Integrating Prevention, Detection and Response Work Flows: SANS Survey on Security Optimization

G.W. Ray Davidson, PhD
Integrating Prevention, Detection and Response Workflows: SANS Survey on Security Optimization

A SANS Survey

Written by G.W. Ray Davidson, PhD
Advisor: Barbara Filkins

April 2017

Sponsored by
ThreatConnect
In 2014, Gartner proposed a security architecture\(^1\) for addressing cyber threats and vulnerabilities that consisted of four “pillars” or functions—prevention, detection, response and prediction—all working in a continuous loop. Others have proposed similar architectures, and guidelines such as the CIS Critical Security Controls provide detailed practices corresponding to each of these pillars. The most common representation of the model starts with prevention (including vulnerability management), then detection (using malware and threat analysis, firewalls, etc.), moving to strong response practices and then incorporating intelligence (prediction/re-utilization) to close the loop.\(^2\)

Organizations are beginning to implement functionality based on these models, so SANS developed a survey to assess how organizations are structuring them: Are these functional groups operating in unison with shared data and workflow, or are they remaining true to the tradition of operational silos in most technology groups?

For purposes of this survey, we recast Gartner’s “prediction” pillar as “intelligence,” and we also added a remediation function after the “response” activity because remediation has historically been handed off from the response group to an operations group after initial response and containment.

Lack of automation/integration and workflow between security operations and response functions are hindering organizations’ ability to prevent, detect and respond to threats, according to 64% of respondents. Only 15% of respondents assert that this lack of automation and integration between pillars does not impact their ability to prevent, detect, respond and remediate.

The survey indicates the need for centralized access to security and operational data to improve visibility and workflow across these functions, with only 17% of respondents saying that their workflow and visibility are completely or even mostly automated and integrated.

Despite low rates of integration, the value of pooling security resources and functions is not lost on these respondents. In this survey, 63% of respondents see great value in integrating prevention, detection, response and remediation to improve visibility and accuracy and to reduce time investment, while 23% see at least some value.

In this survey, we analyze satisfaction with staffing levels, tools and management-support architectures to help provide best practices and guidance for IT security practitioners.

---


2 [www.cisecurity.org/critical-controls.cfm](http://www.cisecurity.org/critical-controls.cfm)
As enterprises implement an adaptive security architecture, they face a decision: What is the best way to optimize each function in the existing organization, while providing both the tools and the focus to enable cross-functional security operations to protect the core business?

Is it better to create and manage separate groups for the prevention, detection, response, remediation and threat intelligence functions, or to combine them—either together, or with existing security or general IT functions? The enterprise’s decision will depend on both the size and maturity of the existing organization, and the choice may affect the efficiency and effectiveness of the architecture.3

Survey Respondents

Based on job title, 63% of respondents have a security-specific focus, with another 25% based in IT (including IT, systems and network administrators and analysts). Some of the write-in titles included incident responder, threat hunter, executive director of IT security, application security analyst and intelligence analyst.

Survey respondents covered a range of industries, with strong representation from those with a high degree of concern for security: 17% from banking and finance, 14% from IT security, 13% from government, 8% from healthcare and 8% from education, accounting for over 59% of the respondent pool. The large majority (85%) of responding organizations operate in the U.S., with 79% headquartered here as well. An increasing number have an overseas presence, as evidenced by 41% having operations in Europe and 31% in Asia.

---

3 This trade-off is sometimes known as the theory of constraints and is attributed to Eliyahu M. Goldratt as described in his 1984 novel, *The Goal* (re-issued in 2014; co-authored by Jeff Cox). The concept has been updated and applied to IT and DevOps in the recent novel, *The Phoenix Project* by Gene Kim, Kevin Behr and George Spafford.
Workforce size is distributed almost evenly across respondents, with 36% having 1–1,000 workers, 35% with 1,001–10,000 workers and 29% more than 10,000 workers. See Figure 1.

