EclecticIQ

Intelligence at the core

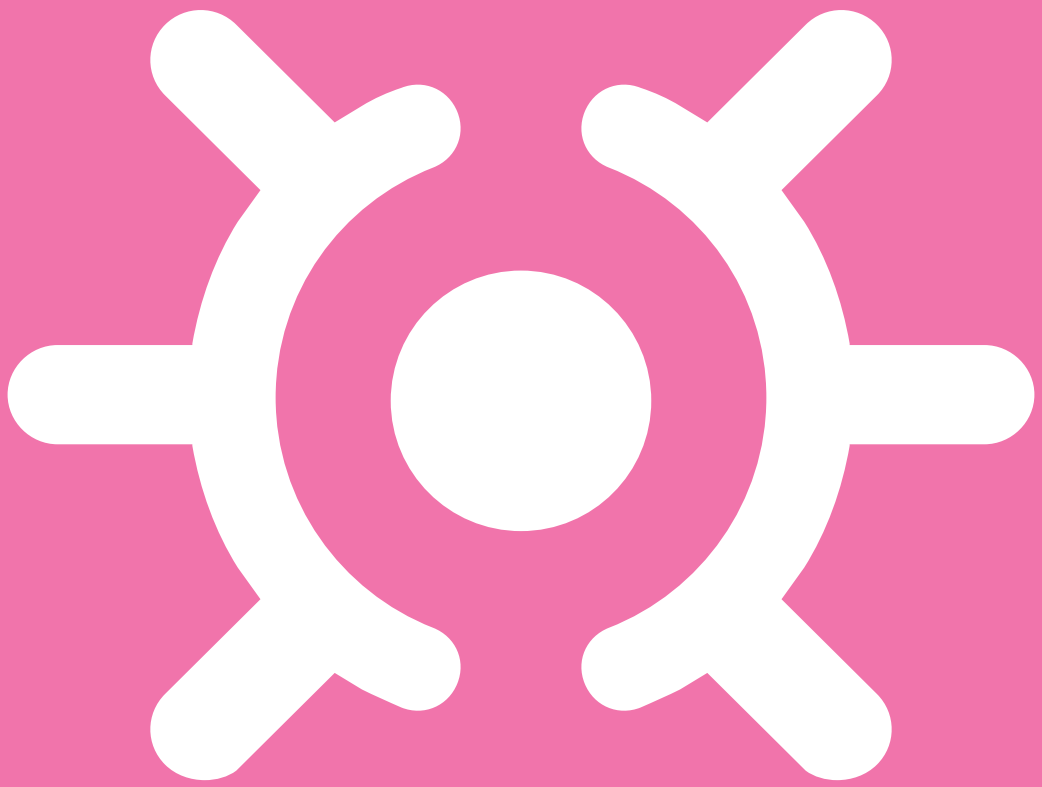
Intelligence
Automation
Collaboration

WHITE PAPER

Accelerate Incident Response with Threat Intelligence

With case studies from **FoxIt**

www.eclecticiq.com



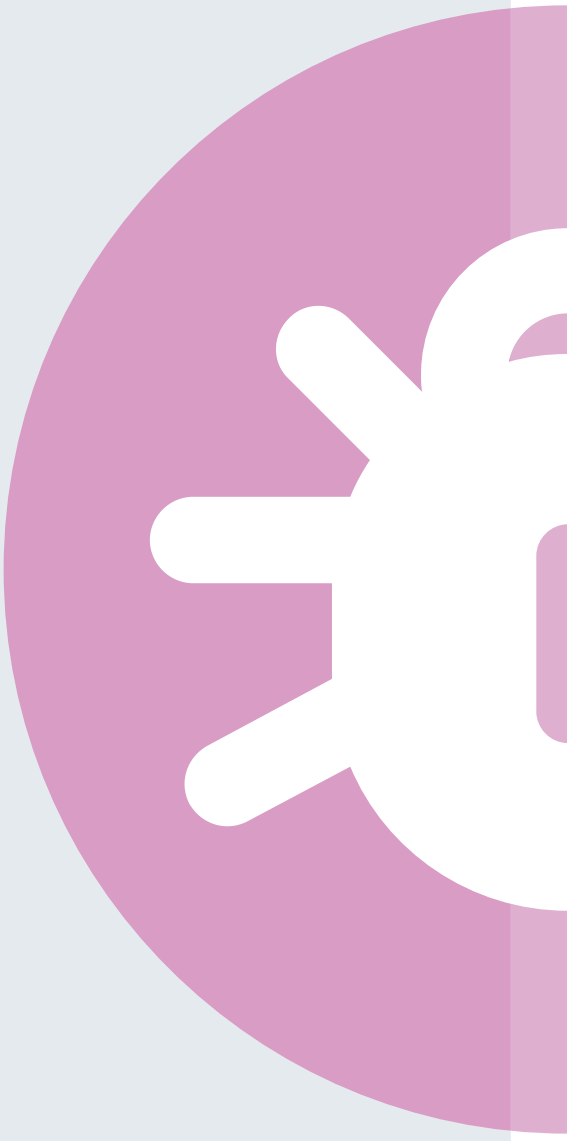
How Threat Intelligence improves Incident Response

