LOOKINGGLASS

THREAT INTELLIGENCE PLATFORM

FROM LIMITLESS INFORMATION TO ACTIONABLE CYBER THREAT INTELLIGENCE

CONTENT

INTRODUCTION: LOST IN DIGITAL BABEL

In Jorge Luis Borges's short story, "The Library of Babel," a narrator describes the harrowing experience of living his entire life inside an unusual library. It's comprised of an unknown number of labyrinthine hallways, stairways, and hexagonal galleries containing books. The structure of galleries and organization of books are unknown. The library seems to be interminable, and the narrator describes its physical existence as, "a sphere whose consummate center is any hexagon, and whose circumference is inaccessible." After decades of exploring the library, the narrator,

"deduces that the Library is total and [contains] …a version of each book in all languages, the interpolations of every book in all books."

On one hand, the narrator recognizes the library as a great resource, containing the sum of all of mankind's knowledge in written format. On the other, the inability to efficiently find and use specific information at any given time hinders its usefulness. The library's inhabitants have appointed "official searchers," and the narrator "ha[s] observed them carrying out their functions: they are always exhausted. …From time to time they will pick up the nearest book and leaf through its pages, in search of infamous words. Obviously, no one expects to discover anything." One reason the library's inhabitants expect fruitless searches is, "for one reasonable line or one straightforward note there are leagues of insensate cacophony, of verbal farragoes and incoherencies."

Borges published the story in the first half of the 20th Century, before the modern Internet era. Yet for today's security analysts, aspects of Borges's description may sound familiar, such as searching for specific answers amid a labyrinth of information with no cohesive structure or predictable organization. Indeed, Borges's Library of Babel, like the Internet, seems to be "limitless and periodic."

Security analysts today share similar challenges with the library's inhabitants. There is plentiful threat information on the World Wide Web. But how can analysts efficiently find what they need to know when they need to know it? Most organizations do not have the ability to generate the volume of useful data required to derive timely and actionable threat intelligence.

Once analysts find sources, how can they effectively extract the key pieces of information needed from the "leagues of insensate cacophony … and incoherencies"? Many organizations have deployed extensive in-house security solutions and teams of analysts. However, human beings are not capable of finding and converting data into intelligence at the rate required for effective threat identification and mitigation.

Assume analysts find the right information at the right time in a format that is actionable. How can they efficiently and effectively enact the proper security safeguards to protect their organizations? Today's cyber threats often seem analogous to the volumes in Borges's library in two other ways: "The Library is so enormous that any reduction undertaken by humans is infinitesimal… [and]… there are always several hundreds of thousands of imperfect facsimiles – of works which differ only by one letter or one comma." The relative ease of creating variants of established threats, such as ransomware and banking Trojans, have multiplied the number available to threat actors. In addition, small modifications to the functionality of existing threats can be enough to bypass an enacted patch or other safeguard that is effective against an earlier iteration of the same threat.

A potential solution available to today's security analysts is one that Borges's narrator and his fellow inhabitants of the Library of Babel did not imagine.

METRIC	VALUE	NOTES	SOURCE
Worldwide Internet Users	3.3 billion		Internet Live Stats
Websites	1.035 billion		Internet Live Stats
Emails Sent so far in 2016	34.4 trillion	As of June 2, 2016	Internet Live Stats
Internet Traffic so far in 2016	470 trillion gigabytes	As of June 2, 2016	Internet Live Stats
Skype Calls so far in 2016	28.4 billion	As of June 2, 2016	Internet Live Stats
Websites Hacked so far in 2016	9.869 billion	As of June 2, 2016	Internet Live Stats
2015 Worldwide Social Network Users	2.04 billion		Statista
Projected Worldwide Social Network Users in 2016	2.22 billion		Statista

The Digital Library of Babel

THREAT INTELLIGENCE PLATFORMS

Threat Intelligence Platforms (TIPs) provide tools to help security analysts make efficient and effective use of data gathered on cyber threats globally. TIPs help to solve the following threat intel challenges:

- Collecting an adequate volume of useful data to understand the threat environment
- Automatically sifting out useless and/or non-actionable data, without human effort
- Contextualizing information to understand its relevance
- Correlating information to see patterns and connections between active threats and potential vulnerabilities
- Prioritizing actions to safeguard against threats and mitigate risk in a timely manner

Many TIPs use data feeds that automate the collection and classification of raw threat data. Data gathered from external sources, such as the Internet, are provided in various formats, which may include:

- Structured threat data in a standardized format, such as Structured Threat Information Expression (STIX), which is distributed via means such as Trusted Automated Exchange of Indicator Information (TAXII). Such formats make it easier to share information between security products and among teams.
- Open source intelligence (OSINT) and unstructured data collected from surface web, deep web, and darknet sources.

