securonix

WHITEPAPER

The Benefits of Unifying Your Threat Detection, Investigation and Response

Scaling security operations to keep up with threat inflation

Table of Contents

www.securonix.com

Introduction

Cybersecurity threats are increasingly putting pressure on security operations teams for several reasons. Cybercriminals are becoming more sophisticated, and our attack surface is constantly expanding as organizations adopt new technologies and expand their digital presence. Security operations teams must be able to monitor and defend against attacks across a wide range of devices, networks, and applications.

In addition to the unrelenting pressure of threats, the demand for skilled cybersecurity professionals far exceeds the supply, creating a shortage of qualified talent. The cybersecurity skills gap puts additional pressure on security operations teams, who must often do more with less. Overall, the combination of these factors creates a challenging environment for security teams, who must be constantly vigilant and proactive to protect their organizations from cyber threats. Organizations must scale up their security operations to protect their critical assets and reputation. But how can we scale up when resources are limited and the threat pressure keeps growing?

Unifying to simplify and streamline

During the past few years, understanding the importance of investing in detection and response, in addition to preventative measures, has grown to the point where most organizations have detection and response capabilities in place, or at least leverage service providers to deliver them. But the implementation of those capabilities rarely occurred in a one time, big bang way; most of the time detection and response capabilities are the product of multiple projects and initiatives, each one bringing to the table new processes, teams and technologies. The result? A complete set of capabilities, but siloed and poorly integrated, with multiple overlaps and inefficiencies wasting the precious resources available and dragging down the times to detect and respond to threats.

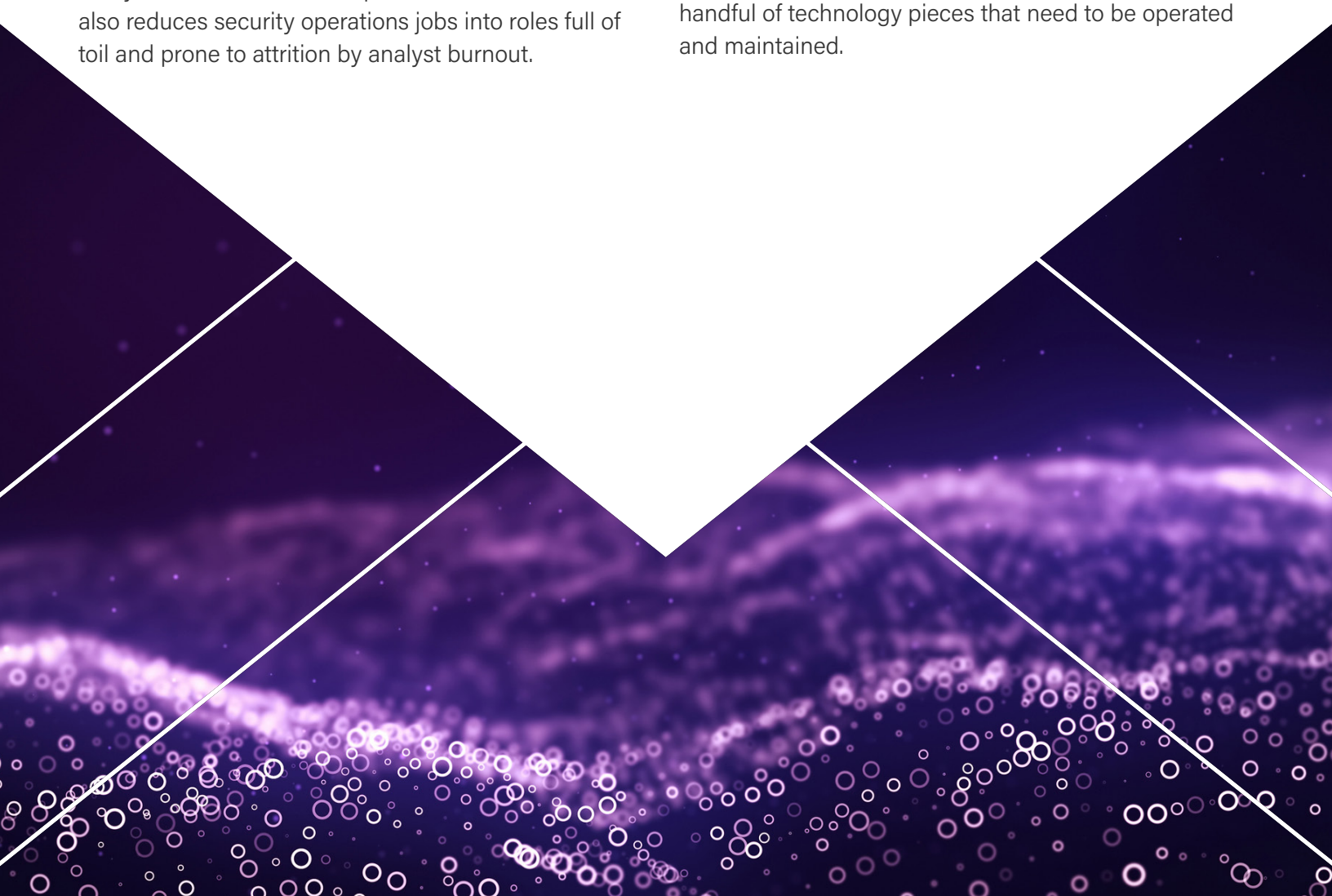
Streamlining the integration of those capabilities is a natural path to scale up. After all, a response process, simple or complex, manual or fully automated, will almost always follow a confirmed detection. Due to the additional work required to confirm detections and to understand the full implications of a breach, the "investigation" step has also become a required step between "D" and "R", creating the now commonly used "TDIR" acronym. But regardless of the acronym letters, the fact is that boundaries between those phases are not as clear as we imagine. While some organizations consider the investigative work as part of the "Detection" phase, others think investigation work is part of their "Response" process. Where should it reside, then? Is it part of detection or response, or is it something completely different from each one of those?

