence to discover relevant "known unknowns," and then, through proactive research, turn them into "known knowns." Threat management provides a holistic view of cyber threats and ranks among the highest levels of maturity and analytic complexity that a threat intelligence capability can create.
- **Exposure Management** is an emerging best practice to measure the extent to which an organization has successfully controlled the cyber threats that it presently understands. The exposure management process measures the gap between known information and an organization's ability to turn that information into action. For example, an organization may receive various technical indicators that stakeholders are unable to act upon. Detection and prevention systems need to be compatible with the indicators managed by the threat intelligence team, and vice-versa. Exposure Management uncovers and mitigates these potential weaknesses.

6 Bootstrap with threat intelligence platform technology

Threat Intelligence Platform (TIP) technologies have emerged to support common challenges with implementing or improving CTI capabilities. TIP provides an easy way of bootstrapping core workflows and processes as part of a successful threat management practice.

When selecting a TIP for your organization, ensure that workflow functionality is available. By doing so, you can ensure that your TIP enables the centralization and consolidation of threat intelligence and the subsequent analysis, production, dissemination and integration of intelligence data into security controls, orchestration and other key processes.

7 Integrate technical indicators into security controls

Organizations commonly use technical indicators associated with intelligence to improve detection, prevention and response capabilities of security controls. This approach improves response times for threat detection and remediation.

Security controls that incorporate intelligence include (listed in order from most-common to least-common capabilities):

- **Security Information Event Management (SIEM) systems** that hold historical and current log information from IT infrastructure and network events. Examples: Splunk, HP ArcSIGHT, IBM QRadar, Logrythm
- **Big data clusters** such as Hadoop, Elastic or Cassandra that hold similar information as SIEM systems, usually built in-house to deal with the new scope and size of this data
- **Intrusion or End-Point Detection and Prevention systems** that evaluate the reality of network or host activity against known threat indicators
- **Security Automation and Orchestration** tooling that automate playbooks for detection and/or incident operations

About EclecticIQ

EclecticIQ is an applied cyber intelligence technology provider, enabling enterprise security programs and governments to bootstrap a threat intelligence practice. Empowering analysts to take back control of their threat reality and mitigate exposure accordingly.

EclecticIQ's mission is to restore balance in the fight against cyber adversaries. Its flagship product EclecticIQ Threat Intelligence Platform enables operationalization of security information exchange, empowers collaborative analyst workflow and ensures timely integration of cyber threat intelligence detection, prevention and response capabilities.

eclectic iq

EclecticIQ is a privately held company headquartered in Amsterdam, the Netherlands, and holds an office in London.

Awarded the 2015 EU IPACSO Cyber Security Award and partner of the NATO NCI Agency Security Incubator.

More information about EclecticIQ can be found at www.eclecticiq.com

For sales enquiries or a product demo, contact us at sales@eclecticiq.com or call +31 (0)20 737 1063.

Follow us on Twitter: @eclecticiq