Logsign

COVID-19 Pandemic: Challenges and Remedial Measures for Remote Security Operations

Contents

Introduction 3

Post-COVID-19 Paradigm Shift in Remote Security Operations 3

Problem Statement: What are the Main Security Concerns? 3

1.4 Migrating a legacy SIEM to next-gen SIEM 4

Remedies: How Can I Stay Protected in Quarantined World? 5

- Create an Explicit BYOD Policy 5
- Browse Safely 5
- Protect Against DDoS Attacks as Employees Work from Home 6
- Deploy Two-Factor Authentication to Ensure Data Confidentiality 6
- Deploy a Network Security for Remote Security Operations 6
- Secure Communication with VPN 7
- Use Anti-Phishing Best Practices 7
- Review Incident Response Plan (IRP), Business Continuity Plan (BCP), and Disaster Recovery Plan (DRP) 7
- Develop a Security Awareness Program 7
- Create a Virtual IT Help Desk 8
- Equip Your SOC with SOAR Tool 8

The Final Word 8

References 8

Introduction

The COVID-19 pandemic has created an enormous challenge for Security Operation Centers (SOC) and security operations teams such as Chief Information Security Officers (CISOs), SOC Analysts, Security Managers, and Cybersecurity Practitioners working around the globe. The distributed employees are remotely connecting with one another and with their working environment that may include cloud systems, data centers, departmental servers, and so forth. Therefore, the role of information technology has become more crucial than ever.

In this whitepaper, we will delve into various security issues that are being created for remote security operations, as well as the remedial measures that can help detect and prevent these security issues. Here is some help!

Post-COVID-19 Paradigm Shift in Remote Security Operations

Transition to remote working is a massive post-COVID-19 paradigm shift. Daily life as well as the working environment are changing for security operation teams. In order to ensure business continuity, many organizations are attempting to provide technologies that facilitate remote working.

Undoubtedly, the paradigm shift has rapidly led to some hasty infrastructure deployment, which may have circumvented routine change-control processes and related risk assessment. Although some enterprises have already applied remote-working solutions, yet they did not incorporate the entirety of the workforce, neither in terms of job roles nor the number of employees.

Problem Statement: What are the Main Security Concerns?

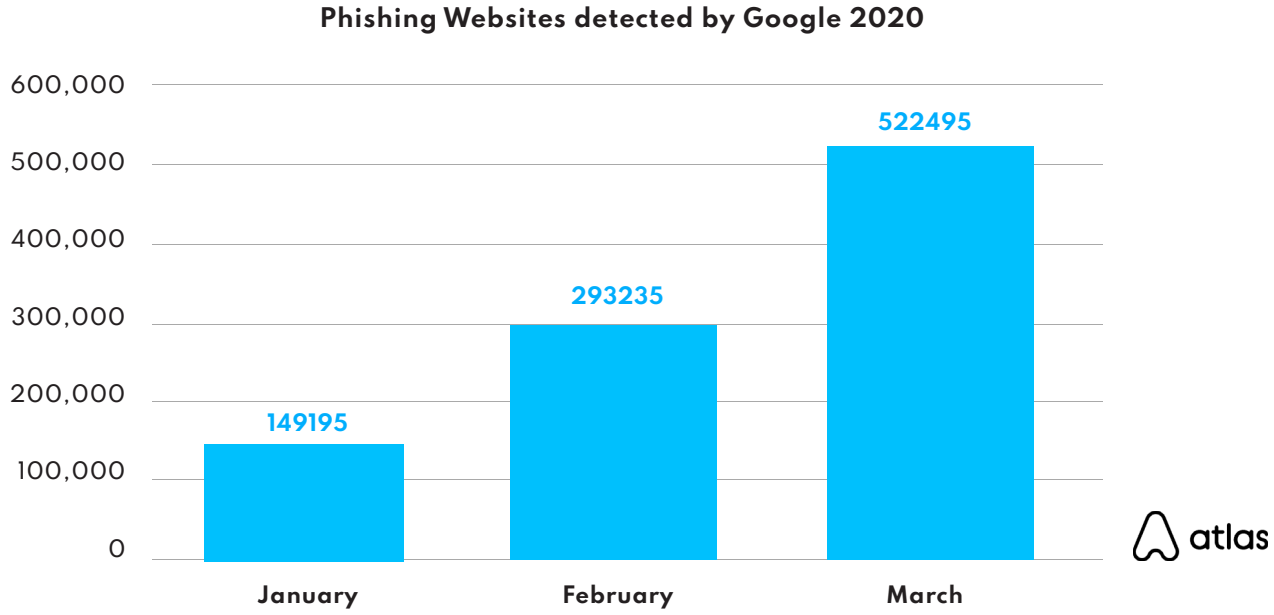
The wholesale shift to operate organizations online and the surge in communications have opened the floodgates of cyber-attacks. COVID-19 pandemic has presented numerous challenges for SOC teams, both in-house and Managed Security Service Providers (MSSP).

