A new breed of distributed employees is raising challenges for infosec teams around the globe, just as SecOps professionals are adjusting themselves to finding success in work-from-home environments.

I. The Coronavirus Curveball

For many of us, it happened swiftly and suddenly. A once-in-a-century pandemic, which began as someone else’s problem, surged across the globe, and during what felt like overnight, our daily lives changed for the foreseeable—and an uncertain—future.

Aside from the mental adjustment required to endure such an abrupt shift in our conventions, the modern workplace also changed in flash, with millions of office workers instantly becoming remote employees. Among those feeling the most drastic reshuffling of their daily routine are security operations professionals, many of whom are accustomed to performing their duties of threat handling inside the four walls of a physical, dedicated SOC with face-to-face conversations and group huddles an essential part of the dynamic.

While the environment of a physical SOC may not make the list of most vibrant places in which to work, it is purposely designed for functionality, comfort and collaboration. And there is no shortage of technological infrastructure needed to support analysts and engineers in their role of preventing, detecting, assessing and remediating threats. The setup ranges from perimeter staples like firewalls and IPS/IDS to SIEM/EDR/DLP and network monitoring/analysis to threat intelligence and vulnerability scanners.

Even as workers shift to remote settings, those same protections and monitoring capabilities should continue to function normally, and properly implemented VPNs (which this paper covers later) allow SOC personnel to securely access critical network resources from home. Not as certain, however, is the team’s ability to ensure workflows go unimpeded. This involves components such as ticketing, task and case management, investigation notes, shift handovers and more.

The typical physical SOC is ergonomically designed and features key elements that help keep productivity and engagement intact, including large video walls, audio-visual integration, console furniture and modular workstations featuring multiple monitors. None of these comforts will be available in your home seclusion, and you’ll have to spend time perfecting your workspace.
Yet SecOps teams must persist in the face of the usual challenges – alert deluge, overreliance on manual tasks, disjointed security tools and that pesky skills shortage – as well the newfound impediments presented by a decentralized workforce.

Indeed, remote work can introduce widespread havoc to the normal functioning of your infosec program. This white paper seeks to smooth out the learning curve involved with enabling a secure remote workforce while instituting a highly functioning SOC. It offers:

A rundown of security threats that will be compounded by mobile working.

Guidance for secure connectivity/VPN usage + video conferencing.

Tips for getting a remote SOC off the ground and efficiently automating & orchestrating.

Best practices for empowering team collaboration, communication and well-being.

It is still too early to know whether this “temporary” migration to remote security operations will usher in a paradigm shift. But one thing is certain: We could be in this for the long haul, so staying educated about how to best execute the transition will hopefully prove valuable.

Might as well enjoy the ride ... and the read below!
II. Common WFH Security Risks

First, let’s start with how you’re feeling: Fully adapting to a work-from-home lifestyle will vary for everyone. Some may adapt quickly. For others, the perils will overshadow any perks. Do not panic! Try to organize yourself from the very beginning and your adjustment period will go away in no time (if it hasn’t already by the time you’re reading this paper). Copious resources exist online outlining tips and tricks for mastering working from home (from maintaining as normal a schedule as possible to setting boundaries to taking breaks), but arguably most pertinent to security operations professionals will be ensuring their workstation resembles their office setup as much as possible. This includes a functional desk with proper sightlines, necessary equipment, connection speed/bandwidth, secure connectivity, and collaboration functionality.

Now that you’re comfortable and assimilating as much as possible, it is time to concentrate on the common threats your remote workforce is facing. These digital risks are not foreign to you, but will be exacerbated by the circumstances. Here is a good summary of what organizations like yours may be experiencing.

For starters, you’ll want to ensure security awareness remains vibrant, and now is as good a time as any to drop a refresher course around best practices.

Your security awareness reminders should include:

- Avoiding using personal computers for work purposes. You can accomplish this by enforcing acceptable-use policies across the entire company. Remember, global quarantine increases the timeframe to re-image or replace affected corporate assets, which leads to a higher risk of employees using some of their own devices to accomplish essential business needs.
- Locking devices when employees step away from them. In addition, all corporate mobile devices should have an MDM product that ensures adequate security controls, including encryption and segmentation of corporate data.
- Making sure their computer is updated with the latest patches and security controls.
- Avoiding clicking links and attachments contained in unsolicited emails.
- Using passwords for all devices and ensuring those passwords are strong (phrases are preferable).
- Backing up sensitive data, but it should only be stored on corporate-controlled devices or authorized cloud storage services.
Now that you have your users more aware and securely connected with enough bandwidth to their jobs (more on VPNs later) — and that you have presumably ensured essentials like network and endpoint security are scaling for remote work and cover any new applications that IT has quickly stood up — it is time to consider all the threats that you commonly face and which will only be amplified by the surge of off-site workers, who are inadvertently creating new vulnerabilities and opportunities for steely cybercriminals.