- Internet intelligence (e.g., malicious command and control servers, infected domains, etc.) to relate the threats to a specific organization's publicly advertised attack surface.

In order to progress from collecting data to generating threat intelligence, the information gathered must be fed into a TIP, which performs the following functions:

- Converts data into relevant and actionable intel
- Creates a window onto global threat intel
- Shows how external threats correlate with internal network telemetry
- Provides a single pain of glass for security professionals to interact with, enrich, and share intelligence
- Generates reports on physical security, threats to brand reputation, and other non-IT related threats

TIPs translate a seemingly limitless amount of raw threat data into actionable intelligence.

THE LOOKINGGLASS APPROACH: THREAT INTELLIGENCE PLATFORM

The LookingGlass TIP plays a key role in the threat intelligence life cycle, which consists of the following:

1. Acquiring
2. Aggregating
3. Actioning

The first step in the threat intelligence life cycle is to acquire the raw threat data to inform intelligence. LookingGlass provides six proprietary data feeds of machine readable threat intelligence (MRTI), which are summarized below.

DATA FEED	WHAT IT DOES
Virus Tracker	Provides one of the largest-scale feeds on current infections worldwide, along with a searchable database of historical records dating back to 2012
Cyveillance Infection Records	Sourced from Virus Tracker, creates a list of newly identified and historical infections globally
Cyveillance Malicious Command and Control (C2)	Sourced from Virus Tracker, reverse-engineers malware and extracts the long-lived and ephemeral domains of command and control (C2) servers that control malware remotely
Cyveillance Malicious URL	Provides a continuous feed of infectious web pages and malware hosting locations discovered to be live on the Internet
Cyveillance Phishing URL	Provides a continuous feed of locations used in thousands of phishing attacks across hundreds of companies, websites, and industries daily
Cyveillance Newly Registered Domain	Gathers the authoritative "master list" of registered domain names for the more than 100,000 new domain names that are registered every day

Table 1. Summary of LookingGlass Proprietary Threat Intelligence Feeds

The Cyveillance Malware Total Life Cycle Protection Data Bundle provides all of these feeds together. In addition to proprietary feeds, LookingGlass draws from third-party sources to provide data from a total of 140 feeds.

Once the data are acquired, they must be aggregated so that humans can analyze them. The primary purpose of a TIP is to aggregate data in a way that can be analyzed and monitored by humans. For this, the LookingGlass TIP portfolio provides the following:

ScoutVision

What it does: Provides a platform for security analysts who are hunting specific threats. Allows analysts to efficiently and effectively monitor tens of millions of global threats aggregated through a single console.

Why it matters: Threat analysts face many challenges, but one of those challenges is not a shortage of data that can be collected from across the Internet. Data feeds such as LookingGlass's MRTI automates data collection, ensuring analysts have enough information to make informed decisions. However, the vast amount of available data is unstructured. Valuable data are intermixed with useless data. And, in native format, the data have no context, making it difficult to see how data are relevant and actionable.

ScoutVision gathers information from 140 feeds across the Internet, providing one of the most complete pictures of the current threat landscape. Using big data analytics, ScoutVision converts unstructured data into a standard format that can be efficiently and effectively managed by humans.

The information is presented in a map that conveys an updated Internet topology, including networks, servers, and domains. This immediately contextualizes the data and enables threat analysts to see how threats outside of the organization's networks relate to their own assets (e.g., servers, applications, devices, etc.).

ScoutVision's Threat Indicator Confidence (TIC) then scores each threat based on the tools, tactics, and procedures (TTP) it uses. The score is directly related to the organization's environment (e.g., networks, applications, etc.). The factors that determine the TIC are transparent to and configurable by analysts. This score contextualizes the data and gives analysts a means to logically prioritize actions based on the relevance, severity, and likelihood of the threat.

