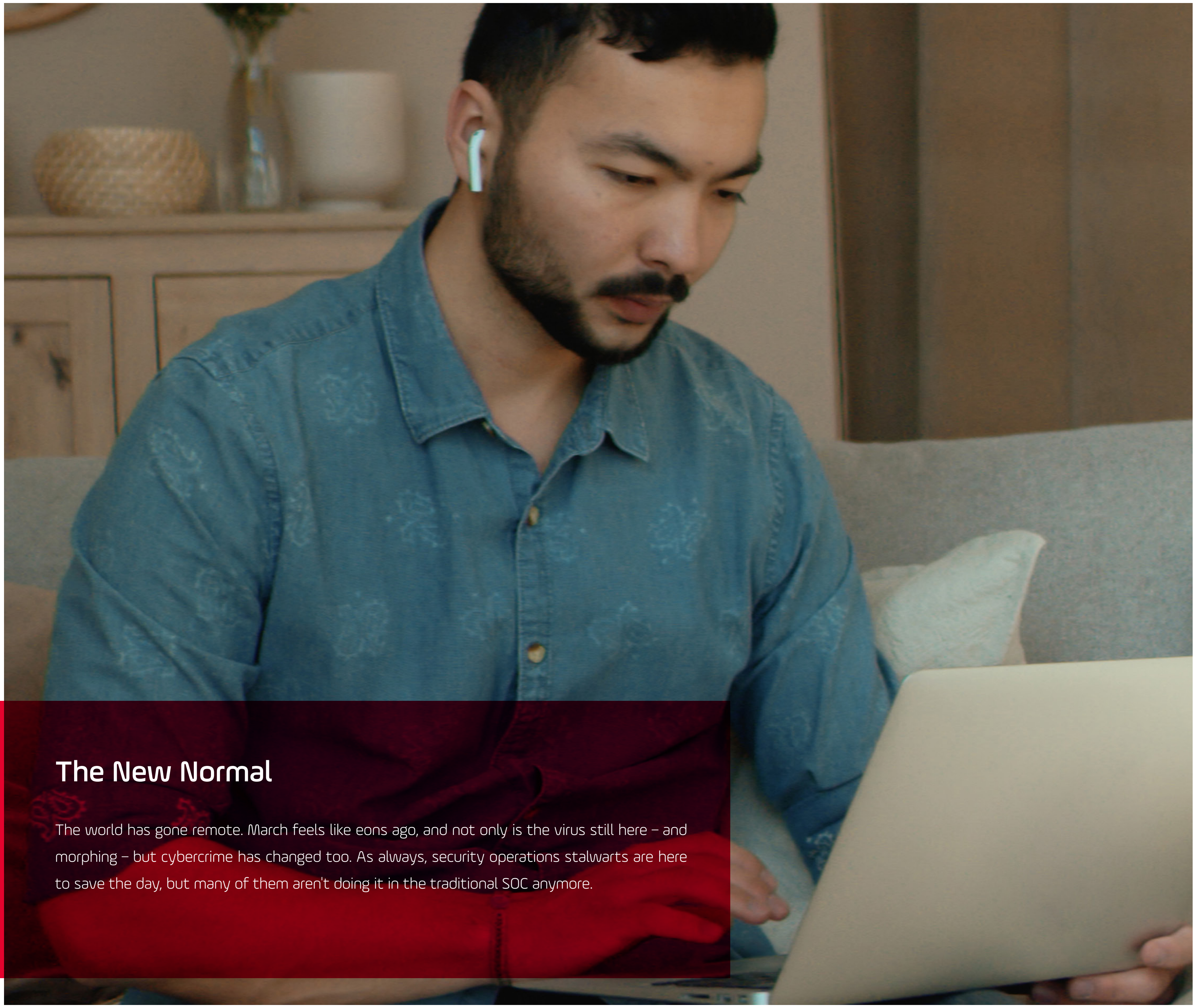
Siemplify

The State of Remote Security Operations

A First-of-Its-Kind Study
Into the Threat and Occupational Impact
of COVID-19 for SecOps Professionals

SURVEY

The State of Remote Security Operations



The New Normal

The world has gone remote. March feels like eons ago, and not only is the virus still here – and morphing – but cybercrime has changed too. As always, security operations stalwarts are here to save the day, but many of them aren't doing it in the traditional SOC anymore.

Survey Index

Introduction

Welcome to the State of Remote Security Operations, a survey report that, at this time last year, we could never have imagined compiling and publishing,

not even amid a backdrop as unpredictable and variable as the cybersecurity landscape. Yet here we are – one disruptive, grueling and life-changing 2020 later – sharing insights around the experiences security operations professionals across the globe have endured thanks to once-in-a-century health crisis and the ensuing home confinement policies, which have collectively changed – perhaps permanently – the way we work.

Security operations is the linchpin to any successful infosec program. In the average organization, its members are charged with detecting and responding to tens of thousands alerts and events per day, from basic phishing ruses all the way to advanced persistent threats. Those are breathtaking numbers, as are the minutes spent daily working false positives, which is why a cooperative, centralized and optimized effort has long been required to perform security operations most effectively. This mission has traditionally been best incarnated by the physical gathering space we all know as the security operations center (SOC). But then 2020 reared its ugly head and decided it wanted nothing to do with human proximity, and suddenly all bets were off, even as the same digital risks still existed and new impediments emerged.

Our report, of course, examines the consequences of these growing threats and budding challenges facing the security operations practitioner. But, arguably more importantly, it also considers the overall psyche of the security operations professional. Remember, even before COVID-19 was a household word, these women and men were toiling in roles well steeped in the tumult and unremitting demands of the digital transformation era. Has the new remote normal fatigued them further? And what are their expectations (and preferences) about returning onsite?

You can probably deduce by now that saccharine this report is not. But it is not doom and gloom either. As you will discover, many security operations teams have ridden the COVID-19 learning curve to successfully adjust, adapt and even revitalize their infosec functions in varying ways, from adopting new security technologies to introducing automation efforts to enlisting outside help. And, for some, the flexibility of remote SecOps has enabled increased productivity while reducing the stress of the daily commuting grind.

We have distilled the report into three parts: 1) the security impact, which will consider COVID's effect on elements like posture, alerts and threats 2) the human impact, which will examine the feelings and desires of SOC professionals and 3) the "path forward," which will study what security operations teams are doing to accommodate (and still thrive) in these trying times.

Some of the questions we asked seemed to demand more than just a multiple-choice response, so survey takers in those cases were able to elaborate on their feelings. This allowed us to share some of the more notable and earnest comments we received, which lends important context, as everyone's work plight during COVID-19 has been unique.

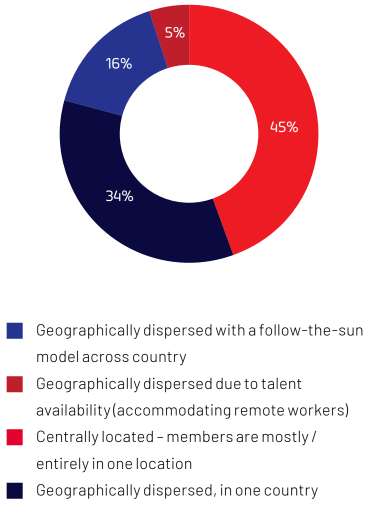
So here you have it, a report we believe is as relevant as ever, if for no reason than to help project much-needed awareness on what security operations workers face moving forward. We hope the research finds you as well as you can be given these unusual times, presents a clearer picture of the current state of affairs you are confronting, and, empowers you to either make the most of this unexpected period in your career or prepare for the continuing pivot that awaits. Please enjoy!