Targeted attacks will likely increase, and scam methods (read: tactics, techniques and procedures) used by adversaries in the era of coronavirus will need additional monitoring and good threat intelligence sharing. There seems to be some divide within the dark web over whether to leverage the pandemic as a hook from which to lure victims, but as the legitimate economy dips, cybercriminals will look to recoup lost revenue. As such, any cybercriminal slowdown manifested out of compassion is likely to be short lived.

As days and weeks go on, you will have more data from which to determine where your weaknesses lie (misconfigurations, elevated privileges, unusual traffic patterns, data exfiltration, cloud worries, etc.) But there is no reason to wait because many of the threats you face with a work-from-home workforce will be familiar to you. This includes insider threats of both the accidental and intentional variety.

Each issue needs its own playbooks to allow for consistent and predictable alert handling, investigation and incident response. Security orchestration, automation and response (SOAR) technologies can kick off these automated workflows so they require limited human intervention, leaving your SecOps professionals to attend to more pressing matters (which will likely be more common in the era of coronavirus). You can use SOAR to build customizable processes that automate everything from case enrichment to remediation, hopefully with simple drag-and-drop functionality.

**When designing playbooks, your methodology should include:**

1. Defining which playbooks you need based on your threat assessment.
2. Prioritizing the most important use cases for your security posture.
3. Understanding the security processes that need to be part of each playbook.
4. Applying rigorous development methods for building each playbook that includes testing, staging and formally introducing into your environment.
5. Measuring what constitutes a successful playbook.
Malware

Coronavirus-themed malware campaigns (typically packaged as part of email scams – more on that in the next bullet) have spun up in earnest, and the payloads are installing keyloggers, harvesting credentials and locking down systems with ransomware (this is especially a big risk at health care organizations as a global medical emergency continues).

One of the challenges arising with the wave of remote work is the lack of endpoint detection and response (EDR) products to secure endpoints while outside of corporate network. While EDR is a valuable tool on its own, using defense-in-depth is an effective malware mitigation strategy.

High-level tips for defending against malware:

• Do not use accounts with elevated privileges for day-to-day operations.
• Secure all endpoints with EDR products.
• Partition/segment your networks (and keep home networks segregated, as devices on them likely will not be fully patched). You can also consider performing home network scans for vulnerabilities.
• Use security analytics and intelligence-driven threat hunting to identify sophisticated attacks.
• Practice zero-trust security, whose central premise is that organizations should not automatically trust anything inside or outside its perimeters at any time.
Phishing

Email-based attacks remain the primary vehicle by which malicious hackers compromise defenses. Whether it’s to pilfer credentials, steal money, install malware or establish an initial foothold on a target network, these dubious dispatches are growing more nefarious, and the coronavirus outbreak provides the perfect jumping-off point for fraudsters hoping to cash in on fears and uncertainty surrounding the crisis.

Lack of continuous cyber training & awareness programs increases the risk of malicious content landing in an organization’s environment. Uncertainty and willingness to urgently address issues remotely, unfortunately, can complicate matters and compound the phishing risk.

One such use case is:

Remote Conferencing

With virtually all company meetings now moved from in person to online, attackers are licking their chops and digging into their toolbox to discover inventive ways to exploit remote conferencing. What was once a presumptive safe space has now moved to a gaping exposure point, where miscreants are waging everything from playful intrusions to targeted attacks that could expose proprietary information or sensitive data, such as credentials that are sometimes shared through chat windows. In addition, online malefactors have stood up numerous domains and apps impersonating popular video conferencing services, with the goal of collecting personal information.