USERS	Expert level: Security incident responders, Threat analysts, Third-party risk monitors
PURPOSE	To identify, analyze, and monitor threats outside the organization in a single console
TYPES OF DATA	Threat intelligence gathered on the global Internet outside of the enterprise network, including: • Tactics, techniques, procedures (TTP) • Domains associated with rogue command and control (C2) servers • Route hijacking / malicious uniform resource locators (URLs)
GOALS FOR INTEL	Gather / Format / Aggregate / Analyze / Search / Correlate / Score / Prioritize / Act
KEY FEATURES	• Aggregated threat data • Current Internet topology • Threat Indicator Confidence (TIC) • Collaboration spaces • Visual search and big data analysis • Extensible application programming interface (API) • Flexible deployment configurations

Table 2. ScoutVision Use Cases

ScoutPrime

What it does: Provides a platform for analysts seeking to create workflows. Provides customizable scoring and alerting features to contextualize the presentation of actionable threat intel.

Why it matters: The ability to act on relevant intel in a timely manner is critical to protecting the organization. ScoutPrime provides a way to customize how threat intelligence is viewed, scored, prioritized, and acted upon. Whereas ScoutVision is suited to expert security professionals hunting threats, ScoutPrime is suited to security professionals concerned with consuming and sharing threat intelligence, as well as organizing responses to threats.

Central to ScoutPrime is the ability to easily share threat intelligence and to collaborate with colleagues. ScoutPrime provides a set of customizable dashboards that can be configured to functional roles, such as internal security operations or third-party risk managers. Dashboards can be shared, along with tools such as response checklists.

A big challenge for security professionals is handling the sheer amount of alerts they receive, which may or may not be legitimate security incidents. ScoutPrime provides TIC as a way to rank threats. TIC is customizable based on factors such as the organization's environment (e.g., networks, applications, etc.), the threat landscape (e.g., geographical prevalence of attacks), and the organization's security posture. This helps prioritize alerts that are more likely to be real, relevant, and imminent to the organization, thereby reducing "alert fatigue."

The features in ScoutPrime are designed to make discovering threats easier and to reduce time to action.

USERS	Intermediate to expert level: Security operations staff, Threat analysts, Third-party risk monitors
PURPOSE	To monitor prioritized threats, share intelligence, collaborate with colleagues, and organize workflows
TYPES OF DATA	Threat intelligence gathered on the global Internet outside of the enterprise network, including: • Tactics, techniques, procedures (TTP) • Domains associated with rogue command and control (C2) servers • Route hijacking / malicious uniform resource locators (URLs)
GOALS FOR INTEL	Gather / Format / Aggregate / Analyze / Search / Correlate / Score / Organize / Prioritize / Act
KEY FEATURES	• Aggregated threat data • Current Internet topology • Customizable dashboards and collaboration spaces • Threat Indicator Confidence (TIC) • Graph explorer • Extensible API • Flexible deployment configurations

Table 3. ScoutPrime Use Case

ScoutInterXect

What it does: Provides an "inside-out" view of threat intelligence that complements ScoutVision's "outside-in" view. Fuses network telemetry with global threat indicators and Internet intelligence to identify in real time, or historically, how internal hosts are interacting with threats located on the global Internet.

Why it matters: ScoutVision and ScoutPrime focus on gathering information and identifying threats outside of an organization's environment. ScoutInterXect is a plug-in for ScoutVision (4.4 and above) that enables analysts to see specifically how assets within their own environment (e.g., applications, devices, etc.) are interacting with threats outside of the organization.

ScoutInterXect achieves this by gathering data using nfdump, a utility that shows how data is flowing through an organization's network. The nfdump data can be organized by IP addresses, ports, or other network parameters. By correlating enterprise network traffic with threat intelligence, analysts can further operationalize data in incident response and digital forensics.