Methodology

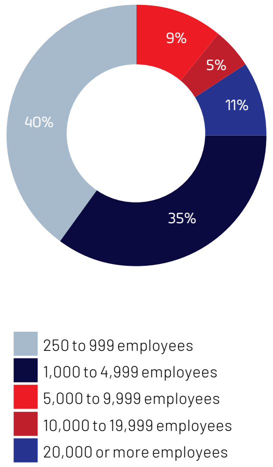
Siemplify commissioned a third-party research firm to survey 393 cybersecurity operations professionals. The objective of the survey was to measure and assess the impact of COVID-19 and the subsequent work-from-home imperatives on their ability to perform security operations. Respondents consisted mainly of managers or directors overseeing a cybersecurity function, security analysts, security architects and security engineers. Respondents work in a variety of sectors, with the most frequent being technology, manufacturing, business and customer services, finance, retail, health care, government and education. Respondents work at organizations that employ an average of 1,095 people. The survey was deployed through emails sent in late 2020. Survey results have a margin of error of 3.9%.

Job Profile

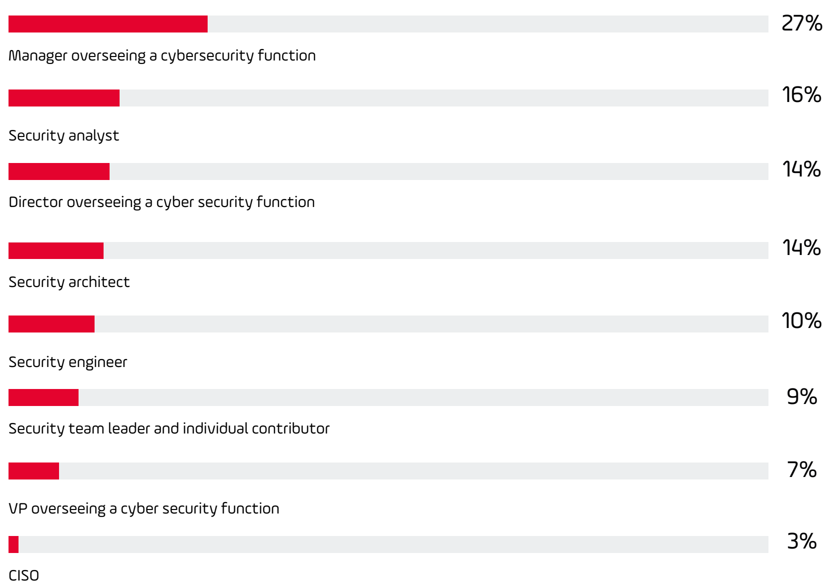
How was your SecOps team situated geographically prior to COVID-19?



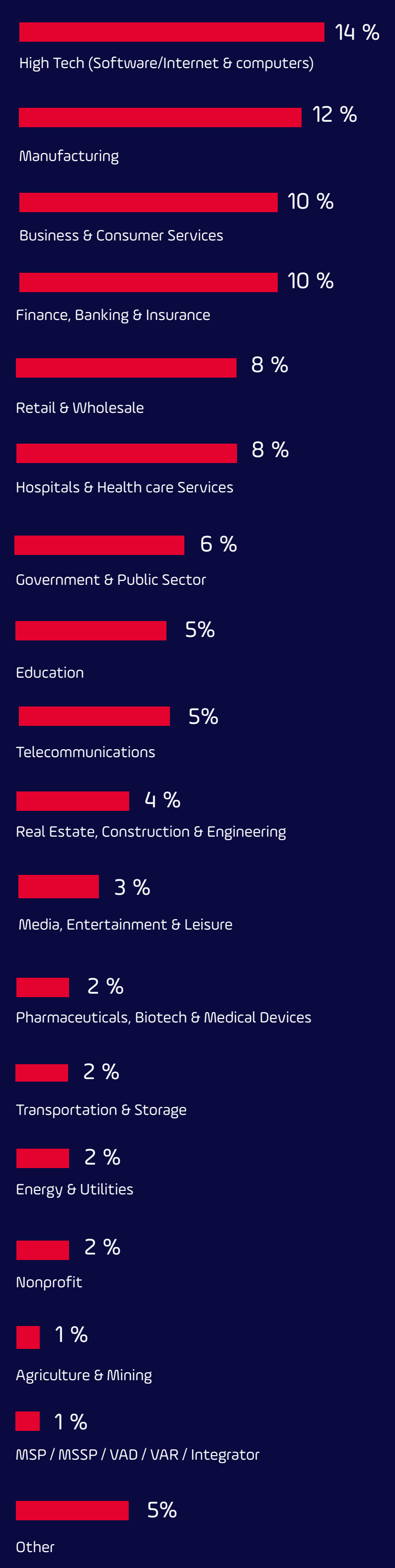
What is your company size?



Job Role



Industry



Key Findings

26% of respondents believe their security posture is "somewhat worse" or "significantly worse" since COVID-19 began. Meanwhile, 27% report that their security postures have actually improved.

42% of respondents said their alert volume is "much or somewhat higher" compared to pre-COVID-19.

The survey asked about specific threats – phishing, network intrusions, malware, vulnerabilities, data leaks, etc. – and the overwhelming number of respondents reported that incidents of phishing have increased. Surprisingly, in light of increased cloud adoption and shadow IT, fewer than a quarter reported seeing more data leaks.

Respondents reported insecure home networks and cloud as the top two remote security risks they have experienced, rounded out by VPN/RDP vulnerabilities, device management and IAM vulnerabilities.

Fifteen percent of respondents expect their transition back to on-site security operations will take a year or later, and 11% expect to never return to on-premises security operations.

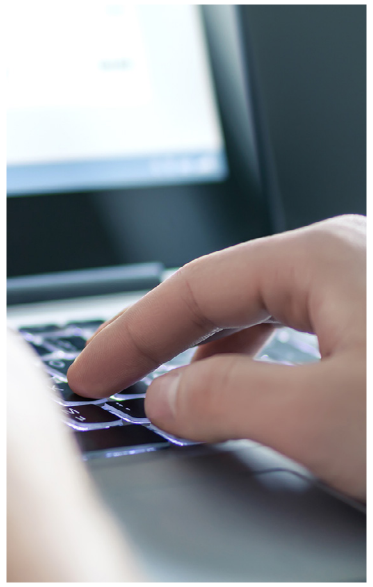
Of all the primary security operations duties, investigating suspicious activities has become the most challenging since going remote.

Twenty percent of respondents have enacted or are considering security operations-related cost cutting measures, while 25% are looking at increasing their SecOps budgets.

Morale is also divided: 30% of respondents said their job morale has been reduced to some degree, but 39% said it is "greatly" or "somewhat" improved. The split seems to be a competing effect of WFH convenience versus pandemic-induced stress and other challenges.