Trying to establish the boundaries between detection, investigation and response is an artificial and unnecessary exercise. Treating detection, investigation and response as a continuum has many advantages. Process boundaries commonly result in separate tools, teams and roles. This excessive fragmentation creates many handovers where the process can break, and it also reduces security operations jobs into roles full of toil and prone to attrition by analyst burnout.

Unifying threat detection, investigations, and response processes helps organizations reduce toil, minimize human error, and streamline incident response.

The security operations toolset

The siloed approach for detection and response has been around for so long that it left its traces on the toolset typically used by those functions. Many security teams use technologies such as Intrusion Detection Systems (IDS), Network Traffic Analytics (NTA) and SIEM for detection. The analysts working on detection are often monitoring the screens from those systems, waiting for alerts of malicious activity. Those alerts go through a triage process, and as any operational process like this one, it often requires some form of workflow tool to support it. Some organizations will rely on the workflow capabilities from their detection tools, while others may bring general purpose solutions such as Jira to keep a queue of alerts to be investigated. Separate detection tools, a workflow tool on top of them and the detection process is already responsible for a handful of technology pieces that need to be operated and maintained.



Each analyst has to be trained on each tool, and move from one UI to another while performing their jobs.

After that, comes the response part. With separate processes and teams, the technology stack for response ended up being built independently too. Some organizations would even put together a separate log centralization tool to be used during incident response, as the solutions used for detection would often keep data for only short periods of time, as well as restrict collection only for data necessary for detection use cases. Using another workflow tool, with case management capabilities, where all artifacts collected during the response process would be stored, is also a common technology component of that stack. To complete it, add forensics tools and solutions that enable containment and remediation actions, such as EDR. Put this stack together with the detection tools and we will end up with many moving parts, with multiple UIs and a lot of duplication.