It's a tough world out there. Even as nation-state actors have developed powerful new capabilities, criminal groups have developed capabilities formerly limited to nation-states. Through online profiles and social engineering, attackers can develop detailed dossiers on their targets and then use that information to create a spear-phishing email. Upon gaining a foothold into an organization's systems, it may take just a couple of days to exfiltrate data.

Most cyber attacks go undetected – fewer than 1 in 4, according to Verizon's 2016 Data Breach Investigations Report. That's one main reason organizations are pressuring their Incident Response teams and Computer Emergency Response Teams (CERTs) to become faster and more effective at detecting and nullifying attacks. Given that it takes mere minutes for an attacker to compromise an organization's systems, Incident Response teams must be able to make an impact as fast as possible to prevent data exfiltration.

Much can happen in those critical days. However, organizations and their Security Operations Centers (SOCs) may miss the opportunity window if they focus on the wrong things. For organizations to be more effective in combatting cyber threats, they must accelerate response times in two important areas, with threat intelligence playing an important role for both:

1. Escalate faster: Speed at escalating serious cyber threats to an incident response team
2. React faster: Speed by incident response teams in neutralizing cyber threats



1 Escalate faster

Many serious incidents never get reported to an incident response team. This happens when the first response to a cyber threat falls upon system administrators whose primary concern is to maintain normal operations. For example, when a sysadmin sees that malicious software (e.g. a password-stealing keystroke logger) has been found on a desktop PC, they may trust in the efficacy of the antivirus software in removing the software. A more careful sysadmin may take the extra step of reinstalling the affected machine from a system image.

These basic approaches miss some potentially important data: How did the malware get into the system? Who put it there? Are there other threats happening simultaneously? Is something dangerous happening, or about to happen? Merely turning the status lights back to “green” is not enough to combat cyber threats.

It’s difficult for a sysadmin to know when a cyber threat warrants escalation to an incident response team. There are too many alerts and intrusion attempts that overwhelm them with unhelpful information. Security vendors often provide raw data, such as large lists of IP addresses, lacking context, quality rating, or expiration dates, and this data generates too many false positives.

To make the information actionable, organizations need to discern between low-level and highlevel threats. That’s a key application of threat intelligence. By incorporating information about cyber threats into the sysadmin dashboard, it makes it possible for sysadmins to know when the escalate in the face of an attack, rather than just switching off the alarm.

2 React faster

When an Incident Response team arrives at an organization, they have hours, or at most, days, to mount an effective real-time response. These teams are responsible for following the trail: How was the malicious executable introduced? From which machine? When? Can the next step be prevented? Yet much of the focus of Incident Response teams has often relied too heavily on digital forensics – which takes weeks or months.

The idea behind data forensics is to gather enough evidence to not only identify the culprit, but also to get a conviction in court. This follows the law enforcement approach in other areas of criminal investigation.

This requires specialists to take infected machines offline, create copies of storage media, and analyze the interactions between infected files and the computing environment, all while maintaining auditable records of forensic activities.

Due to these complexities, data forensics is a difficult activity. It takes significant investment in time and resources to conduct digital forensics, and in the best-case scenario investigators can provide law enforcement with sufficient evidence to report a crime within weeks or months. Furthermore, the expected payoff is low. It's very difficult to arrest or otherwise create negative consequences for foreign adversaries, and cyber crime is not the biggest priority for local police departments.

That's why Incident Response teams are moving instead to a faster approach that values speed to an effective defense rather than perfect preservation of evidence.

Using Threat Intelligence, an Incident Response team can draw upon vast sources of information about everything from zero-day exploits of connected devices to well-known phishing attacks using email. Instead of spending time analyzing PC hardware and disassembling code samples, responders should instead start by searching through consolidated feeds of threat intelligence to locate a match.

The combination of Threat Intelligence and Incident Response allows organizations to detect threats faster, repel attacks with less disruption, and respond quickly enough to prevent adversaries from stealing data or causing any other lasting damage.

