PATHFINDER REPORT

451 Research® | Advisory

Make Threat Intelligence Smarter With Security Orchestration

Automation and Optimization Are Your Best Friends

JANUARY 2018

COMMISSIONED BY

Infoblox®
CONTROL YOUR NETWORK

About this paper

A Pathfinder paper navigates decision-makers through the issues surrounding a specific technology or business case, explores the business value of adoption, and recommends the range of considerations and concrete next steps in the decision-making process.

About 451 Research

451 Research is a preeminent information technology research and advisory company. With a core focus on technology innovation and market disruption, we provide essential insight for leaders of the digital economy. More than 100 analysts and consultants deliver that insight via syndicated research, advisory services and live events to over 1,000 client organizations in North America, Europe and around the world. Founded in 2000 and headquartered in New York, 451 Research is a division of The 451 Group.

The information contained herein has been obtained from sources believed to be reliable. 451 Research disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although 451 Research may discuss legal issues related to the information technology business, 451 Research does not provide legal advice or services and their research should not be construed or used as such.

451 Research shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.

NEW YORK
1411 Broadway
New York NY 10018
+1 212 505 3030

SAN FRANCISCO
140 Geary Street
San Francisco, CA 94108
+1 415 989 1555

LONDON
Paxton House
(Ground floor)
30, Artillery Lane
London, E1 7LS, UK
P +44 (0) 207 426 1050

BOSTON
75-101 Federal Street
5th Floor
Boston, MA 02110
Phone: +1 617.598.7200
Fax: +1 617.357.7495

EXECUTIVE SUMMARY

Effective enterprise security has always required a blending of tools, and advances in the threat landscape are changing the careful balance that many have maintained. Protection and mitigation elements continue to be important, but the rate at which new threats appear now requires a much greater reliance on threat intelligence and tightly integrated solutions to provide insight into protection priorities and more efficient incident response. Selecting, managing and integrating intelligence feeds can be complex and is fraught with hazards for those that are new to this arena. Gaining visibility into DNS indicators of compromise with actionable network context and responding to these events using existing security tools is difficult without integrated network and security tools. This Pathfinder digs into the opportunities and challenges that exist for infosec practitioners.

Key Findings

- Actionable threat intelligence feeds are a necessary component in today's threat landscape.
- To be effective, threat intelligence has to be timely, prioritized by category, and have context and relevance.
- To handle the scale of today's threats, security operations need to be automated and orchestrated using tool integration to share data.
- Actionable network intelligence should be used to help in response prioritization.
- Centralizing threat intelligence can be beneficial to serve as a source of truth and coordinate action.
- Threat intelligence orchestration reduces the workload for security operations teams and allows them to be more effective while improving their organization's security posture.

Introduction

Information security has always been an area where the race between attacker and defender has been fiercely fought. A key element in that race has been the ability to gain an edge through timely information, effectively applied. Attackers scour for the latest vulnerabilities, while defenders build up protections and listen for hints of an attack. In recent years, enterprises have been turning to threat intelligence feeds to guide and prioritize their efforts. To gain the most value from threat intelligence, it needs to be integrated with security operations, and its actions need to be orchestrated. Feeds come in many forms, from informal updates to structured and packaged digital streams.

Whatever form it takes, threat intelligence needs to provide information that an enterprise can put to work efficiently. Because of the scale of attacks and the increasing agility of attackers, a good threat feed will generate a significant amount of information, and enterprises have to sort out what's relevant and what's urgent. That volume of data can place a significant burden on overworked security teams that need to establish the context of the alert and determine how it might impact their environment. It's a complex task of correlating assets, people and processes to put in motion. Sophisticated security orchestration and automation tools provide the kind of scale and speed necessary to accomplish the task and relieve teams from this potentially heavy burden.

COORDINATING ACROSS TEAMS

THE PROBLEM	THE RESOLUTION
Organizational boundaries limit effectiveness.	Integrate information to speed responses.

One of the largest challenges that enterprises face is sharing information across departments and teams. Often, each group has different priorities and operational management systems, and groups may refer to various assets in the environment in different ways. Navigating across technical boundaries and maintaining context can also be challenging. For example, if an operating system vulnerability is identified, there may not be current information on which applications are running on impacted servers, complicating the task of organizing remediation. Networking teams may refer to network addresses, while server admins look at machine names, and virtualization teams know VM names. To effectively use threat intelligence, the entire organization needs to be able to refer to a single reliable source of truth.