Multiple UIs, many moving parts and duplication is why it's so important to consider the technology pieces when looking to unify TDIR processes; this unification has to go through a rationalization of the technology stack. If the processes will be treated as a unified continuum, a single workflow should be in place, to control all steps from early detection to the last steps of response. There is a lot of room to optimize interfaces and also opportunities to reduce toil.

The same UI can, and should accommodate detection and response, in a way that the transition between those two phases, as well as all the investigations work, can happen on the same platform without the need for context switching.

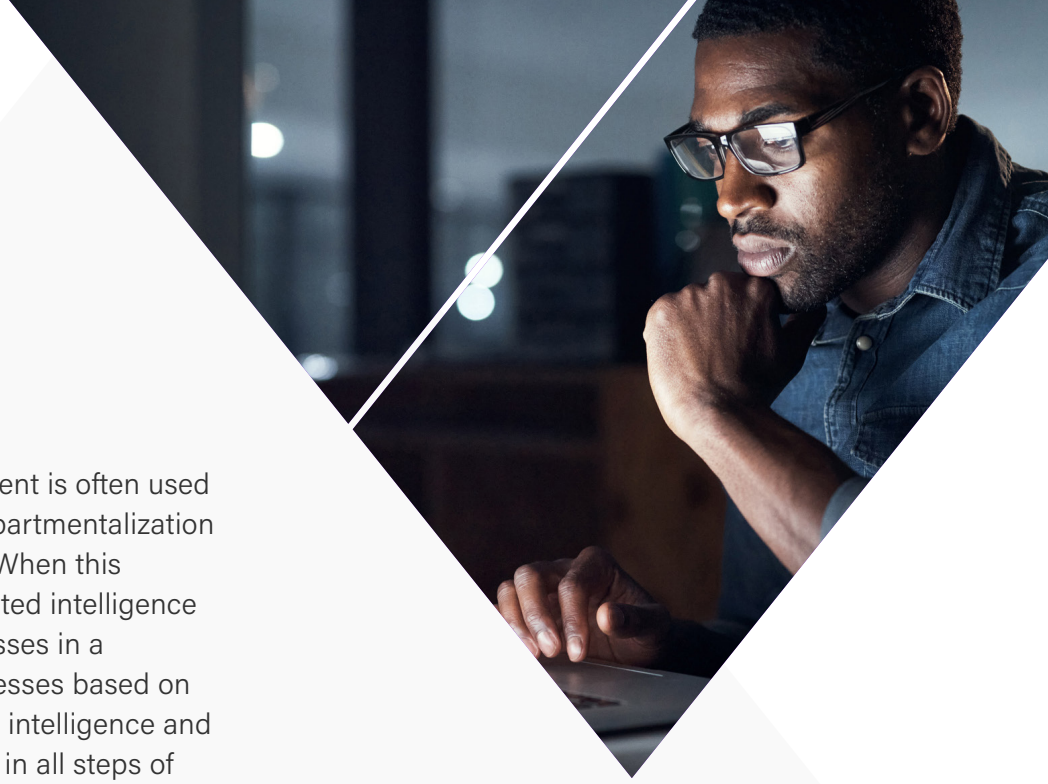
The consolidation should not stop at the user interface. In fact, a unified backend and platform is the major unification requirement, as it can enable and drive the changes more visible to the end user.

By unifying the data backend, for example, there is no need to separate log repositories, and having all security data stored in the same place not only makes sense from an economic perspective (it provides benefits from an economy of scale), but also provides consistency to processes and users, since the same data will be feeding the different processes and steps of TDIR.

Using the same platform across security operations processes provides more than just efficiency gains. It also enables the full integration of threat hunting with detection engineering and other detection-related processes. Threat hunters operating on the same platform can leverage all the data enrichment used for detection purposes, and detection engineers can operationalize hunts for online detection. Hunters save time leveraging work from the detection processes, and detection engineers save time leveraging work done by the hunters.