**Table 1. Organization Size Categories**

<table>
<thead>
<tr>
<th>Size Category</th>
<th>Parameters</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small</td>
<td>&lt;1,000</td>
<td>36%</td>
</tr>
<tr>
<td>Small Medium</td>
<td>1,001 to 5,000</td>
<td>22%</td>
</tr>
<tr>
<td>Medium</td>
<td>5,001 to 15,000</td>
<td>18%</td>
</tr>
<tr>
<td>Medium Large</td>
<td>15,001 to 50,000</td>
<td>9%</td>
</tr>
<tr>
<td>Large</td>
<td>Over 50,000</td>
<td>15%</td>
</tr>
</tbody>
</table>

For the purposes of further analysis, SANS then classified the organizations as described in Table 1.
Size of Teams

Size of security teams loosely correlates with the workforce size distribution:

- 30% of organizations have fewer than five security/risk management and privacy-related employees and contractors, and 28% of them fall into the small and small medium categories
- 33% have 5–20 such team members, with 30% of them coming from small and medium-size organizations
- 20% have 21–100 members, 13% of whom fall in the medium and large categories
- 14% have 101–1,000 such team members, with 10% coming from medium large and large organizations
- 3% have more than 1,000 team members, with 2.5% coming from large organizations

These relationships are likely due to the variety of industries represented and, of course, the variety of organizational types and efficiencies represented. See Figure 2.

![Team Size Versus Organization Size](image-url)
**Staffing and Leadership**

Just over 30% of respondents overall feel they have fully staffed their prevention, detection, response and remediation programs; and only 22% feel their intelligence functions are fully staffed. One possible conclusion is that intelligence is at the edge of the maturity horizon for this cohort of survey responders.

SANS also evaluated these results against the size categories defined previously. Completeness of staffing for each function appears to vary by size, with small organizations having significantly higher percentages for partially staffed functions. This emphasis on partial staffing appears to fall off as the size of the organization increases. In other words, not surprisingly, larger organizations rely on a greater number of dedicated resources for each function.

Across the board, about 30% say they are fully staffed, with intelligence being an exception at 21%; between 57% and 60% say they are partially staffed, again with the exception being intelligence at 48%. There is more of an emphasis on staffing for intelligence, however, with 22% saying that area needs additional staffing, as opposed to the rest of the functions, where between 8% and 10% point to the need for additional staffing.

Looking at the sample in its totality, the majority of responses indicate each function (prevention, detection, response/remediation, intelligence) is staffed by fewer than five dedicated or shared people, followed by “none,” and then 5–10 dedicated or shared people. The majority also indicate these are shared functions, rather than dedicated functions (see Figure 3).
Who’s in Charge? (CONTINUED)

Whether staffing is dedicated or shared, it appears to vary by size of organization. Additional analysis using our size categories revealed the following:

- Average team size, whether dedicated or shared, appears to be 1 to 4, with some small variations based on organization size. Team size, however, doesn’t expand dramatically for larger organizations.

- Smaller organizations appear to have a larger percentage of shared functions (as opposed to dedicated). They report sharing staff almost twice as frequently for prevention, detection, response and remediation. This difference appears to converge in most cases as organizational size increases. Larger organizations appear to rely more on dedicated staff.

TAKEAWAY

Just under 70% have full or partial staffing for cyber threat intelligence, and 8% say the function doesn’t need staffing at all. If an organization is not performing the basic operations of detection and remediation well, it isn’t sufficiently mature to implement threat intelligence functionality.
Primary oversight for prevention, detection, intelligence and response is mostly provided by security personnel who cover multiple security functions, rather than dedicated security staff. This may be a business decision—some organizations see wisdom in rolling security into everyday operations. Or, it may simply reflect the skills and staffing shortage noted in the following section. These demographics may be related to the size of the organization, but there is no clear correlation; still, smaller organizations tend to combine functions, and larger ones have more resources with which they can hire dedicated staff.