Figure 1: Insight into the overall threat landscape – Verizon Data Breach Investigations Report

How to Add Threat Intelligence to Incident Response

Add Threat Intelligence to Incident Response with the following four components:

1 Intelligence Requirements

The starting point for threat intelligence is to understand your needs, by generating answers to the questions including:

- What are the biggest risks involved with your industry and business?
- What types of attackers would have the motivation to target your organization?
- What data and processes would be most valuable to attackers?

By auditing your organization's intelligence requirements with the assistance of cyber security specialists, you can get an overall sense of which categories of attack you should be best prepared to defend against.

2 Threat Intelligence Feeds

Based on your research into intelligence requirements, the next step is to find intelligence feeds that address the most likely threats.

For example, if your biggest risk is industrial espionage of R&D projects, focus on feeds that specialize in malware being used by entities known to be working for government entities.

At the same time, you should also be plugged into threat intelligence provided by informationsharing and analysis centers (ISACs) and other communities specific to your industry.

There may be overlap between the information delivered by multiple feeds. This is to be expected, and it's an advantage to cross-check data from multiple sources. With the right tooling, duplicate data can be handled easily.

3 Threat Intelligence Platform

Organizations with immature cyber threat defenses often have an overreliance on the raw data from their threat intelligence feeds. Without the right tooling to ingest and make use of the various feeds, those feeds are very difficult to use. Organizations may miss important items contained in rarely-used feeds, or become overwhelmed by information from data-rich daily feeds. Even the act of sorting through and processing the feeds can be a significant chore for an enterprise IT department.

A threat intelligence platform automates intelligence consolidation from diverse sources, including internal and external feeds. By having the latest threat information at hand in a single, searchable location, system administrators and incident response teams can create the best benefit of the extensive data provided by diverse sources of threat intelligence.

4 Process and Roles

System administrators use threat intelligence to become better at spotting cyber attacks that justify calling incident response teams; incident response teams use threat intelligence to achieve faster results with less effort; and threat analysts use threat intelligence to adjust the organization's overall stance to cyber risk on an ongoing basis.

System administrators: An enterprise-ready threat intelligence platform integrates with enterprise security technologies, giving enriched data to system administrators within the platforms and diagnostic tools that they already use. Instead of only seeing that a cyber attack has been detected, a system administrator can discover information about the attacker, giving correct justifications for the decision to call in an Incident Response team where warranted.

Incident Response teams: An Incident Response team can tap directly into the full range of feeds contained in the Threat Intelligence Platform, searching based on any number of key characteristics. In addition, the integration between threat intelligence and enterprise IT solutions provides a window into internal data sources and systems that can enable Incident Response teams to respond faster to cyber threats.

Threat analysts: Even at organizations that rely heavily upon Incident Response teams, internal threat analysts have an important role to play in ensuring that the feeds being brought into a Threat Intelligence Platform match the evolving risk profile of the organization. As an ongoing role, threat analysts also need to collaborate with industry peers, stay informed about emerging threats, and assess organizational vulnerabilities based on incoming information.

Organizational Benefits of Threat Intelligence with Incident Response

1 Faster Incident Response

Instead of commencing a drawn-out process of digital forensics, experts in cyber defense can instead focus on formulating the correct response to a cyber attack. Repair the breach based on timely, complete information about adversaries and attack methods.

2 Damage and loss control

Threat Intelligence improves the ability of an Incident Response team to prevent attackers from reaching their ultimate objectives, whether it be gaining user rights, installing surveillance software, or exfiltrating data.

3 Cost savings through automation

By connecting Threat Intelligence to existing IT security solutions and system administration tools (e.g. updating a proxy server with daily updates to an IP address blacklist), organizations not only narrow the attack window for cyber attackers, but also reduce system downtime and free up IT resources for more productive activities.

Case study: Faster than Forensics

When the recipient of a suspicious email questioned the sender about its contents and authenticity, it raised the alarm about a potential cyber threat at a large company. Fox-IT's Computer Emergency Response Team (FoxCERT) arrived at the client site and discovered that an employee's machine was infected with malware and was sending out emails to everyone in the victim's address book.

In situations like these, the usual response is to start a traditional forensic investigation, in which the investigators pore over the infected machine for malicious code samples. Then, specialists place the potential malicious code in a protected sandbox environment, observe it in action and reverse-engineer it when needed to determine its capabilities. Such a process can take days or longer, depending on the complexity of the malicious code.

Fox-IT took a much faster and more effective approach during this case. FoxCERT captured the unique "signature" of the malware by applying a hash function to a sample of infected code, and then checked that signature within EclecticIQ Platform. They quickly found a match, learning from the EclecticIQ Platform how the malware works and what the malware capabilities are. This revealed that the malware after installing itself on the victim's machine is speading itself by sending emails to other users based on the sender's address book.

