THREAT INTELLIGENCE

Threat Intelligence Integration:

# FROM SOURCE TO SECURE

graylog

# TABLE OF CONTENTS

# INTRODUCTION

As cyberattacks grow in frequency and complexity, businesses are turning to threat intelligence to better understand those attacks and protect themselves. Threat intelligence uses data points to provide an understanding of threats to an organization, but intelligence is only as good as the data available. If data isn't delivered in a form that's actionable, organizations won't know how to use that information to defend their environments.

Even with clean, usable data available, many organizations still don't make use of any sort of threat intelligence in their operations. Others may have a source of threat intelligence, but are not getting the value they could. Some simply lack understanding of choosing a threat intelligence source or how to integrate that information into their environments.

In this guide, you'll learn what you stand to gain through the use and integration of threat intelligence, what to consider when selecting a source of threat intelligence, and how to make threat intelligence work for your organization.

# WHY THREAT INTELLIGENCE

Threat intelligence can be a useful addition to your security toolkit. It can provide your analysts with information and context they would not have otherwise. There are many factors to consider, including where to obtain the intelligence, how to collect it, how to integrate it, and how much to automate.

Threat intelligence may offer opportunities to increase efficiency through automation, perhaps even enabling automated responses to the most common and highest severity threats. However, this often requires additional stakeholder education and technical safeguards to avoid interfering with business processes.

Threat intelligence is not a cure-all. No threat intelligence sources or platforms can replace a team of skilled analysts, but they can make those analysts faster and much more effective by giving them powerful tools to do their jobs better. And that means better security for your systems.

## CHOOSING THREAT INTELLIGENCE SOURCES

Threat intelligence providers track indicators of compromise (IOCs). IOCs are identifiable pieces of information captured from a compromise attempt that has happened either on your network or somewhere else in the world.

These indicators are collected and distributed, either by open source or commercial entities. Organizations can subscribe to one or more feeds and build databases of indicators.

As you begin to research threat intelligence sources, let your needs and your team's capabilities guide you.

However you choose to collect and integrate threat information, make sure your current technology stack can support those methods before you select, much less purchase anything. Once you've established some must-haves and guiding principles, you'll be better equipped to consider multiple options:

### FREE / OPEN SOURCE FEEDS

Free feeds all get their indicators from the same sources and report on the same indicators. Although that provides a large breadth of knowledge, it also creates large areas of overlap and duplication of data, which must be managed.

**Though logs are the usual method to get information from your environment to compare to these feeds. They are not the only way to gather this data.**

## PURCHASED FEEDS

Several dozen vendors offer feeds for purchase, each with their own areas of focus. The quality of paid feeds is often high, but their focus can be narrow, requiring multiple feeds to get the breadth desired.

## THREAT INTELLIGENCE PLATFORMS

Threat intelligence platform providers can offer a valuable stepping stone for organizations just getting started with threat intelligence.

These providers offer feeds of their own original research and a large number of curated open source or other free feeds. They also typically provide a well-developed API or other tool that simplifies feed integration. Included curation, enrichment, and deduplication can enhance the quality of "free" threat intelligence feeds considerably.

Many platform providers also provide a "knowledge base" of indicators, threat actors, campaigns, and methods. Since they bundle curation, integration toolkits, and knowledge base features, platforms can come with a higher price than individual threat intelligence feeds.

As you make your decision, consider the methods supported for collecting and ingesting those feeds. Some are much more manual than others. Though logs are the usual method to get information from your environment to compare to these feeds, they are not the only way to gather this data.

# INTEGRATING THREAT FEEDS

**Once you've chosen a threat intelligence source, you'll be ready to integrate threat feeds and start understanding what your security is up against.**

Depending on vendor support, there are direct integrations available for firewalls, proxies, DNS, EDR, web gateways, and IPS. Additional custom integrations are possible for any technology that supports making API calls.

During integration, you may opt to enrich indicators as they come in, adding information that will be useful to analysts right into the log events themselves. Keep in mind that whatever enhancements you build into your process will require ongoing maintenance, which should be part of your overall cost/benefit analysis.

You can create something real-time like email alerts for when a log event matches an indicator, but depending on your sources and the volume of events you produce, that may result in a flood of notifications. For most, starting with a daily report that details indicator matches works best.

## HOW TO INTEGRATE THREAT FEEDS WITH LOG MANAGEMENT/SIEM

- Determine types of indicators available in the feed
- Examine the logs from your security devices
- Determine which fields from these logs contain information that is comparable against indicators
- Establish mechanisms (rules) for comparing and alerting analysts when a match exists
- Notify analysts of a match

However, matches do not necessarily represent attacks against your network. You'll need to investigate and vet matches to know if they represent an imminent threat. This situation is where a threat intelligence knowledge base can help decrease the burden of investigation on already under-staffed IT teams. These knowledge bases differ from threat intelligence feeds by providing context on indicators found in your environment. Using a knowledge base helps speed up investigations and provides useful context to analysts trying to make decisions about incident response.

## HOW THREAT INTELLIGENCE INTEGRATION WORKS

Integrating threat intelligence feeds with a log management or SIEM solution lets users create rules that compare each indicator against relevant information in a log entry. Users can opt to receive notification of every match in real time or via a list for later review.

