Enterprise Strategy Group | Getting to the bigger truth.™

ESG SHOWCASE

The Threat Intelligence Requirement

Date: November 2021 **Author:** Jon Oltsik, Senior Principal Analyst and Fellow

ABSTRACT: Organizations are engaged in a constant battle against cyber-criminals and other types of hackers. Sophisticated adversaries modify their tactics, techniques, and procedures (TTPs) as part of cyber-attack campaigns while simpler attackers change their indicators of compromise (IoCs) (e.g., IPs, domains, and files) to stay under the radar. In response, defenders must consume and internalize threat intelligence to efficiently filter the threats, understand offensive methods, and counteract them with cyber-defensive strategies and controls. Staying ahead in this battle depends on timely, comprehensive, and accurate threat intelligence from vendors like Bitdefender.

Overview

Organizations face perpetual waves of damaging cyber-attacks (i.e., data breaches, nation-state attacks, ransomware, supply-chain attacks, malware campaigns, etc.). To address this risk, CISOs are championing threat detection and response objectives, including (see Figure 1):[1]

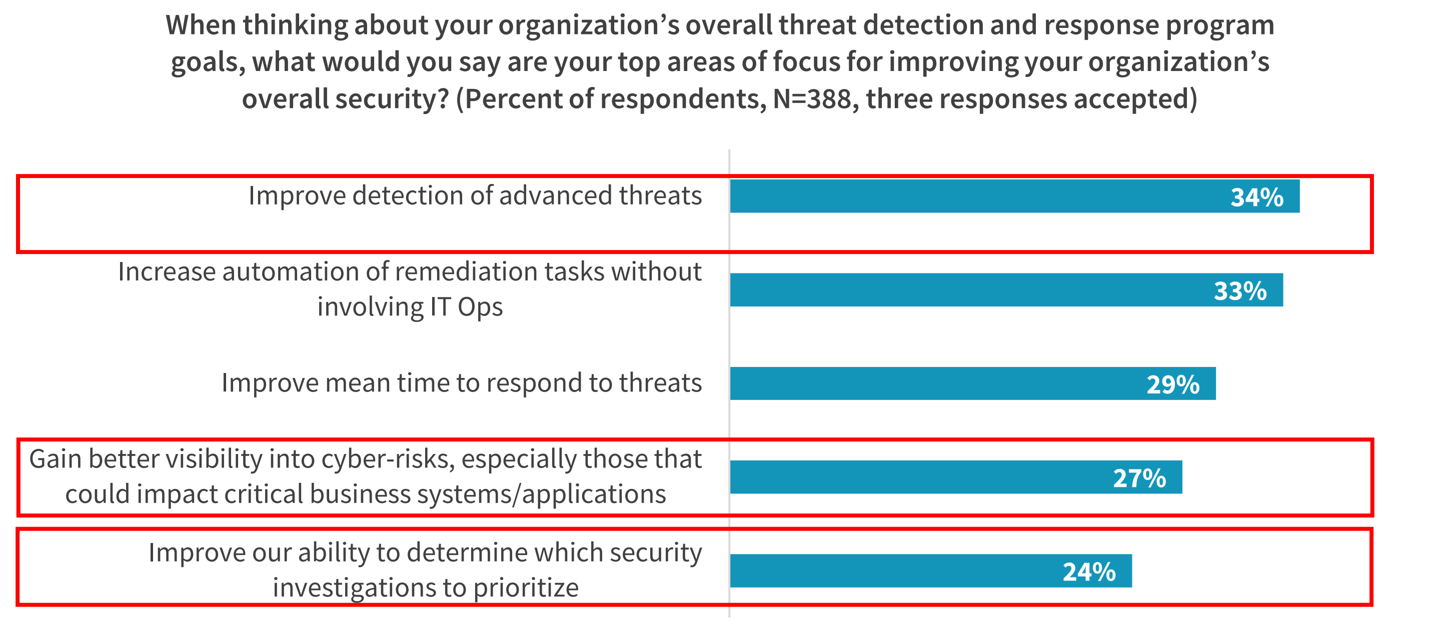
- Gaining better visibility into cyber-risks. SOC teams want a more detailed understanding of what bad guys are doing and how this could impact their business-critical IT systems. This requires granular knowledge of all assets across the attack surface correlated with threat intelligence about adversary IoCs and TTPs including known exploits. This information can help security teams prioritize remediation actions with the biggest business impact.