With that said, however, 13% to 16% do have dedicated oversight for each function (with the exception of intelligence at 11%).

In contrast, the remediation function is generally handled by IT operations staff, based on responses. IT operations staff are also the second-most common overseers for the prevention and response functions. This use of IT operations for processes in these functions reflects increasing maturity on the part of organizations. As processes become common, they can be documented and moved to operational groups, saving incident-specific activities associated with detection and response for the more specialized (and expensive) security group.4

**So Who’s in Charge? It Depends.**

Enterprises are struggling to determine the ideal structure for their security functions. In some enterprises, security functions are being handled by people wearing multiple hats. In others, the groups have dedicated leadership and focus. Each of these configurations is likely driven by the realities within the organization, but each has its advantages and disadvantages, and the ideal configuration is likely specific to each organization.

While enterprises see value in integrating their remediation workflow and security data processing, the specifics of how to organize these units are elusive. Integration of tools and workflow is equally problematic, as we discuss in the next section.

---

Disconnected Workflow and Tool Output

Some of organizations’ staffing problems are directly tied to their shortage of tools, particularly automation and integration. For example, survey respondents still spend considerable manual effort collecting security and intelligence data and applying data automatically where needed.

**A Matter of Workflow**

Results suggest the need for an industrial revolution in threat intelligence analysis and incident response, bringing enhanced automation and integration to these predominantly manual efforts. In this survey, a combination of manual and automated processes is used for data-related functions (collection, storage and analysis) and process-related functions (prevention, detection, response and remediation).

For 39%, data collection, storage and analysis processes are mostly or completely manual, with 42% saying they’re equally manual and automated. Overall, 45% say that their prevention, detection, response and remediation processes are still mostly or completely manual, with another 35% saying they’re half and half. Because less than 20% of respondents have their data and processes more than 50% automated across these security and risk management pillars, expansion of automation and integration represents a big area for improvement.

Overall, the survey shows a considerable skew toward manual, rather than automated and integrated processes, as illustrated in Figure 4.

![Figure 4. Automation and Integration Lacking](image-url)
The higher skew toward manual effort in the process-related functions is to be expected, as is the higher skew toward automated effort in the data-related functions. Maturing organizations attempt to automate routine processes, and data-related processes tend to be more routine than security-specific processes.

**Tools Deployed**

Organizations are deploying multiple tools to support their prevention, detection, response and remediation functions. Results show higher deployment in the proactive areas of prevention and detection, and somewhat lower implementation in the reactive areas of response and remediation. See Figure 5.

**What types of security tools and services does your organization use to protect, detect and respond to cyber threats? Select all that apply.**

![Figure 5. Prevention Most Common Use for Tools; Followed by Detection and Response](image-url)
Looking at the three most common tools deployed, anti-malware and endpoint security are the most commonly used for prevention and detection, closely followed by IDS/IPS/UTM, vulnerability management and web security. SIEM is most commonly used for detection, as is IDS and, interestingly, vulnerability management plays a strong role in detection. The latter is understandable, given that threats target specific vulnerabilities that may or may not be within the target organization.

Protection and prevention also strongly include web security, which makes sense, considering that browser-based vulnerabilities constitute one of the two leading causes of endpoint compromise. For the purpose of this discussion, SANS considers web security to include both the web portion of network connectivity and the web-enabled portion of a web-based application, but not necessarily the strictly internal part of the application that has no direct user interaction. The detection function adds IDS/IPS/UTM, and the response function, not surprisingly, also utilizes incident response-specific platforms.

**Endpoint Systems Protected**

An interesting finding regarding coverage of these tools is that 92% say their tools currently cover server endpoints, 86% say they cover company-owned devices and 79% cover their web-facing applications, as illustrated in Table 2.