Indicators can take many forms, such as: IP addresses, domain names, URLs, MD5, SHA hash values, or snippets of code. Creating a database of these different indicator forms can help you in the future. You can build this database by allowing users to check an IP address seen in firewall logs to help you determine if it has been involved in any malicious behavior, or let users compare hashes in the logs of their anti-malware solutions to those in the database. This process of database building can and should be automated, since tens of millions of daily indicators makes checking even a tiny fraction of indicators against logs manually impossible.

## BUILDING AN INDICATOR DATABASE

- IP Addresses
- Domain Names
- URLs
- MD5
- SHA Hash Values
- Snippets of Code

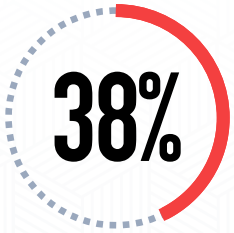
# THREAT INTELLIGENCE AUTOMATION

Automating your own processes squeezes some extra value from security dollars you have already spent. If some decisions are so simple that a machine can make them, why waste an expensive human on them? However, not all decisions are simple enough for automation — for instance, some security processes.

When Intrusion Prevention Systems (IPS) began supplanting Intrusion Detection Systems (IDS), IDSes were meant to detect intrusions and humans responded to them. IPSes offered the ability to see attacks in real time and to block threats automatically. However, false positives were common enough that management did not allow automatic blocking to be enabled. For long stretches of time, IPSes stayed in "passive" or "observe" modes.

Now, improvements in IPS technology have made them trustworthy enough to automatically block malicious traffic, whatever its source. Threat intelligence feeds are at a similar crossroads now. To respond to the most pressing needs of organizations, threat intelligence solutions already automate the most repetitive tasks, such as data collection and processing. This automation results in fewer manual processes, allowing analysts to focus on higher value tasks. The next logical use of automation is to allow automated blocking for the highest threat matches that are found by these automated processes.

**Before automated blocking begins, most organizations must convince business stakeholders that legitimate traffic won't be blocked with an automated system.**




**of organizations rely on manual processes to aggregate and analyze threat intelligence today**

Source: Enterprise Strategy Group

## MAKING THE CASE FOR AUTOMATED BLOCKING

Automation is an efficient way to inform users of events, but the burden of response still lies with people. So, without a full staff to review results, automation could be of limited benefit.

Before automated blocking begins, most organizations must convince business stakeholders that legitimate traffic won't be blocked with an automated system. Several strategies can help. For example, you can mitigate the risk by setting a high bar for automated blocking, using indicator confidence scores or restricting blocking to communication with critical assets only. Or, mandate that simple connections or attempts to or from a known indicator are not enough to block automatically, but a connection attempt accompanied by an alert from a second technology is.

This obstacle may also be overcome when security practitioners help decision makers fully understand the advantages of automation as well as the risks of choosing not to automate. For instance, weigh the risk of blocking legitimate traffic against the risk of interacting with a known bad indicator — does your organization really want to keep communicating with a supplier if they are compromised and could potentially compromise your systems as well?

# INTEGRATING THREAT INTELLIGENCE WITH GRAYLOG

Graylog simplifies threat intelligence integration by shipping with a threat intelligence plugin that allows lookups of IPv4 addresses and domain names. In just a few steps, you can prepare your data and generate a pipeline to draw out threat intelligence. Graylog supports many feed providers and allows for easy integration of those not yet supported.

## PREPARING DATA FOR THREAT INTELLIGENCE

Choose which log event sources you want to compare against

Identify the fields to use for comparison

Normalize field names

Select streams to be included in lookup processing

Install & configure the Graylog Threat Intelligence plugin

# CONCLUSION

Threat intelligence can be a useful addition to your security toolkit. It can provide your analysts with information and context they would not have otherwise. There are many factors to consider, including where to obtain the intelligence, how to collect it, how to integrate it, and how much to automate.

Threat intelligence may offer opportunities to increase efficiency through automation, perhaps even enabling automated responses to the most common and highest severity threats. However, this often requires additional stakeholder education and technical safeguards to avoid interfering with business processes.

Threat intelligence is not a cure-all. No threat intelligence sources or platforms can replace a team of skilled analysts, but they can make those analysts faster and much more effective by giving them powerful tools to do their jobs better. And that means better security for your systems.

## ABOUT GRAYLOG

Graylog is a leader in log management and Security Information Event Management (SIEM), making the world and its data more efficient and secure. Built by practitioners with the practitioner in mind, Graylog unlocks answers from data for thousands of IT and security professionals who solve security, compliance, operational, and DevOps issues every day. Deployed in more than 50,000 installations worldwide, Graylog is an award-winning platform built for speed and scale in capturing, storing, and enabling real-time analysis of terabytes of machine data. Graylog eliminates the noise and delivers an exceptional user experience by making data analysis, threat hunting, detection, and incident investigation fast and efficient using a more cost-effective and flexible architecture.

www.graylog.org
info@graylog.com
1301 Fannin Street, Suite 2140
Houston, TX 77002