According to the **13th annual State of the Network Global Study,** information technology is living in the age of dynamic disruption, which is twofold. First, **COVID-19 is pushing the employees into working remotely** and the second thing is that it is making emerging technologies go mainstream.

In the aftermath of the outbreak, security operations teams are highly dependent on the internet to establish a communication channel and make human interaction possible. Not so long ago, the **US Department of Health and Human Services (DHHS)** was attacked by bad guys to disrupt information flow and operations.

Threat actors and scammers are capitalizing on people's fear and emotions during the COVID-19 Pandemic to launch **phishing campaigns.** They target Skype credentials and leverage fake Zoom video conferencing meeting notifications. Most hackers are impersonating as **WHO and CDC to launch phishing campaigns.**

According to a **Google report**, there were 149,195 active phishing websites in January 2020. In February same year, the number rose to 293,235. And in the next month, March, 522,495 phishing websites were reported.



FBI has also issued an alert regarding COVID-19-related phishing attacks. Moreover, Confense researchers revealed that scammers are spoofing Skype amid the spike in remote work.

Besides, hackers are posing a grave threat to an organization's perimeter security. Businesses are on the verge of destruction unless they continually monitor their physical and network security.

Distributed Denial of Service (DDoS) attacks are also skyrocketing amid the outbreak. According to the Kaspersky Lab, a cybersecurity firm, in the second quarter of 2020, DDoS attacks were increasing by leaps and bounds, which had tripled from the second quarter of 2019.

Organization leaders and decision-makers recommend a SOC to perform their IT functions effectively. Distributed employees need to access internal applications and services so that they can carry out necessary business functions remotely. Typically, most companies don't have any security mechanism to make their data and applications online over the Virtual Private Network (VPN) or the internet. Doing so can allow threat actors to gain their malicious goals. That is the reason traditional SOCs don't allow open access to remote-users unless there is a stringent access mechanism.

According to Charles Thompson, senior director at Viavi Solutions, since remote working has become a new norm, it is challenging for security teams to identify and adopt technologies, such as troubleshooting applications, VPN oversubscription, and flow-based reporting to manage bandwidth consumption.

Miten Marvania, COO at Agio Inc, an IT managed services firm based in New York, also adds that organizations without proper VPN licensing have to make compromises to let more people in, and they let their guards down a bit.
In addition, the U.S Department of Homeland Security has also issued a warning in March 2020 with regard to a rise in hackers exploiting VPN vulnerabilities during the COVID-19 pandemic.

The enforcement of corporate security policies and controls on the distributed employees is a Gordian Knot. The organization's current Incident Response Plan (IRP) and Business Continuity Plan (BCP), which are specifically designed for in-house security professionals, are inappropriate for remote workers and deem unfit for pandemic scenarios.

Distributed employees use their own devices, also known as Bring-Your-Own-Devices (BYOD), at home that is not as monitored and protected as they are in the corporate network environment where security operations teams continually

keep a check on them. As per the CISO's Benchmark Report 2020, companies are endeavoring to manage remote employees' use of smartphones and other mobile devices. The report found that, according to 52% of respondents, protecting mobile devices from cyber threats is a daunting task.