More than three-quarters of respondents have increased automation efforts, and 37% have prepared new automated playbooks to respond to emerging remote-specific threats.

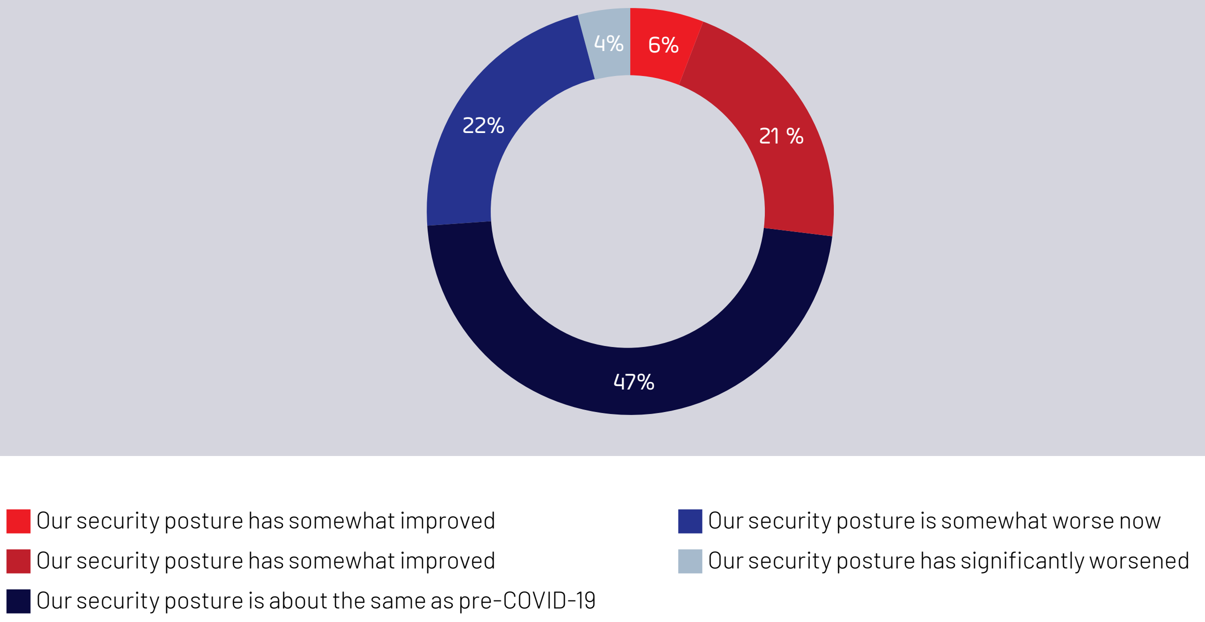
Just over half of respondents said their use of MSSPs is increasing as a result of remote shifts.



42% of respondents said their alert volume is "much or somewhat higher" compared to pre-COVID-19.

Part 1:
The Threat Impact

How would you rate COVID-19's impact on your security posture?



The upheaval happened in days. The shift to remote work was sudden and was initially met by most as a temporary break of the daily routine. In short order, however, the outcome grew more bleak, and reality set in that things might not get back to normal for quite a while. For many security operations teams, that meant not only fleeing the SOC to their home offices but also encountering new risks brought on by a newly minted remote fleet of workers.

As a result, 26% of respondents reported that their security posture is "somewhat worse" or "significantly worse" since COVID-19 began. Many attributed the erosion of resilience to the obvious: an unexpected expansion of the corporate network via unmanaged endpoints connecting to the network, an infusion of unprotected cloud applications and the increasing risk of lost or stolen devices. Here is a sampling of responses:

"Increased attack surface with remote working."

"So many devices connecting from foreign networks."

"Pre-COVID, most of our work was from our office, which gave more visibility to the SecOps team. With work from home, much of that traffic goes straight to the cloud and bypasses our monitoring."

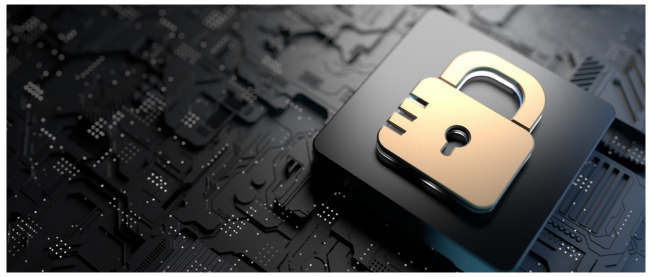
"The amount of remote workers doubled. This could lead to a possible loss of equipment or data from remote locations."

However, what began as playing catchup and performing classic blocking and tackling, security operations teams gradually acquired more data and were able to better determine where their biggest weaknesses lied (misconfigurations, elevated privileges, unusual traffic patterns, data exfiltration, cloud worries, etc.), eventually yielding some level of stability. Forward-thinking organizations used the moment as an opportunity to invest in greater security controls and awareness training efforts. This likely explains why 47% of respondents stated their security posture is roughly the same as before COVID, and 27% reported it has even improved. The latter group shared some additional background:

"We had to adapt to changing situations which allowed us to be more secure as a result."

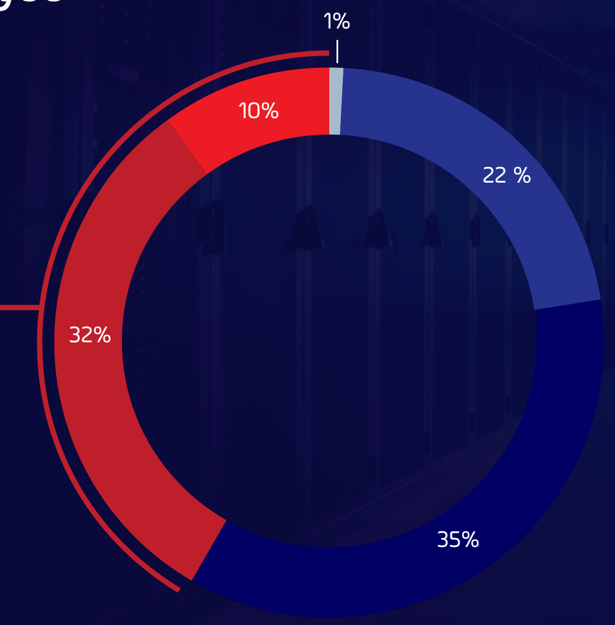
"We implemented more tools, formalized processes and outsourced some functions."

"We increased our security measures through implementation of MFA, VPN and endpoint security usage."



Security events

Compared to pre-COVID-19, how would you characterize alert volume?