<table>
<thead>
<tr>
<th>Answer Options</th>
<th>Yes</th>
<th>No, but Need To</th>
<th>No, and Don’t Need To</th>
<th>Unknown/Unsure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud services</td>
<td>35.0%</td>
<td>36.0%</td>
<td>23.2%</td>
<td>5.9%</td>
</tr>
<tr>
<td>Company-owned devices</td>
<td>85.6%</td>
<td>9.4%</td>
<td>3.5%</td>
<td>1.5%</td>
</tr>
<tr>
<td>Internal applications</td>
<td>77.2%</td>
<td>15.3%</td>
<td>4.5%</td>
<td>3.0%</td>
</tr>
<tr>
<td>Personal mobile devices</td>
<td>34.0%</td>
<td>35.0%</td>
<td>27.6%</td>
<td>3.4%</td>
</tr>
<tr>
<td>Server endpoints</td>
<td>91.5%</td>
<td>5.5%</td>
<td>1.5%</td>
<td>1.5%</td>
</tr>
<tr>
<td>Web-facing applications</td>
<td>78.6%</td>
<td>10.4%</td>
<td>6.0%</td>
<td>5.0%</td>
</tr>
<tr>
<td>Other</td>
<td>16.7%</td>
<td>4.2%</td>
<td>8.3%</td>
<td>70.8%</td>
</tr>
</tbody>
</table>

However, when we asked about cloud services and personal mobile devices, only about a third (35% and 34%, respectively) said they cover these endpoints, while about the same portion (36% and 35%, respectively) said those devices need to be covered. This seems counterintuitive, especially for personally owned devices, given that users, through their endpoints, are a primary source of compromise in the enterprise, according to multiple SANS surveys.6,7 As personal devices are used more often for business applications, these devices will be more important to protect the network and data from being compromised.

Centralizing Security Data

For organizations that want to integrate and automate their security processes, it is important to centralize, or at least provide appropriate access to security-related data. However, responses to the survey indicate that over half (54%) are not centralizing this data. Of the 37% who do centralize their prevention, detection, response and remediation data, 79% do so in a SIEM, 25% utilize repositories in the cloud and 24% use other analytics systems, meaning there is more than one repository for security data at most organizations. See Figure 6.

How/where is your prevention, detection and response data centralized? Select all that apply.

![Figure 6. SIEM Most Common Form of Data Centralization](image)

SIEMs and other centralization solutions are not “set it and forget it,” but require substantial customization and tuning. Given that (as noted previously) most organizations are not sufficiently staffed, maintaining a SIEM for organizing and centralizing data adds to the challenge.

---


Accessing Security Data

It’s also not clear whether all the appropriate parties have access to the data, but there are clear indicators that multiple roles—from security analysts to incident responders and operational IT members—do have access to the same security data. At organizations that centralize their prevention, detection and response data, 69% provide access to security analysts, 63% to responders, 61% to administrators and 57% to operational IT groups. See Figure 7.

Security-related data can be sensitive, and access should be restricted to those who need it for prevention, detection, response and remediation. With proper controls, this data can be used by both the security and operations groups to create a holistic approach to utilizing security and response information to support the overall security culture of the organization.

However, making the data available is only part of the challenge; it also needs to be interoperable. The field of interoperability is still maturing, with challenges in both syntax and semantics. This, again, speaks to the need for a holistic approach, covering both proactive and reactive components.
Integration Is Difficult

The same efficiencies that can be gained when centralizing data and integrating workflow across these functions are, perversely, the most critical inhibitors to organizations achieving this integration, according to respondents. In this survey, as with other SANS surveys, lack of skills and staffing for organizations of all sizes, cited by 84% of respondents, followed by lack of funding and management buy-in, highlighted by 56%, are the top two impediments keeping organizations from achieving the full visibility needed to prevent, detect, respond to and remediate events on their networks. The shortage of skilled practitioners in the field is well documented.\(^8\)

The third overall inhibitor was lack of workflow among prevention, detection, response and remediation programs (selected by 34% of respondents), which points back to the lack of interoperability noted previously. Another 33% of respondents also noted problems resulting from lack of a centralized knowledge aggregation tool. See Figure 8.