It's common for organizations to have multiple sources of threat intelligence, and this can also add complexity. More information should be help strengthen defenses and detect attacks, but if it's not correlated, or worse, if it's not combined at all, attack patterns can go unrecognized, and the opportunity to act early in the kill chain can be lost. Threat intelligence has to be combined across teams and sources and has to receive supporting levels of context and prioritization by category to make it actionable.

Effective Use of Threat Intelligence

Making effective use of threat intelligence goes beyond simply combining or correlating the information. It's important to ensure that event streams can catalyze action, and linking event streams between domains can be effective. For example, having a suspicious domain query that causes the DNS system to generate an event for a host management system to start a scan is a good start. However, there has to be greater sophistication in how those links are made, and they need to be automated. A speedy response favors the defender, and automation is the only way to gain sufficient advantage.

Correlation between threat intelligence and the enterprise's assets provides the next level of sophistication. A good threat feed could generate lots of potential actions, in some cases on a scale to swamp even automated systems. The more sophisticated approach manages the level of activity by prioritizing potential issues around the relevance and urgency necessary for the local environment. This approach applies activity effectively, with resources being directed to the activities that will have the greatest impact.

THE THREAT INTELLIGENCE PUZZLE

THE PROBLEM	THE RESOLUTION
Threat intelligence integration is complex.	Categorize and prioritize with local context.

Pulling together threat intelligence is like assembling a puzzle. The pieces need to fit together well, and the goal is to build a complete picture. The picture needs to encompass the various aspects of the infrastructure that the threat intelligence tool is working to protect. Systems and applications, as well as people and their associated identities all have a relevant part to play in solving the puzzle. Threat intelligence can come from external sources, but the people and systems that are being protected also generate fundamentally important information. This internally generated information benefits from the local context and relevance available with it. An effective threat intelligence environment will combine both internal and external sources.

Threat intelligence can offer insight, but the sheer volume of information has its own costs. It's easy to presume that all of the data in a feed is relevant or applicable. The reality is that, depending on the quality of any individual feed, a reasonable percentage may not apply to the local environment. Without a way to manage that event stream, a significant number of false positives will likely occur. False-positive events can waste resources and, in more egregious cases, reduce availability because systems or applications are taken off-line for unnecessary testing and remediation.

The level of detail that the threat intelligence provides is one measure of its quality. High-level intelligence on broad classes of vulnerabilities is good, but it's even better to understand the impact on local systems and processes, and that requires detail. Good sources of internal intelligence often provide much more detail, and this is particularly true in cases of active exploitation. Combining and curating internal and external threat intelligence can reduce false positives and allow more effective security operations. Augmenting external information with high-quality internal intelligence, and adding threat prioritization by category such as classes and properties, can build a powerful base from which to work.

SOLVING THE THREAT INTELLIGENCE PUZZLE

The benefit of detail is that it allows security operations to understand more about the applicability of any piece of threat intelligence. Establishing relevance is key to both prioritizing any necessary actions and understanding levels of risk. It ties an understanding of a potential issue to the parts of the local environment that it could affect.

To gain a more complete understanding of relevance, there has to be accurate correlation between events, risks and assets. A single source of truth – a system of record for the local infrastructure – has to be in place in order to allow the triangulation among all of the pieces of information. Many enterprises have independent or outdated configuration management systems. Networking records and address assignments may be maintained manually. These situations can lead to problems when trying to establish the relevance of any threat intelligence alert. If a server no longer runs a particular application, or a host now has a different address, the hope of accurately aligning threats and remediations can be dim.

Out-of-date information leads to either missing or misdirecting actions. To validate the impact of any suspected attacks or compromises, it's necessary to correlate the indicators of compromise (IoC) with the environment in which they occur. The IoCs will be specific to the type of event and the situation in which it occurs. If the facts available don't match the real environment, teams can miss compromised systems and target remediations at systems that don't need them.

To use threat intelligence more effectively, enterprises need to consider the full cycle of operations in their information security planning. Like the completed puzzle, all of the elements have to be considered and positioned correctly. A uniform threat intelligence environment has to extend across the infrastructure so that teams can coordinate their actions and knowledge. That will allow them to use a common language when working through issues and understanding risk. That understanding has to extend from knowledge to action. When issues are identified, there has to be the means for the organization to understand what actions are required and that the necessary remediations have been applied and are effective. While it's easy to tell when a piece of a puzzle is missing, it's much more difficult to do so in a complex IT environment, making a full-cycle approach important.