- Improving detection of advanced threats. Organizations want to detect threats faster and more accurately moving forward. This requires high-fidelity security alerts combined with threat intelligence on the latest adversary TTPs. In this way, security operation center (SOC) teams gain an understanding of anomalous/suspicious behavior on internal networks combined with timely intelligence about what's happening 'in the wild' (i.e., adversary TTPs, deep/dark web chatter, malicious reputation lists, etc.).

- Improving alert prioritization ability. Improving the fidelity and prioritization of alerts requires a deep understanding of asset value, attack campaigns, and discrete threats. Strong threat intelligence helps fine-tune detection rules, leading to improved security efficacy while streamlining security operations.

[1] Source: ESG Research Report, *The Impact of XDR in the Modern SOC*, March 2021. All ESG research references and charts in this showcase have been taken from this research report.

Figure 1. Top Five Threat Detection and Response Program Objectives



Source: Enterprise Strategy Group

Threat detection and response demands the ability to cope with scale and threat variety and then relate this intelligence to notable internal events in a timely manner. Organizations are pursuing the objectives above for these purposes.

Organizations Need High-quality Threat Intelligence

How can organizations make improvements and achieve these objectives? High-quality threat intelligence is a critical component of any solution. Indeed, CISOs recognize that they need high-quality threat intelligence delivered quickly and in sufficient quantities to enhance threat detection/response, security hygiene and posture management, and risk management.

As part of their consumption of high-quality threat intelligence, organizations are also:

- Demanding security technologies armed with strong threat intelligence. Many firms don't have teams of threat researchers to analyze threats or manage a threat intelligence platform (TIP) to operationalize raw threat feeds. As an alternative, security teams are asking for these capabilities from their security technology vendors. CISOs want security products that collect, process, analyze, and operationalize strong threat intelligence on their behalf. To achieve this, organizations need MRTI of timely and accurate IoC to filter out and block threats.

- Operationalizing threat intelligence. CISOs want timely and accurate threat intelligence so they can detect malicious TTPs early in the kill chain cycle, and automatically filter and/or qualify known IoCs to help in prioritization and reduce the defender's burden. Beyond threat detection, however, SOC teams seek to create a lifecycle process where machine-readable threat intelligence (MRTI) is shared with security systems and controls to block indicators of compromise (IoCs) like malicious websites, IP addresses, and files before they can execute or communicate with adversary command-and-control (C2) servers.

- Adopting the MITRE ATT&CK framework. The framework can help SOC teams gain a better understanding of how their security controls respond to specific cyber-adversary campaigns and TTPs. This knowledge can help organizations develop a threat-informed defense. To be clear, a 'threat-informed defense' applies a deep understanding of adversary tradecraft and technology that SOC teams can use as they build cybersecurity defenses to protect against, detect, and mitigate cyber-attacks.

Not All Threat Intelligence Is the Same

Threat intelligence varies from open source to expensive proprietary feeds. While all threat intelligence tries to cover the same needs, there are vast differences in threat intelligence quality and timeliness. Open source threat intelligence and even some commodity commercial threat feeds can contain a lot of false positive information and may suffer from timing delays, minimizing its value. Furthermore, some threat intelligence provides high-level information about threats but lacks any analysis or details specific to each threat.

CISOs know they need threat intelligence, but what threat intelligence characteristics are most important? ESG believes that the best (and most useful) threat intelligence will include:

- Volume and variety of threat sources. Threat intelligence should be collected from many globally distributed nodes, across different vectors like files, web domains, APIs, IP addresses, etc. Collection methods should also be varied using sources like active endpoints/servers, geographically distributed cloud-based sensors, and attractive honeynets. It's also important to have first-hand data with unique IoCs from a threat intelligence expert rather than a mix of third-party sources with overlapping repetitive data culled from other sources. The goal is to find and distribute details about threat capabilities, sources, infrastructure, and TTPs, as well as adversary motives, objectives, and resources.

- Data processing and management. Aside from collecting data, threat intelligence should also be codified and contextualized so it can deliver instant value. This is the essence of what separates threat intelligence from basic information. To achieve this, threat intelligence data processing must include normalization, synthesis, deduplication, labeling, categorizing, etc.

- Analysis. Beyond strong threat feeds, threat intelligence can be enhanced by an experienced team of threat analysts focused on specific types of attacks and adversaries. For example, some threat analysts may specialize in specific nation-state attacks, cyber-criminals, ransomware TTPs, or vertical industry attack campaigns. This analysis can be especially useful for targeted industries or organizations, helping them safeguard assets, block IoCs, and design the right countermeasures.