Ensuring Data Confidentiality is a big issue when two or more parties are communicating over a network. Verizon's Data Breach Investigation Report discovers that 30% of all data breaches involved the use of stolen credentials. The traditional password creation strategies are inadequate to protect communications.

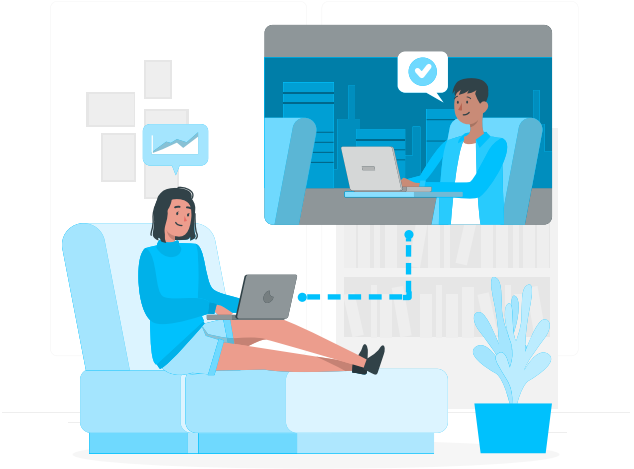
Remedies: How Can I Stay Protected in Quarantined World?

Create a Remote Working Policy

The IT Governance recommends creating a remote working policy for any company with employees working from home. The policy must include the following guidelines:

- Store devices securely
- Create and maintain strong passwords
- An appropriate Acceptable Use Policy (AUP) for websites that are not related to work.

Also, the remote policy should incorporate technical solutions that have been implemented to protect sensitive information and explain how the workforce can comply with them.



Create an Explicit BYOD Policy

In addition to in-house SOC infrastructure, the role of BYOD in remote security operations is also critical. Distributed employees use BYOD from home, and ensuring their security is out of the question. BYOD is often considered a vulnerable device.

The SecOps or SOC teams should ask their customers or employees not to use public WiFi on their business BYOD. Since BYOD are insecure, employees should prefer storing their corporate data and other sensitive information on the cloud storage.

Browse Safely

Whether you are a CISO, Security Manager, SOC Analyst, or any cybersecurity professional, using a browser and visiting websites is always indispensable to conduct business operations. Frustrations and complaints about web browsing are on the rise. Disruptive pop-ups, lack of data privacy, and intrusive advertising are the main concerns of insecure browsing. Panda Security recommends the following tips for safe browsing:

- Always keep your browser and plugins updated
- Block suspicious pop-ups
- Use ad blocker app
- Clear your web browser cookies and cache
- Enable "do not track" in your web browser
- Use a Password Manager
- Use a VPN
- Turn on Private Browsing
- Always apply the latest patches to your antivirus and firewall and keep them up-to-date

Moreover, remote security operations should be conducted through secure websites with protocol "HTTPS" rather than "HTTP." The SSL certificates show a grey padlock and HTTPS against the domain name in the address bar of a web browser. Secure web browsing with web filters when working remotely. Web filters can also detect and prevent malicious web traffic, as well as block access to untrusted domains.

Protect Against DDoS Attacks as Employees Work from Home

Identifying weak nodes and increasing their reliability can prevent DDoS attacks. To this end, Kaspersky Lab recommends conducting a fault tolerance analysis. Since attack vectors and traffic peaks are changing, some resources may work unstably.

Besides, Kaspersky also recommends protecting the non-public servers as they have a crucial role in business continuity. Due to their significance for critical business operations, they are becoming increasingly attractive and valuable targets of malefactors.

Deploy Two-Factor Authentication to Ensure Data Confidentiality

Distributed employees often work on corporate laptops that are subject to remote access security controls. To add a strong security layer to the traditional login process, Two-Factor Authentication or 2FA is implemented that is a robust identity verification method.

Unlike a traditional login method where a username and password are required, in 2FA, a user must provide two pieces of evidence to authenticate himself on the website. An additional key is also be required that can be one or more of the following items:

- Possession (something that you have)
- Knowledge (something that you know)
- Inherence (something that you can provide)
- Location (any place that only you know)

The 2FA is also necessary to comply with PCI regulations and FFIEC's mandate regarding identity protection.