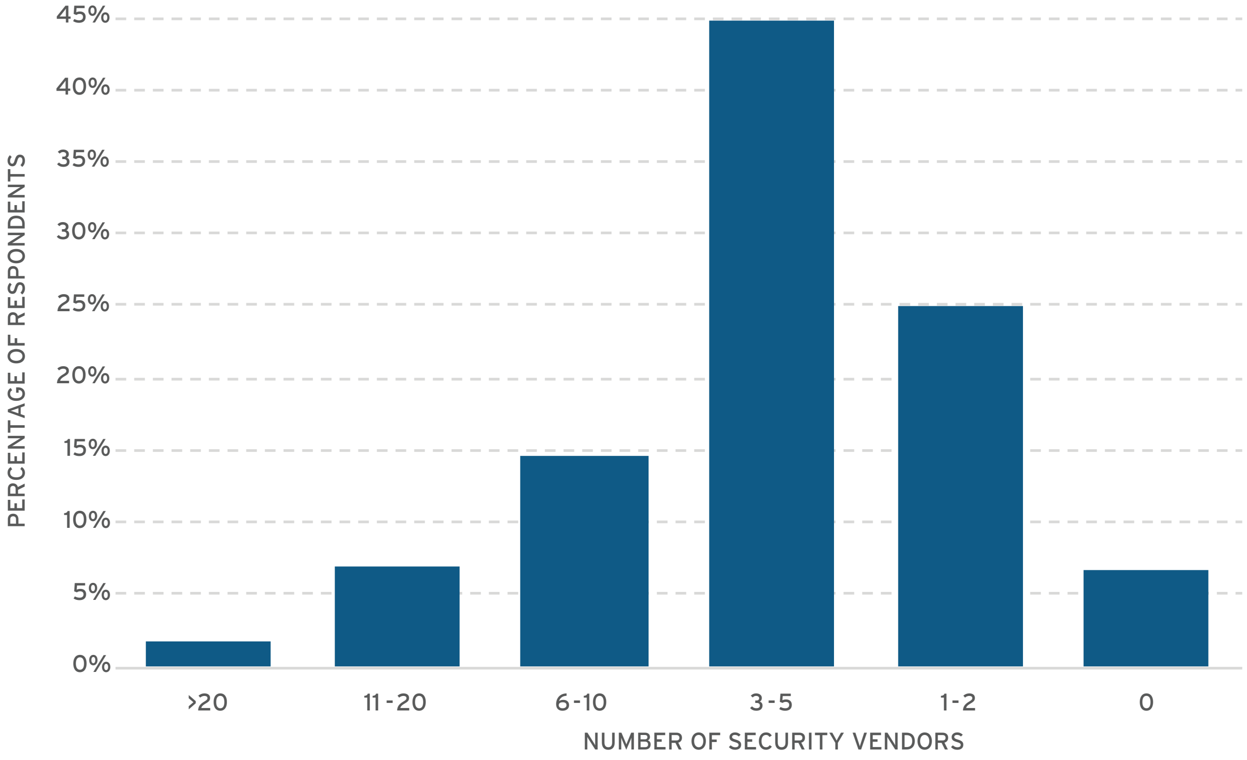
The tactics for success in security operations are built on coordination and integration. Information sources need to be coordinated and correlated. The information flows that guide operations have to be integrated into the systems, policies and procedures that make them all possible. Threat intelligence can raise the defensive posture when it's put to work effectively.

Security Orchestration and Automation

The operational environments for most enterprise security teams are filled with tools. In the recent 451 Research Voice of the Enterprise (VotE): Information Security, Budgets & Outlook study, we found that the median organization has three to five information security tool vendors as part of their operational environment. That translates to a significant management burden in existing environments. For most, there is limited information sharing between tools and, where SIM/SIEM systems exist, there isn't significant reduction in operational complexity. Lack of context prevents SOC teams from addressing the critical threats first. There is little visibility into DNS indicators of compromise. That's why it's critically important, when looking at threat intelligence and responding to DNS indicators of compromise, that network tools integrate with the existing infosec tool chain.