**TAKEAWAY:**

Automation and centralization can help relieve the sting of staffing and skills shortages if the new levels of automation and integration don’t require staff to master and maintain new, highly specialized skills.

---

Reviewing this information in light of organization size, however, reveals that although all organizations place the greatest emphasis on staffing and skills shortages as the main inhibitor holding their organization back from achieving full visibility, the secondary emphasis is not necessarily as consistent. Small firms through medium to large firms agree that lack of funding and management buy-in is the second largest inhibitor. Large firms differ in that they consider lack of communication among prevention, detection, response and remediation tools to be the second most important inhibitor, as illustrated in Table 3, where blue shading indicates the highest percentage of response, red represents the second level and yellow represents the third highest concern.

As organizations grow from small to large, they struggle with lack of technology (tools), then process (workflow) and then people-related challenges (especially communication).

<table>
<thead>
<tr>
<th>Table 3. Inhibitors by Size</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td>Small</td>
</tr>
<tr>
<td>Small Medium</td>
</tr>
<tr>
<td>Medium</td>
</tr>
<tr>
<td>Medium Large</td>
</tr>
<tr>
<td>Large</td>
</tr>
<tr>
<td>-----------------------------</td>
</tr>
<tr>
<td>Staffing and skills shortages</td>
</tr>
<tr>
<td>Lack of funding and management buy-in</td>
</tr>
<tr>
<td>Lack of a centralized knowledge aggregation tool</td>
</tr>
<tr>
<td>Lack of workflow among prevention, detection, response and remediation</td>
</tr>
<tr>
<td>Lack of standards for communicating security and threat data</td>
</tr>
<tr>
<td>Lack of communication among prevention, detection, response and remediation tools</td>
</tr>
<tr>
<td>Disjointed or disparate search capabilities for sources of threat intelligence</td>
</tr>
<tr>
<td>Lack of communication among prevention, detection, response and remediation teams</td>
</tr>
<tr>
<td>Inability to justify more spending because current investments don't work</td>
</tr>
<tr>
<td>Other</td>
</tr>
</tbody>
</table>

More differences are evident as one looks to the third and less important inhibitors. Despite the loose correlation between size of organization and security team, it is tempting to indulge human nature and perceive patterns in the data. Smaller firms (small and small medium) would like to support their overworked staff with more centralization of data in the form of a tool. As the organization (and perhaps the security team) increases in size, workflow among team members and different teams becomes increasingly important.
As the organization continues to grow, it may gain enough maturity to recognize that the critical nature of security is important and to fund and staff the security function. As the organization and security function become even larger, the tertiary inhibitor is communication among the teams. One way to think about this is to perceive that as organizations grow from small to large, they struggle with lack of technology (tools), then process (workflow) and then people-related challenges (especially communication).

Impact of Disparate Data and Workflow

Respondents felt strongly that the lack of workflow process integration and data centralization impacts their ability to prevent, detect and respond to threats. In the survey, 64% of responders felt that lack of automation impacted these functions, and another 21% said that they didn’t know. Only 15% definitively said that this lack of integration does not hinder their abilities in these areas. Figure 9 points out the shortfalls in reporting, lack of visibility and inability to detect new threats as the top limitations caused by lack of automation and integration.

In what areas have limitations in automation and/or centralization of security and threat data affected your ability to detect and respond to threats?

Select those areas where you see an impact.

- Shortfalls in reporting capabilities
- Lack of visibility into risk posture
- Lack of visibility into live threats under investigation
- Inability to detect new types of threats our antivirus doesn't know about
- Poorer detection rates
- Remediation failures
- Other

Figure 9. Limitations Due to Lack of Automation and/or Centralization
Most respondents are dissatisfied with time to detect incidents; several pointed out that if an incident is detected, it has already occurred, which is too late. Respondents are generally most satisfied with time to respond to an incident once detected, but are less satisfied with the time required to consider remediation complete. See Figure 10.