The recommended approach to reduce the risks associated with remote conferencing is:

- Enforce mandatory security training & awareness programs. Short videos describing what is approved/not approved when it comes to video conferencing, followed by a few questions, will help ensure employee readiness across all remote locations.
- Enable password protection for all meetings and avoid sharing links to meetings via social media posts.
- Always double-check all external participants.
- Don’t fall for fake apps or URLs professing to be Zoom or some other video conferencing software.
- If you use SOAR to help streamline phishing response, your monitored mailbox (where users can report phishing) can be set up to automatically ingest cases into the platform, which then performs automatic enrichment in a matter of minutes and runs a flow to take necessary actions, which can range from determining a false positive to full remediation.

A Note on Zoom

Popular enterprise video conferencing service Zoom has recently come under fire over alleged privacy missteps and security weaknesses, from “zoombombing” to concerns over illegal personal data disclosure. Since then, the company has pledged to address the problems, including instituting a 90-day freeze on features while it responds to the issues. The flap has prompted some organizations, including Google, to ban the use of Zoom, while the Taiwanese government has imposed an outright ban on the popular software. But there is a notable split within the security community over the true risk that Zoom presents, with some experts arguing it depends on a company’s threat model and can be assuaged with security basics.
DDoS Attacks

Distributed denial-of-service attacks are easy to launch and can significantly degrade website, server and application (including VPN, services) performance and availability. These assaults can be even more consequential when an entire remote workforce is collectively reliant on access to corporate network resources. Oftentimes, the takedown of a targeted system is the one and only goal of a DDoS attack, but these disruptions can also act as the canaries in the coal mine and/or smokescreens for an infiltration or data theft heist happening elsewhere on your network. Cybercriminals like to create confusion, and they sometimes turn to DDoS attacks to distract and misdirect resource-deprived organizations from their primary goal: to pillage sensitive data. Carnegie Mellon University’s Software Engineering Institute has offered useful suggestions for deterring DDoS attacks.

Remote Access Hacks

As mentioned, enterprise VPNs and remote desktop products are key pieces of technology to ensure secure connectivity – and their usage is booming. But because they are so integral to the protection of an enormous influx of remote workers, they will enter more than ever into the crosshairs of attackers, who are actively hunting for vulnerable iterations of the technology or delivering phishing emails.

Mitigations against remote attacks:

- Update VPNs, network infrastructure devices and devices being used to remote into work environments with the latest software patches and security configurations.
- Be prepared to ramp up the following remote access cybersecurity tasks: log review, attack detection, and incident response and recovery.
- Implement multi-factor authentication on all VPN connections to increase security. If MFA is not implemented, require teleworkers to use strong passwords.
- Ensure IT security personnel test VPN limitations to prepare for mass usage and, if possible, implement modifications — such as rate limiting — to prioritize users that will require higher bandwidths.

-Source: U.S. Cybersecurity and Infrastructure Security Agency

General Teleworking Tips

1. Develop and enforce a telework security policy, such as having tiered levels of remote access.
2. Require multi-factor authentication for enterprise access.
3. Use validated encryption technologies to protect communications and data stored on client devices.
4. Ensure that remote access servers are secured effectively and kept fully patched.
5. Secure all types of telework client devices – including desktop and laptop computers, smartphones, and tablets – against common threats

Source: U.S. CERT
III. Setting up and Succeeding with a Remote SOC

For some organizations, conducting security operations remotely is something they have done long before coronavirus, while for others the pandemic has ushered in a drastic change to their day-to-day, leading to big challenges in maintaining SOC efficiency at a high rate.

Fully remote SOC and IT setups should be, at least to a certain degree, part of an organization’s business continuity and disaster recovery processes. For example, SecOps and IT teams must have plans in place for how they will interact with technology, such as to reimage a laptop that is not physically reachable. This requires ensuring sufficient control over a cloud environment.

Another solution to these newfound challenges is having the ability to integrate with hundreds of different third-party solutions from a single workbench (aka a SOAR platform), allowing SOC teams to drastically reduce their work surface and decrease mean time to detection (MTTD) and mean time to response (MTTR), even as they call the shots from remote locations.

Pointers for establishing a highly functional remote SOC:

• Ensure the SOC obtains proper visibility across all urgent changes that might impact their operations. Proper syncs among affected teams are crucial.
• Establish daily check-in meetings for SOC personnel.
• Review playbooks/use cases to make sure they are covering the threat landscape that may have changed due to the pandemic.
• Deploy real-time secure collaboration tools across the SOC to ensure all team members have proper awareness of all alerts and are able to contribute to each in a convenient way.
• Ensure each remote resource has supporting technology to be efficient in their day-to-day operations, including overall visibility into real-time SOC dashboards.
• Implement a layered “on-call” approach, where applicable, to make sure more than one person is always available for escalations.
• Redistribute the workload to give the ability for each analyst to perform different types of SOC activities during their shift. This will help keep them motivated.