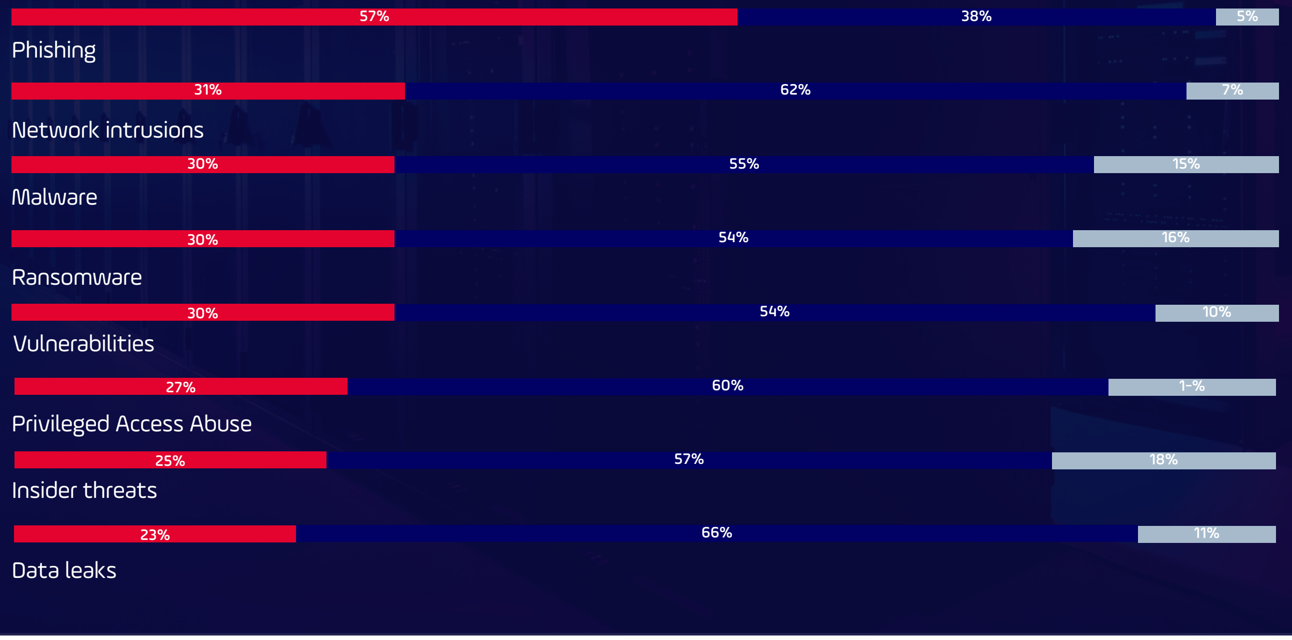
42% Much or Somewhat Higher

Arguably the most pressing challenge needing to be solved by today's modern security operations center is the unceasing inundation of alerts that are driven by an ever-broadening attack surface and stem from the implementation of disparate tools which, in turn, fire off more alerts than depleted resources are able to handle. Then, there is the challenge of sorting through false positives and applying context to the legitimate alerts – and what results can range from analyst fatigue to missing something big.

When it rains, it pours – and 2020 brough the monsoon. Indeed, the unceasing stream of the alert fire hose has grown even more pronounced with the shift to remote work, with 42% of respondents reporting "somewhat" or "much" higher alert volume in the COVID era, compared to 23% whose alert volume has fallen. The remaining pool of respondents (35%) reported conditions remained roughly the same.

Meanwhile, roughly one-third of respondents reported seeing more each of network intrusions, malware, ransomware and vulnerabilities, with about a quarter of respondents saying they experienced more privileged , insider threats and data leaks.

Please indicate if you are seeing more, less or about the same of these security alerts and events?



When the world shifted to remote work, cybercriminals did not need to suddenly invent or reimagine their ploys, methods and tactics. There was no need to as the tried-and-true stuff is just as reliable, especially when it involves a work-from-home crowd. As told in the previous finding, security alerts and events have increased across the board in the COVID era, with respondents reporting that spikes have outgained slowdowns for every type of threat on which they were queried.

Impressively, incidents of phishing have increased for 57% of respondents, topping the list. Even before a pandemic was gripping the world, email-based chicanery was already the most prolific part of an attacker's playbook, so the findings here are telling of how much of it is currently going on. For malicious senders, realistic-looking messages designed to hoodwink the unsuspecting and induce reckless behavior are a relatively low-cost lift that can yield great gains. COVID obviously has presented the perfect bait, as an unfamiliar and anxiety-ridden event can easily inspire bad decisions.

Meanwhile, roughly one-third of respondents reported seeing an increase of network intrusions, malware, ransomware and vulnerabilities, with about a quarter of respondents saying they are experiencing more privileged access abuse, insider threats and data leaks.

Speaking of emergent threats brought on by working from home, respondents rated insecure home networks (47%) and cloud (46%) as their two biggest remote-specific digital risks, followed by VPN/RDP vulnerabilities (39%), device management (35%) and identify and access management (IAM) vulnerabilities (33%).

Recent research from cyber risk management firm BitSight determined that home networks were 3.5 times likelier than corporate networks to contain at least one malware family – and 7.5 times likelier to have five or more distinct types of malware. Meanwhile, cloud applications and services have helped to smooth the transition to remote work by making it easy for employees to access corporate resources and remain productive. Of course, a rush to adopt these services without instituting due diligence and proper controls can correlate with the higher risk of data exfiltration and malware infections.

Of these options, choose your top two remote-specific security risks.