USERS	Expert level: Security incident responders, Threat analysts, Third-party risk monitors
PURPOSE	To correlate telemetry data from inside the enterprise environment (e.g., servers, applications, etc.) with external threat intelligence for incident response and digital forensics
TYPES OF DATA	Data gathered via the utility nfdump on net flows inside the enterprise network, including: • Traffic between IP addresses • Traffic to specific ports • Other networking data, such as number of packets, flags, type(s) of service, bytes, packets per second, bytes per second, bytes per packet, etc.
GOALS FOR INTEL	Gather / Aggregate / Analyze / Correlate / Prioritize / Act
KEY FEATURES	• Threat correlation • Active and forensic reporting • Collaborative investigations • Intelligence filtering • ScoutVision integration (as a plug-in) • API accessible

Table 4. ScoutInterXect Use Cases

Cyber Threat Center (CTC)

What it does: Complements existing network and Internet Protocol (IP)-based threat capabilities, with a focus on identifying OSINT and threats not directly related to the enterprise network. Combines surface/deep web and darknet search, social media monitoring, underground forum information, and image-based search with a suite of tools and databases in a single platform.

Why it matters: ScoutVision, ScoutPrime, and ScoutInterXect are designed around a network-centric threat intelligence model, which focuses on how threats affect the enterprise network and IT assets (e.g., applications, devices, etc.). However, network-centric intel is but one type of important threat information. The Cyber Threat Center (CTC) provides a suite of tools focused on non-network indicators.

For instance, following a successful breach, stolen data often appear for sale in darknet forums. Identifying enterprise data online would be indicative that a successful attack on the organization has already occurred, prompting the need for digital forensics to identify how the attack happened and if the threat is persistent. CTC enables advanced searches of the surface/deep web and the darknet, including underground forums.

Another example of non-network centric intelligence would be indicators of an insider threat. CTC enables monitoring of social media, which could provide intel on a planned or past insider attack (e.g., a blog post or tweet expressing frustration with the employer or bragging about a successful exploit).
The CTC supplements network-centric threats with valuable non-network/IT-based threat intelligence.

USERS	Intermediate to expert level: Security incident responders, Threat analysts, Third-party risk monitors
PURPOSE	To identify, analyze, and monitor non-network-centric and IT-based threats, such as physical security and brand reputation
TYPES OF DATA	Threat intelligence gathered on the global Internet outside of the enterprise network, including: • Surface/deep web and darknet searches • Image searches • Social media • Underground forums
GOALS FOR INTEL	Gather / Format / Aggregate / Analyze / Search / Correlate / Score / Prioritize / Act
KEY FEATURES	• Centralized Internet monitoring • Analyst toolbox • Alerts and reporting • Global intelligence reports and threat maps

Table 5. Cyber Threat Center Use Cases

CONCLUSION: TRANSLATING DIGITAL BABEL

Today's IT professionals charged with security face countless challenges. One of the biggest is gaining a complete picture and clear understanding of the threat landscape. The Internet is so large, the threats are so numerous, and the volume of data is so high, yet the key information needed to make informed, timely decisions is out there. The challenge is to efficiently acquire, aggregate, and act on it.

Threat intelligence platform enables analysts to gather enough data to understand the threat landscape and then convert that data into actionable intel. A TIP creates a window onto global Internet, correlates threats with internal network telemetry, and provides a single platform for analysts to analyze, share, and monitor threats.
Threat Intelligence Platform is one key piece in the threat intelligence life cycle of:

1. Acquiring
2. Aggregating
3. Actioning

TIPs translate a babel of seemingly limitless information into actionable intelligence.

LookingGlass is the only company that incorporates a TIP into an end-to-end threat intelligence solution.

For more, read the white paper on Machine Readable Threat Intelligence and Threat Mitigation. Learn more by visiting LookingGlass.

ABOUT LOOKINGGLASS CYBER SOLUTIONS

LookingGlass delivers the most comprehensive threat intelligence-driven solutions in the market, enabling security teams to efficiently and effectively address threats throughout the cyber threat life cycle.

With a scalable solutions portfolio of threat data feeds, a threat intelligence platform, threat mitigation solutions, and threat intelligence services, LookingGlass enables security teams to prevent, detect, understand, and respond to analyzed, prioritized, relevant threats.

Additionally, with a deep knowledge of the global Internet topology and near real-time activity, LookingGlass helps organizations understand threats inside and outside their perimeter – including threats that may be impacting third party trusted partners, other organizations in their industry, and the latest threat trends impacting the global Internet at large.

Know More. Risk Less.