Making defense more proactive

A lot of time is wasted by security operations teams searching for indicators of compromise and additional context for investigations, usually obtained from threat intelligence sources and services. Interestingly, many times these items have been seen or produced by other members of the team, or even by security operations teams in other organizations that may be facing the same threats. Enhancing collaboration within the security team and with other organizations can elevate the value of threat intelligence. By sharing information and working together, teams can better understand emerging threats and develop effective mitigation strategies.



Threat intelligence and detection content is often used in a siloed manner, following the compartmentalization of TDIR processes mentioned above. When this happens, it's hard to ensure that ingested intelligence is being used throughout these processes in a consistent manner. Unified TDIR processes based on a unified platform can consume threat intelligence and even more complex detection content in all steps of TDIR, increasing the value of the collaboration. This consumption, when done via automated processes on a unified platform can make defense more proactive and ensure threats will not only be detected, but also disrupted in the shortest possible time.

Scaling up content production

Even when detection, investigations and response are flowing without artificial boundaries and perfectly integrated, there are still points in security operations that may introduce bottlenecks. Developing threat detection content and response playbooks is a typical, if not the major case. Content is hard to produce and tune given the many proprietary languages of disparate tools which are difficult to learn and master. The constant barrage of new threats makes it hard to meet the demand for new content, a situation that is directly affected by the cybersecurity skills shortage. Obtaining threat detection content as a continuous feed, in the same manner as we usually ingest threat intelligence, can eliminate this bottleneck. But how could organizations produce content in that manner, considering all their resource limitations?

Content-as-a-service, delivered in a continuous manner by specialized service providers can provide organizations with access to the latest threat intelligence and detection content updates.

The TDIR technology providers have a privileged position to provide content in this manner: They have the required technical skills and direct access to the delivery channels that ensure the content can be quickly deployed and tuned when necessary.

This continually updated content helps organizations stay ahead of new threats and improve their ability to detect and respond to incidents. There will always be a need for bespoke, business-specific content, but organizations should not be wasting cycles in developing and tuning content to detect threats that affect most organizations, such as typical ransomware or crypto mining campaigns. With content-as-a-service covering those general cases, internal teams can focus on better understanding the specific business needs and develop content that is unique to the organization.

Conclusion

Scaling up security operations is critical to protecting organizations against cyber threats. By unifying threat detection, investigations and response, organizations can remove artificial bottlenecks and inefficiencies in their security operations.

A modern platform, capable of enhancing collaboration and driving a more proactive defense, leveraging threat content, and utilizing powerful data cloud technology, can enable this unification and simplify the path to mature security capabilities.

Our most comprehensive TDIR solution is built on a highly scalable data cloud and offers seamless end-to-end experience from the analyst to the executive. Your team has access to threat content as a service, 365 days of hot search capabilities, and built-in automation and collaboration features for unified, rapid detection, investigation and response.

Securonix is leading the evolution of SIEM for today's hybrid cloud, data-driven enterprises. Securonix Unified Defense SIEM provides organizations with the first and only content-driven threat detection, investigation and response (TDIR) solution built with a highly scalable data cloud that provides a unified experience from the analyst to the CISO. The innovative cloud-native solution enables organizations to scale up their security operations and keep up with evolving threats.

For more information about Securonix, schedule a demo at: www.securonix.com/request-a-demo.

securonix

About Securonix

Securonix is leading the evolution of SIEM for today's hybrid cloud, data-driven enterprises. Securonix Unified Defense SIEM provides organizations with the first and only content-driven threat detection, investigation and response (TDIR) solution built with a highly scalable data cloud and a unified experience from the analyst to the CISO. The innovative cloud-native solution enables organizations to scale up their security operations and keep up with evolving threats.

Contact Securonix

www.securonix.com
info@securonix.com | (310) 641-1000