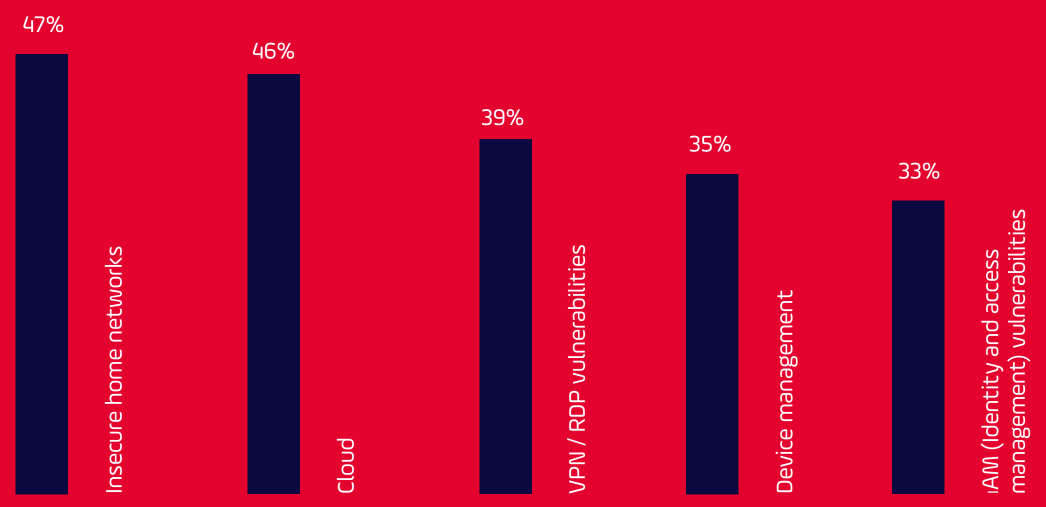
47%

Insecure home networks

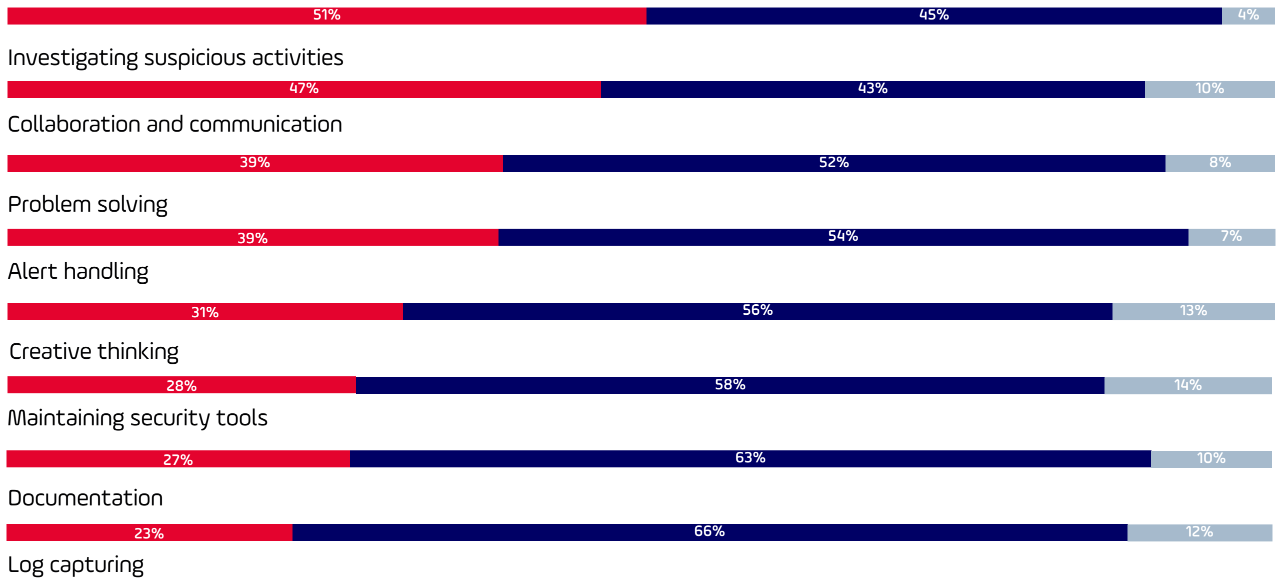
46%

Cloud

Remote-Specific Security Risks



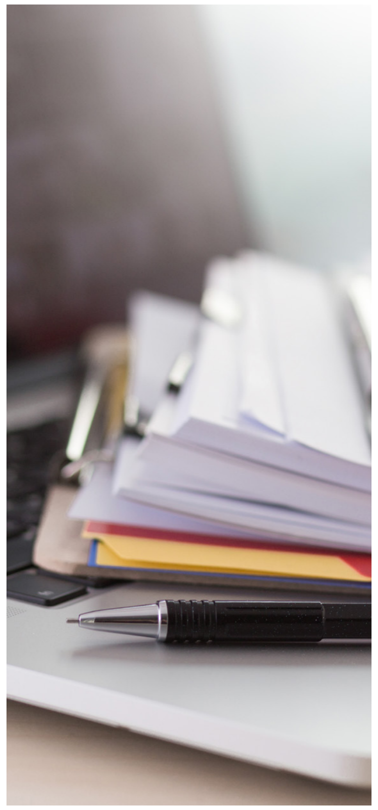
Have the following become more challenging, less challenging or stayed the same since going remote?



Common security operations duties of both the soft and hard variety grew more challenging, not less, for every SOC function respondents were queried on. Most noteworthy – but unsurprising – was "investigating suspicious activities" becoming more challenging for 51% of respondents, likely dealing with the rigors of balancing the secure management of remote infrastructure and users with the corporate demand to get them to pre-COVID production levels.

Collaboration & communication and problem solving naturally also suffered, with 47% and 39% of respondents, respectively, reporting these tasks to be more challenging. One of the greatest luxuries of an onsite SOC setup is that staff members can tap on a colleague's shoulder and huddle around monitors to brainstorm on a particular incident. With that luxury now gone, respondents were forced to seek that same intimacy, idea exchange and decision making instead via remote tools like Zoom. Fortunately, certain security operations-specific platforms, like SOAR (security orchestration, automation and response) can support and foster interaction among decentralized and dispersed teams.

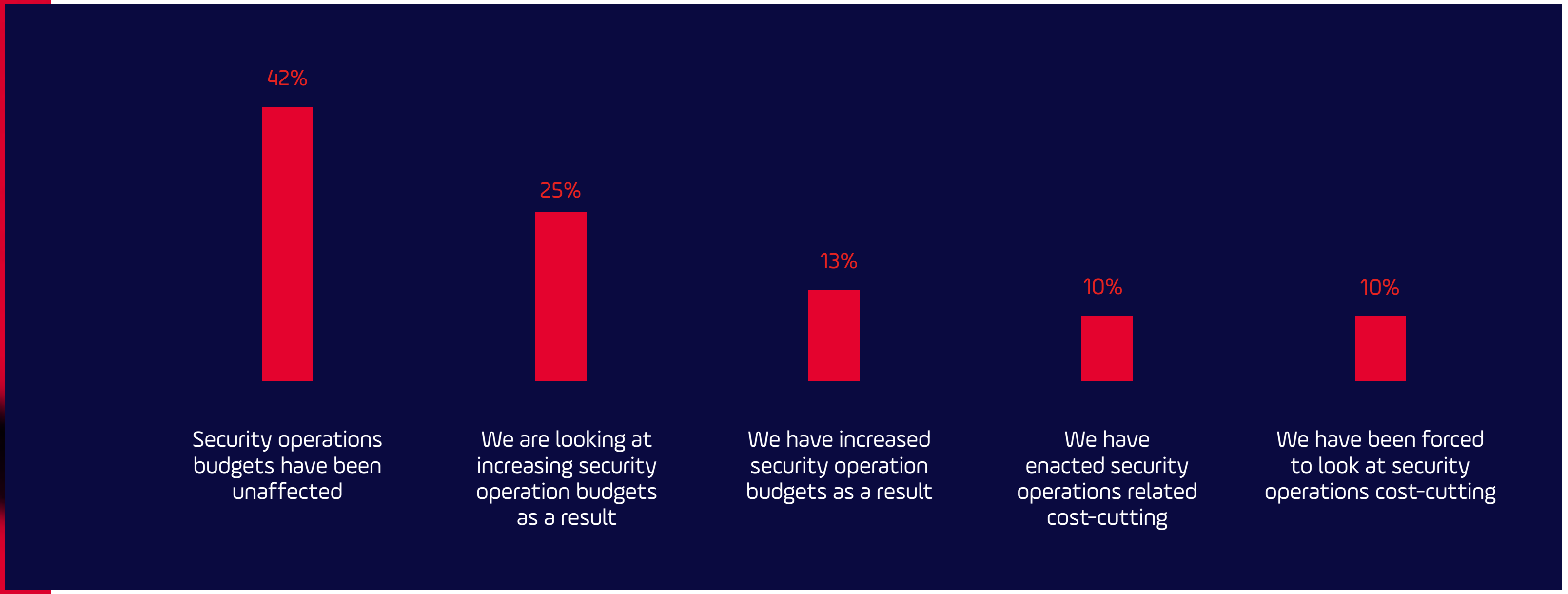
Meanwhile, further down the list, the challenges posed by documentation and log capturing remained largely unchanged for a majority of respondents. It stands to reason that these tasks have been largely solved by technology and require less human connection to perform successfully.