Reassessing Visibility Amid New Risks & Security Gaps

The spike in coronavirus-themed threats detailed above would appear to imply that remote security operations professionals will have little time to adjust to their new surroundings before being tasked with an influx of alerts related to the very crisis that has sent them out of the physical confines of a SOC. But that may not always be the case.

With employees now relying on untested and unresilient VPNs and other remote access systems to ensure secure connectivity – in addition to other departments quickly standing up unmanaged apps and a general rise in work being conducted from non-approved endpoints – your SecOps team may lack adequate visibility and sufficient monitoring into the actions of a much higher percentage of end-users than normal, resulting in actually a reduction in alerts, including false positives, you are seeing.
No, cybercriminals did not reform overnight and your users did not suddenly become policy-abiding goody-goods. You’re just not seeing everything you are used to seeing, which spells trouble. You may be missing alerts (some of which could signal new areas of risk, requiring new data sources, playbooks and use cases), but you also may be losing awareness as to where sensitive data resides and whether you can attest to compliance demands with the same confidence you once could. Now is the time to be nimble.

Here again, SOAR technology can assist. The ability for these platforms to integrate with a wide variety of third-party solutions allows them to accommodate crucial synchronization among different departments, even those that have no access to the platform. Asynchronous actions are additionally available in case certain tasks that require a documented approval (i.e. “send email and wait”, “send SMS and wait”, “update ticket and wait”, etc.)

Keeping Communication Flowing

Communication is always a key element but now during a pandemic-forced quarantine it is an essential need that SOC personnel stay engaged and on the same page. Not everyone is able to immediately adjust to the abrupt transition to remote work and keep the same pace of their work and sync with key stakeholders as they did prior. Individualization and expectation-setting here will be key so managers can determine how newly remote analysts and engineers can work most effectively and succeed within the spectrum of their personal style. Plus, people tend to make poorer decisions when under duress, and the current situation of global crisis is not helping matters.

Well-practiced shift handoffs and regular sync-up calls are critical as the team conforms to its new workplace surroundings... Daily sync-up calls are recommended during the first several weeks as the team conforms to its new workplace surroundings, especially Tier 1 analysts who tend to be younger and may have trouble finding focus in potentially distracting (and potentially dysfunctional) living quarters.

Maintaining Focus on Well-Being and Training

Anyone knows that life in the SOC can be full of grunt work requiring the “eyes on glass” tedium of monitoring, triaging and potentially escalating alerts, with much of analyst time spent sifting through the digital equivalent of a monster haystack in search of a needle or two. While SOAR can help to alleviate alert deluge – and the harsh consequences of alert fatigue and analyst burnout – front-line coverage is needed.

But not everyone will thrive away from their cubicle, especially during periods of quarantine when homes will include others (and possibly children) under guidance to also stay put. This is not to mention that Tier 1 work is often performed by entry-level analysts whose domiciles may not be conducive for multi-monitor telecommuting, who may be uncomfortable with the autonomy work-from-home life requires or who simply may be distracted by the temptation of their PlayStation sitting a few yards away from their workstation. To overcome this potentially damaging dynamic, your SOC will require strong mentorship and support from more experienced colleagues.

Finally, nationwide lockdowns, combined with the psychology of uncertainty, can take a toll on even the most strong-minded of individuals. The e-book we recently published on burnout in the SOC contains information and recommendations that may come in particularly handy during these turbulent times.

Last Word: A New Normal?

The good news is that your business is likely still functioning and its security hasn’t eroded in one fell swoop. Yes, new obstacles and hardships may have arisen, but as Benjamin Franklin said, out of adversity comes opportunity.

In addition to the due diligence evaluation suggested above, collect key SOC metrics to measure, for example, how analysts are progressing. It may be too soon to discuss a paradigm shift is underway, but the expectation should be that remote security operations may become standard operation procedure – at least to some extent – going forward, and you should use this period as a trial run, of sorts, to ascertain what works and what does not.

To learn how Siemplify can help your SOC thrive and remain agile amid these fresh challenges and continued uncertainty, visit siemplify.co.
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.