Figure 1: Making threat intelligence smarter with orchestration

Q9. How many different security vendors do you currently have in place in your organization? Base: Information Security Respondents



Source: 451 Research Voice of the Enterprise: Information Security, Budgets & Outlook 2017

THE CHALLENGES OF USING SILOED SECURITY TOOLS

THE PROBLEM	THE RESOLUTION
Too many tools don't share information.	Link tools and orchestrate actions.

The scope and scale of threats that enterprises are facing require that automation be put into place to allow teams to put up solid defenses. Operational management tools are often acquired independently by the different departments that use them, which means that the information they collect is often siloed – unavailable to other teams. It can also mean that there aren't common reference points for assets, and sometimes not even a common language to describe problems. Security analysts and administrators can easily fall prey to event fatigue; the constant stream of events, most of which don't require action, wears down their ability to react to events that do require attention.

TACTICS FOR EFFECTIVE SECURITY ORCHESTRATION

Implementing security orchestration and automation allows infosec professionals to raise their game by integrating tools and sharing information. They are free to deal with active threats, rather than wading through the mundane task of triaging ever-increasing event streams. Orchestrating and automating operations has the additional benefit of ensuring that there is real-time visibility into infrastructure changes that affect the enterprise security posture. Changes to network configurations and application environments can be immediately reflected in security environments so that the relevance of threat intelligence can be used to its full advantage.

Building a solid automation base enables the next stage of security orchestration maturity – automated threat response. This can be a game-changing enhancement to traditional security operations and can be integrated with little risk. There are a set of tasks that can be managed by more modern systems that can get a jump on potential problems when they're fed by high-quality threat intelligence. For example, DNS-derived IoCs, such as requests for malicious websites or botnet command and control servers, are high-fidelity drivers that can kick off scanning and protection strategies quickly and deliver information directly to security analysts, saving them precious time in knocking down infections or attacks.

Security orchestration and automation saves steps and can offer locally relevant context to more accurately prioritize actions. That avoids fatigue and lets teams be more efficient. That context allows the right actions to be applied and can form the link to validation and remediation systems, which can close the loop on the full security management cycle.

Conclusion

The operational benefits of a well-integrated threat intelligence capability go beyond making staff more effective. The insight provided can create an earlier understanding of threats and attacks. When threat intelligence is properly optimized, the information that it contains can be directly correlated with the current state of the enterprise infrastructure. It dramatically extends the situational awareness of security and operational teams. It can aid them in working together more effectively by providing a common source of truth, and it can expose the risks to the broader enterprise environment. Most importantly, it can speed the response to an attack, a critical factor in limiting damage and regaining control.

That improved situational awareness goes beyond the traditional focus on external threat actors and covers risks from internal actors as well. Blocking malware and botnets is important, and those same insights can be put to use managing data loss prevention and malicious data exfiltration. Activity information can show anomalies that can identify bad actors wherever they are operating.

There is a strong additional benefit for auditing and compliance that's created by the wealth of information that an integrated and orchestrated security environment provides. It can aid enterprises as they move to a continuous compliance footing and offer compliance information all the time, rather than just at audit. It can give an organization detailed information on the devices that are present and insight into what they're doing. This is particularly important as enterprises gear up for the greater volumes of devices that will arrive with the first wave of the Internet of Things.

Threat intelligence optimization and orchestration is an investment that can pay for itself many times over in the benefits that it offers in operational coordination and simplification and the improvement in the organization's overall security posture.

Managing enterprise security has always been challenging, but the availability of higher-quality threat intelligence has the power to transform traditional security operations. If it's put to work effectively, it can not only inform more intelligent actions, it can work to transform the manner in which security teams operate and the speed with which they get results. To capitalize on all of the potential benefits, enterprises need to invest in threat intelligence optimization and orchestration. They have to integrate threat feeds with the automation of security management systems to reduce the time and effort of threat identification and remediation. On this journey, there are important points to keep in mind:

- Threat intelligence can be a powerful addition if it's used effectively.
- Threat intelligence with local context, such as information from DNS infrastructure, is powerful.
- Operational security requires coordination and integration across teams and tools.
- Automation and orchestration are required to fully optimize threat intelligence use to improve the overall security posture.

With these as their guide, security teams can be prepared to address current threats with a more informed position and keep them aware and on guard for whatever the future holds.