Budget

Enterprise goals are firmly aligned with the need for workers to be productive. When the pandemic took hold, and employees were forced to retreat to their home offices, the IT and security teams were pivotal in getting workers up and running and enabling organizations to remain open and operational – and the smartest organizations took notice. Now, as digitization across businesses only accelerates because of COVID-19, those properties will need further protection.

How has your security operations budget been affected by COVID-19?



Despite the rough economic climate, there are hopeful signs that security will emerge even stronger. While big SecOps projects likely were put on hold during the uncertainty of the months following the start of the pandemic, evolving corporate attitudes around risk and the ability for security to support remote workforce productivity mean budgets are likely to be at least partially sheltered from any serious reduction.

Indeed, 38% of respondents have either increased or are considering increasing their security operations budgets because of the impact of COVID-19. Another 42% report their spending plans have gone unaffected, and just 20% have either been forced to make or contemplate making cuts to their security operations outlay.

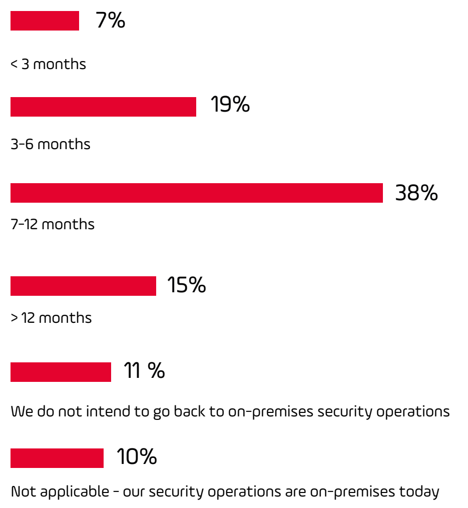
38% percent of respondents have either increased or are considering increasing their security operations budgets

Part 2: The People Impact

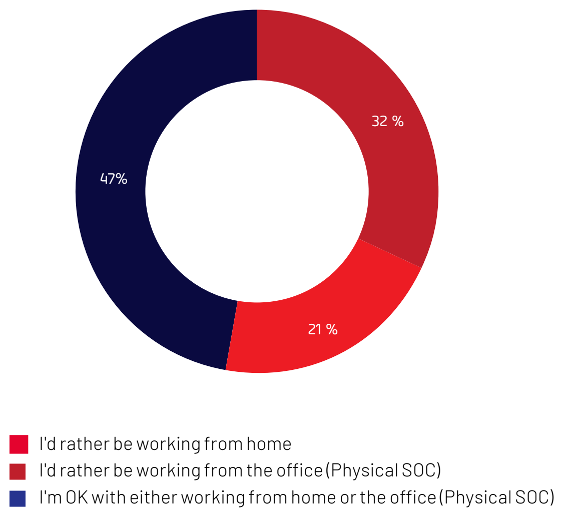
Current Working Location & Location Preference

After-COVID plans

What is your best estimate of when most, or all, of your SecOps team will transition back to a physical SOC?



What is your current preference for where you want to work?



For decades, the security operations center has served as the physical nerve center for threat detection and response. It is characterized in its classic sense by rows of multi-monitor consoles with optimal sightlines; contrast lighting that supports a combination of focus, energy and – especially for customer tours – drama (often, SOCs bring in little to no natural light); and acoustics to control ambient noises. The goal of all of this is to maximize comfort, concentration and productivity in a space where critical stakes are on the line.

While not all organizations are equipped with movie set-like command hubs, few white-collar professions have such a unique work setting. But COVID-19, like it has done for so many aspects of our normal, upended the traditional SOC model and ushered in the Zoom era.

So for how long will these mission controls – which bore huge expenses to build – go unoccupied? Just over a quarter of respondents expect to return to on-premises security operations in the next six months, with 53% expecting it to take seven months or longer. Roughly one out of 10 expect to never return to an onsite SOC. Another 10% remain working on prem. And even when, and if, staff does return, social distancing and hygiene will need to be considered in a way they never were before.

Yet while the amenities offered by a physical SOC – not to mention the convenience of in-person interaction – are unmatched via video conferencing in a home environment, close to one out of five respondents prefer remote work, and another 47% are content with either arrangement: remote or onsite. Still, nearly one-third of respondents prefer being in the office.

Some respondents elaborated on this question with written comments, which heavily leaned toward the work-life balance benefits of remote work. One person even noted that other than for a major cyber emergency, they are just as effective at home than in the physical SOC. Here is a sampling of responses:

> "Working from home gives me instant access to my suite of tools. Unless there is a physical intrusion, I do everything remotely regardless of being in the office or being at home."

> "The commute is 45 seconds instead of 45 minutes. Other than that, I can do everything I need from the home office."

> "I prefer working at the office to work in person with people...IT is just better in person."

> "I enjoy working from home because I get much more done. A lot less distractions."

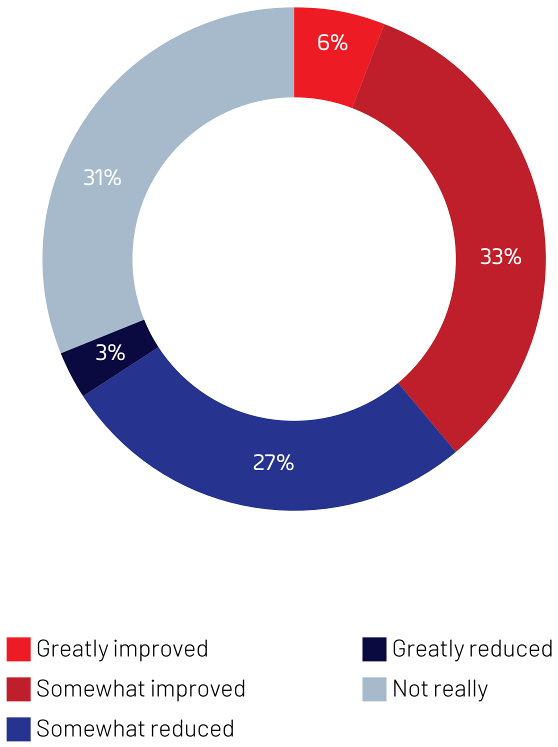
Job Morale

39% Greatly or Somewhat Improved

The COVID pandemic and subsequent lockdowns have taken a toll on our mental health and emotional well-being. For employees, mood and motivation have suffered, especially as they adjusted to remote life. But despite the tumultuous year, remote workers overall have reported increased workforce satisfaction compared to those who must show up at the office, which makes sense given the peace of mind that being able to stay put, while still earning a paycheck, brings.

The security operations industry is no stranger to burnout risk, yet practitioners also seem to be finding contentment in working from home. In fact, 39% of respondents reported their morale has "greatly" or "somewhat" improved, compared to 30% who said it has "greatly" or "somewhat" reduced. Another 31% of respondents cited little to no change in their morale.

How has COVID-19 affected your job morale?