It’s interesting to note that it is also easier to determine the time between detection and response than it is to determine the time required for the other activities. One can never truly say that a compromise is remediated, for instance. That lingering doubt could affect satisfaction.

**Advice from Survey Takers**

*Knowing what assets you have is half the battle. Integrating the software tools is important.*

*Integration is much required now-a-days. It improves the efficiency of the IR team. I would strongly recommend my peers look for opportunities to integrate and automate.*

*Hire a developer guru who understands security and can code to integrate the numerous tools/feeds.*

*More automation for detection and response is needed. There is a great need to separate business and personal, such as assigning passwords that are for the business functions and separation of duties.*
Vendors on the Hook

In a write-in question, we asked responders what they need from vendors to improve efficiency/integration of security, threat, prevention and risk information, as well as team functionality. Responses varied, but can be summarized in a few categories:

- Use of vendor-neutral standards, such as STIX™ and TAXII™, rather than APIs, for tool integration
- Increased ability to tailor specific solutions to business needs, while allowing tool integration for data exchange and process automation
- Increased vendor sensitivity to business processes rather than tool capabilities
- Lowered barriers to entry (i.e., cost)

Some of these may be mutually exclusive in the general case, and we will see organizations choose combinations appropriate for their environment, just as they combine automated and manual approaches for data handling and incident response.
Conclusion and Looking Ahead

Just as 64% feel the lack of integration and automation is affecting their detection and response capabilities, 63% of respondents feel that removing the barriers and integrating functionality, resources and data would greatly improve their accuracy and time investments across their prevention, detection, response and remediation functions. An additional 23% see some value (these are organizations that feel they already have the visibility they need with their partially automated systems), and only 4% feel there is no value in integration and automation.

Based on survey responses, the real key to success is high-level management buy-in, regardless of tools or process. Security, and its optimization, affects the entire organization, and cannot be accomplished by multiple separate groups that don’t interact with each other. Organizations need to move toward a more unified security strategy that leverages centralized data through a documented system and shared knowledge and processes across teams and tools.

Leadership and vision must come from a common source. Once that’s in place, organizations can begin to align the goals of each security function. Then, when goals have been aligned, they can use teams, processes and tools to automate and further integrate.
G.W. Ray Davidson, PhD, is the former dean of academic affairs for the SANS Technology Institute. He continues to serve as a mentor, subject matter expert and technical reviewer for the SANS Institute and holds several GIAC certifications. Ray started his career as a research scientist and subsequently led global security projects for a major pharmaceutical company. He has taught at the college level and co-founded a security startup. Ray currently works with clients to develop and implement network security monitoring and threat intelligence capabilities. He is also active in the leadership of the Michigan Cyber Civilian Corps.

Barbara Filkins (advisor), a senior SANS analyst who holds the CISSP and SANS GSEC (Gold), GCIH (Gold), GSOC (Gold), G越高 (Gold), GCPM (Silver) and GLEG (Gold) certifications, has done extensive work in system procurement, vendor selection and vendor negotiations as a systems engineering and infrastructure design consultant. She is deeply involved with HIPAA security issues in the health and human services industry, with clients ranging from federal agencies (Department of Defense and Department of Veterans Affairs) to municipalities and commercial businesses. Barbara focuses on issues related to automation—privacy, identity theft and exposure to fraud, as well as the legal aspects of enforcing information security in today’s mobile and cloud environments.

SANS would like to thank this survey’s sponsor:
<table>
<thead>
<tr>
<th>SANS Essentials Australia 2021</th>
<th>Melbourne, AU</th>
<th>Feb 15, 2021 - Feb 20, 2021</th>
<th>Live Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS OnDemand</td>
<td>OnlineUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
<tr>
<td>SANS SelfStudy</td>
<td>Books &amp; MP3s OnlyUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>