The EclecticIQ platform also showed that the malware had remote control and keylogging functionality. EclecticIQ Platform also provided information on how to confirm the diagnosis and remove the malware. The response team checked for other Indicators of Compromise on the machines within that organization and identified that more machines were infected with the same malware. Within a short period, FoxCERT cleaned up the infected computers throughout the organization.

Moreover, the threat intelligence in EclecticIQ Platform offered a broader view of the attack. The malware was part of a known malware family, and part of a wider campaign that could be attributed to a foreign group whose activities were being widely followed in the intelligence community. Using this knowledge, the incident response team was also able to inform the customer that this attack not only targeted them, but was part of a broader scope.

Takeaway: Forensic investigation continues to have a highly important role in cyber defense, especially when new attack types and code samples are discovered. Yet it's a significant waste of time and resources to perform forensic analysis on code samples that have already been detected, analyzed, and distributed among cyber defense sharing communities. Incident response drawing upon threat intelligence delivers the fastest and most effective method of neutralizing and finding (other) threats within the environment. Furthermore, by using threat intelligence to identify an adversary's other modes of attack, an incident response team can perform a more thorough job of protecting clients.

Case study: Understanding the *modus operandi* of an attacker

A company executive received an email, purportedly from the recipient's mother, containing a suspicious attachment. The email was detected as fraudulent and forwarded to Fox-IT's CERT team.

The FoxCERT team performed a detailed analysis on the email, the attachment, and the infected payload that was part of the attachment. This analysis yielded several data points: the subject line of the email, the filename of the attachment (an MS Word document), the IP address that was used to send the email, the domain name that was used as the "from" address, the intended behavior of the payload (e.g. attempted outgoing connection to an IP address or domain), and the unique hash of the payload.

Then, the FoxCERT team fed these data points into EclecticIQ Platform. This turned up information about a known threat actor whose preferred attack method was to send "spearphishing" emails to targets. The threat actor's modus operandi was to send infected attachments, using different filenames. In the platform other filenames were stored, that have been seen in other attacks by the same threat actor.

Given that intelligence, the FoxCERT team searched in the email logs for those suspicious filenames. By doing so, they identified other "spear-phishing" emails to other employees – i.e., other company executives who may have opened an attachment from the same threat actor. The FoxCERT team investigated the other employee machines that have received the emails with the other filenames but did not find any traces that the emails have been opened.

Takeaway: By using threat intelligence to identify the source of a campaign, the incident response team followed the most direct path to remediation not only for the original email, but for other spear-phishing emails from the same adversary.

Through this approach, the Incident Response team avoided the need to conduct a full companywide incident response search across the whole network, ultimately reducing cost and saving time.

Conclusions

Focusing on the wrong things during the first critical hours and days of a cyber attack causes organizations to miss the window of opportunity to prevent data or financial loss. Faster detection of serious threats leads to faster escalation, and hence faster reaction. The combination of Threat Intelligence and Incident Response allows organizations to detect threats faster, repel attacks with less disruption, and respond quickly enough to prevent adversaries from stealing data or causing any other lasting damage.

For organizations seeking to add threat intelligence to their emergency incident response capacity, the starting point is to establish the scope of intelligence requirements. Based on those requirements, the next step is to select and acquire the relevant intelligence feeds and opensource intel data. Then, to make that data actionable during an attack, it's essential to ingest, normalize and analyse intelligence feeds within a threat intelligence platform that connects with other IT security solutions and external partners.

Using this approach, organizations can respond to incidents faster, reducing the financial and reputational damage caused by cyber attacks. Moreover, by automating processes and systematizing controls involved with incident response, organizations have achieved significant cost savings and efficiency gains relative to unstructured, manual approaches to managing the complexities of threat intelligence.

EclecticIQ

Intelligence at the core

Intelligence
Automation
Collaboration

About EclecticIQ

EclecticIQ is a global provider of threat intelligence technology and services.

The most targeted organizations in the world – including governments and large enterprises – use our platform to automate intelligence management at scale and accelerate collaboration across security teams.

With our open and extensible cybersecurity platform and ecosystem, they are able to stay ahead of rapidly evolving threats and outmaneuver adversaries by embedding Intelligence at the core™ of their cyberdefenses.

Founded in 2014, EclecticIQ is a leading European cybersecurity vendor operating worldwide with teams across Europe, the UK, and North America, and via value-add partners.

Contact us at:
info@eclecticiq.com
www.eclecticiq.com