Hiring

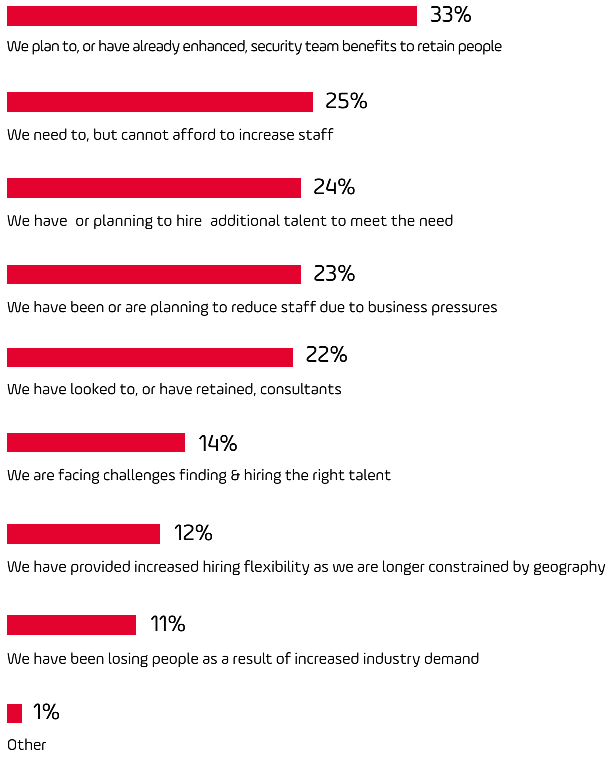
People, at the end of the day, are the beating heart of any security operations effort. And while automation (which this report will discuss in Part 3) has arrived on the scene to act as a force multiplier in the SOC, human help remains critical, especially for advanced cognitive tasks like threat hunting and incident response.

In other words, people will be a part of the SOC for a long time to come. The news was mixed, however, how the disruption of the pandemic will impact hiring and the ability to attract and preserve skilled personnel. (This question allowed respondents to select all options that applied to them, hence the percentages adding to above 100%.)

"In a positive sign, 33% of respondents are planning to or already have enhanced benefits to retain staff, while 25% need to but cannot afford to increase staff and 23% are planning to cut staff due to business pressures.

A possible silver lining, although admittedly still a work in progress, is that 12% of respondents, formerly hampered by geographical divides, expect to use the new remote norm to acquire skilled staff regardless of their location.

How has your SecOps staffing been affected by COVID-19?



Part 3:

The Path Forward & Conclusion

Collaboration & Communication

Collaboration and communication are key pillars by which organizations can reduce arguably their most important security metric: detection and response time. But teamwork and camaraderie can be eroded when security operations personnel move out of a central physical setting and into remote locales.

Earlier, we shared findings showing that respondents in general are being increasingly challenged around their team's ability to effectively collaborate and communicate. For those who are finding heightening difficulties, we queried them to share more, specifically asking: *What do you think would improve collaboration and communication among the SecOps team and relevant stakeholders?* Here are some of the more colorful responses. As you can see, the suggestions varied from functional to technical, although in some cases, respondents just weren't sure how to improve on this front.

What do you think would improve collaboration and communication among the SecOps team and relevant stakeholders?

"More graphics demonstrating log findings, configuration issues and architectural best practices would be helpful. Video conferencing works well, but people get bored with it quickly."

"We are already using Microsoft Teams. I can't think of anything more."

"I think automating system alerts would be most important."

"Nothing more can be done. Tools are now available and policies have caught up to the pandemic response."

"Having a SOAR and case management solution."

"Have teams work together and respect each other, especially when they have different backgrounds."

"We were WFH and distributed even prior to COVID, so no real impact for us."

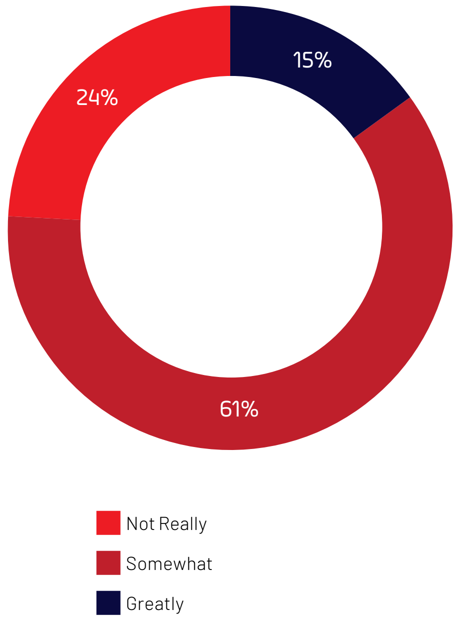
"No specific ideas. Collaboration is just a little simpler and easier when everyone is in one location together."

"Fewer overall meetings. What was a quick five-minute conversation at someone's desk has turned into 30-to-60 minute virtual meetings, making it difficult to get time to have quick conversations with people."

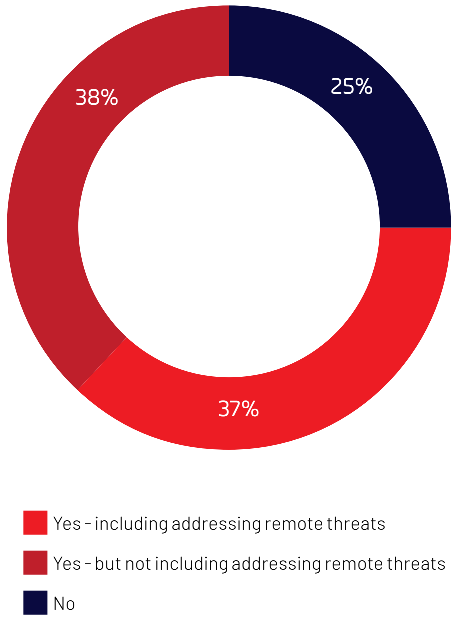
"Nothing more can be done. Tools are now available, and policies have caught up to the pandemic response."

COVID-19 Impact on
SecOps Automation and Creation of Automated Playbooks

Have you increased your use of security operations automation during COVID-19?



For those who selected "somewhat" or "greatly in the previous question: Have you prepared any new automated workflows or playbooks as a result?



Dating back to Henry Ford's assembly line, automation historically has been relied upon across industries. As long as there is a desire to perform routine and redundant tasks faster, automation will thrive.

A key capability of SOAR technology is automation, which can drive efficiency within the SOC by streamlining repetitive and manual tasks involved with investigating and mitigating threats, from data gathering to log enrichment to lessons learned. The question, then, is not if businesses – and security departments – are relying on automation (of course they are) but how their use of automation is changing amid the COVID era.

Indeed, 76% of respondents said the pandemic and ensuing WFH boom has contributed to increasing efforts around automation, while 24% disagreed.

SecOps professionals have faced new risks amid a culture that is emphasizing speed over security in workplaces preparing for a long-term remote situation. Creativity has been critical here as security staff is forced to quickly adapt and react to new challenges, but many of the most maddening threats analysts are encountering are just new takes on old problems.

From VPN and RDP issues to unmanaged mobile device usage to insecure home networks, security operations teams have experienced, as this report showed earlier, a surge in alerts. As a result, 37% of respondents have stepped up their automation as a result of the COVID impact by implementing new workflows addressing remote-related threats.