- Distribution and automation. To bolster defenses as quickly as possible, new threat intelligence indicators should be updated and distributed as quickly as possible. Furthermore, threat intelligence must be available in machine-readable format and then integrated directly with security controls to automate remediation actions like blocking network connections, suspicious domains, and malicious files. Through rapid distribution and automation, organizations can operationalize threat intelligence, even organizations lacking their own TIP or threat analyst team.

Aside from its technical benefits, accurate and timely threat intelligence can also help improve SOC team productivity. How? By doing analysis upfront and then delivering the who, what, why, where, and when of cyber-threats. This data can also help security analysts contextualize and prioritize risks to the business and then take actions for risk mitigation.

Enter Bitdefender Threat Intelligence

Threat intelligence has been coopted into a marketing term, as it seems that every vendor in the cybersecurity technology space claims to have 'industry leading' threat intelligence. This has led to lots of confusion, forcing security professionals to sort through marketing claims—a tedious waste of time.

Bitdefender threat intelligence is an exception here, as it stands out from industry hyperbole. Bitdefender has been working with security professionals since its inception in 2001 and has grown to more than 75,000 customers in 170 countries. Bitdefender threat intelligence aligns with the requirements defined above, as it:

- Covers a wide variety of data sources. Bitdefender collects various data elements from hundreds of millions of machines, including anonymized telemetry from business customers and end-users, global OEM ecosystems, dark web monitoring systems, web crawling systems, email traps, honeypots/honeynets, APT monitoring, and law-enforcement organizations. Data uncovered encompasses the gamut of adversary campaigns and TTPs.

- Processes, enriches, and collates threat intelligence data. Beyond distributing this raw threat intelligence data, Bitdefender processes the data through sandboxes to extract additional information on IoCs and TTPs. Additionally, Bitdefender algorithms are designed to find threat intelligence data similarities, correlate behavior across threat campaigns, associate attacks on vertical industries, and even attribute threat intelligence elements to specific threat actors and cyber-attack campaigns. This context can help Bitdefender customers operationalize threat intelligence to fortify their defenses.

- Supplements raw data with a global team of analysts. Of Bitdefender's 1600 employees, 285 are elite security researchers, threat hunters, and security analysts. Aside from internal threat analysis, this team works closely on incident response with law enforcement and collaborates with leading academics on quantum computing and cryptography. This team helps Bitdefender turn raw data into threat intelligence insights for customers.

- Provides comprehensive reputation services to end-customers and OEMs. Reputation lists provide a 'quick win' for organizations by helping them operationalize threat intelligence in real-time and continuously block IoCs used in the latest cyber-attacks. Bitdefender provides comprehensive reputation lists covering domain reputation, URL reputation, vulnerabilities, file hashes, and IP reputation, and delivers its threat intelligence in a machine-readable, digestible format that can be integrated into other security technologies such as security information and event management (SIEM) systems; security orchestration, automation, and response (SOAR) tools; web application firewalls (WAFs); secure web gateways (SWGs); etc. Reputation feeds are delivered in real-time and include domain reputation, URL reputation, vulnerabilities, file hash reputation, and IP reputation. Bitdefender threat intelligence is consumed by its global customers and a growing list of OEM partners.

With its coverage, analytics, and reputation services, Bitdefender threat intelligence can help customers and OEM partners identify ongoing threats, anticipate future threats, and block TTPs *before* they turn into damaging cyber-attacks and data breaches.

The Bigger Truth

Security professionals are often encouraged to 'think like the enemy' to determine how an adversary would attack their organization and what TTPs they would use to accomplish these goals. Experienced infosec pros may understand general attack techniques but rely on threat intelligence to fill in details about the latest attack campaigns. Armed with this knowledge, they can then identify cyber-risks, determine risk mitigation strategies, and design effective security controls for protecting business-critical assets.

While this is a proven recipe, the ingredients can mean the difference between success and failure. Timely, comprehensive, and accurate threat intelligence is a key ingredient here—an area where Bitdefender has 20 years of experience, process automation, and continuous improvement. This enables Bitdefender customers to operationalize threat intelligence and improve security efficacy while streamlining operations. Bitdefender OEM partners can also benefit by empowering customers to accurately detect, assess, and block pressing threats.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188