Managed Security

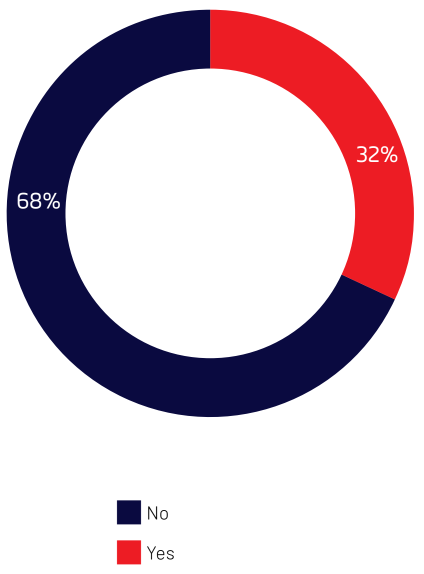
Managed security has been flourishing for years, with organizations of all sizes coming to grips with their limitations, including in-house security skills shortages, a widening attack surface needing coverage and a desire for more visibility into their environment.

When COVID-19 struck, most businesses pivoted to remote work, which, not surprisingly, accentuated a new set of security challenges, from coronavirus-themed phishing attacks to remote access weaknesses to data leakage risks spurred on by increased cloud adoption. And even as these new deficiencies rose to the forefront, organizations still were operating with many of the same limitations as before the health crisis, only fortifying the need to call on outside help.

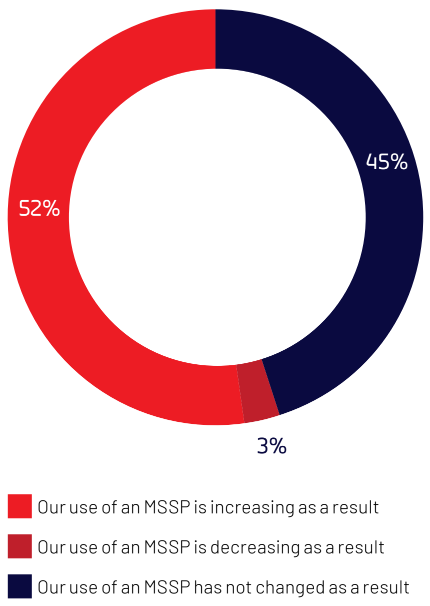
For those respondents who confirmed they are currently using (or plan to use in the near future) an MSSP for any aspect of their security operations, 52% reported they have increased those relationships as a result of COVID-19, with only 3% declaring a decrease in MSSP usage.

Of the security operations disciplines that respondents are most commonly delegating to managed security providers, security monitoring led the way for 77% of them, with incident response (66%) and threat hunting (49%) following. The modern MSSP, meanwhile, must respond to this increasing market demand with strong offerings and appreciation for the customer's individual needs, as this e-book showcases.

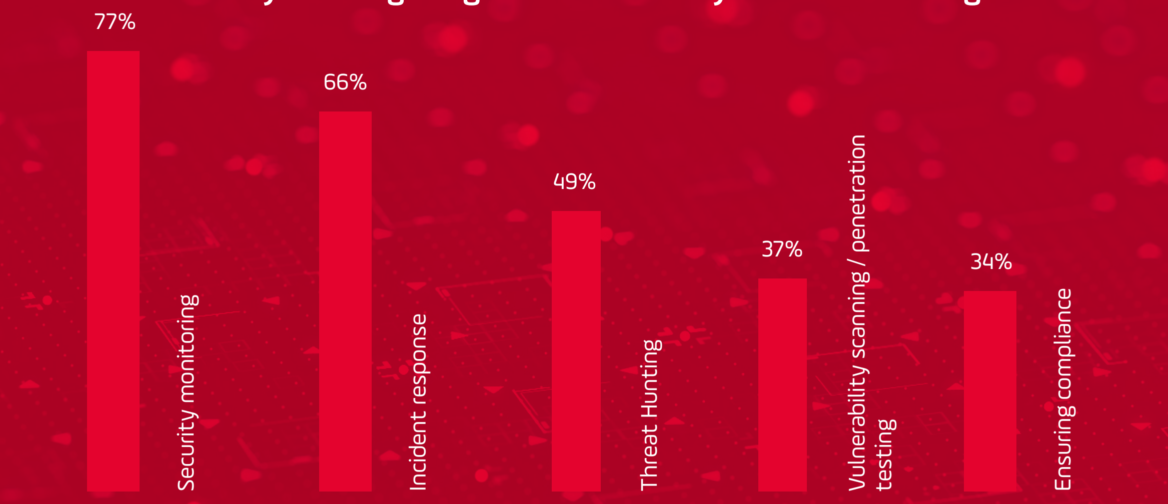
Do you use an MSSP?



For those who selected "yes" the previous question: Have you increased your use of an MSSP during COVID-19?



Which tasks are you delegating most commonly to MSSPs during COVID-19?



(Respondents were able to select multiple options, which is why percentages add to greater than 100%)

Conclusion: The Courage to Soar and Overcome

"All the adversity I've had in my life, all my troubles and obstacles, have strengthened me. You may not realize it when it happens, but a kick in the teeth may be the best thing in the world for you." — Walt Disney

Talk about a kick in the teeth. The COVID-19 era is far from over, and, truth be told, there is no silver lining to a health crisis that has killed tens of millions and forever scarred the lives of countless more. Still, human beings have a miraculous ability to adapt to even the most stressful and uncertain of events.

Within our little world of security operations, the ability to adapt was tested in dramatic ways by the new remote normal. The chaos and fog of the early work-from-home days are now far in the rear-view mirror. While a smorgasbord of challenges persist, as our survey attests, a vast majority of companies have either stabilized their security stances or advanced them even beyond pre-pandemic standards.

COVID-19 underscored the need to react quickly and ingrain stronger controls to cover previously ignored – or insufficiently served – blind spots, and technologies like security automation and orchestration (SOAR) have helped SecOps teams hurdle these obstacles, enabling them to do everything from analyst onboarding and knowledge capture to playbook building and analyst collaboration (not just among internal teammates but with external security services providers as well.)

"Remember **diamonds** are created under **pressure**, so hold on, it will be your time to shine soon."

— Sope Agbelusi

The resilience of security operations professionals is now on full display. While stressors like burnout and hiring issues remain pressing problems within the industry, and insider threats and cybercriminals show no signs of slowing down, SOC staff will persevere. If not now, soon.

Written by Dan Kaplan

Siemplify

About Siemplify

Siemplify is a security orchestration, automation and response (SOAR) provider that is redefining security operations for enterprises and MSSPs worldwide. Its holistic security operations platform is a simple, centralized workbench that enables security teams to better investigate, analyze, and remediate threats. And, using automated, repeatable processes and enhanced measurement of KPIs, Siemplify empowers SOC teams to create a culture of continuous improvement. Siemplify's patented context-driven approach reduces caseload and complexity for security analysts, resulting in greater efficiency and faster response times. Founded by Israeli Defense Forces security operations experts with extensive experience running and training numerous SOCs worldwide, Siemplify is headquartered in New York with offices in Tel Aviv.

siemplify.co