Deploy a Network Security for Remote Security Operations

Network security is the first line of defense in the face of nefarious cyber threats and attacks. Below are some recommended security practices for security teams:

1.Apply Network Encryption: There might be frequent communication between employees and their corporate IT environment such as SOC. Security engineers or SOC analysts must provide strong network encryption that should be compatible with employees' devices so that any wireless device seeking connection with the corporate network will require the key. Configure the router with a WPA2 encryption scheme to ensure a robust security posture.

2.Change the Default SSID: The SSID provides identification to the router. My routers, by default, use the name of the router as their default SSID. For instance, the routers of the Linksys brand often use "Linksys" as the default SSID. This can be a security risk because the name is very obvious and hackers can easily exploit this. Therefore, it is recommended to change the default SSID of your router.

3.Disable SSID Broadcast: The wireless routers broadcast SSID to help make finding the wireless network easily. If security experts disable SSID broadcast, it is difficult for malefactors to find your network when browsing available on wireless networks.

4.Change the Default Router Password: The security practitioners need to change the default router password with a strong password, which should contain upper- and lower-case letters, numbers, special characters, and their combinations. The password length should be at least 8 characters.

5. Enable Router Firewall: The SOC analysts should configure all business laptops and other official devices with a firewall that is implemented through the Endpoint Protection software for Host Intrusion Prevention (HIP).

Secure Communication with VPN

Secure your communication with Virtual Private Network (VPN). Update your VPN frequently and implement multi-factor authentication on all VPN connections. The security professionals must know VPN limitations. If any problem occurs, these security professionals should address it and provide appropriate recommendations.

Use Anti-Phishing Best Practices

Anyone can be a victim of a phishing attack. An Email is an official link between the employee and his SOC or business leaders. Nowadays, Organizations are relying heavily on Emails to conduct their day-to-day business operations. Unfortunately, cyber pests are exploiting people's fear and uncertainly and send phishing Emails to gain their malicious goals. Below are some best practices to avoid phishing emails:

- Report suspicious activities to your SOC
- Stay vigilant against malicious Emails, links, or attachments
- Comply with corporate Email policy
- Configure your Email client
- Avoid using removable media
- Protect your password
- Install anti-phishing tools such as Bit Defender Antivirus Plus or Norton Antivirus Plus.

Review Incident Response Plan (IRP), Business Continuity Plan (BCP), and Disaster Recovery Plan (DRP)

After the outbreak of the pandemic, people from all spans of life, including educationists, healthcare specialists, engineers, and so on, are shifting their traditional office work to remote work. This is the reason the internet traffic has been increased tremendously. So, conducting remote communication during this big data traffic is a daunting task, and organizations are required to adjust their IRP, BCP, and DRP plans to cover scenarios that should be pertinent to the current crisis. Conduct a routine audit of these plans to identify weaknesses and apply necessary updates to deal with them. Don't forget to wear masks and maintain social distancing when a physical appearance is necessary for the SOC.

Develop a Security Awareness Program

Enterprises' security training providers must establish a short work-from-home security awareness program to assist the employees to understand the potential threats and their preventive measures that are required when working remotely. This program should include at least the following best practices:

- Password policy that further incorporates strong password creation rules, as well as creating unique passwords and not reusing passwords between different accounts and devices.
- Apply frequent patches and install updates regularly
- Don't click on unwanted links or malicious attachments, especially when they are given in a suspicious Email. These Emails might be a phishing scam.
- Don't' share your username and password with anyone.
- Don't install any unknown application because it might be malware.
- Don't visit torrent websites as they provide a great many potential avenues to threat actors.
- Don't be lured through gifts or online stores offering absurd deals.
- Check the URLs thoroughly before you visit them. For example, there is a difference between www.yahoo.com and www.yahooo.com.
- Use up-to-date antivirus and antimalware programs.
- Avoid connecting your business laptop with public WiFi or networks.
- Keep your Bluetooth off when you are not using it.
- Use a complex passcode for your BYOD.

Create a Virtual IT Help Desk

SOC analysts need to create a virtual IT help desk in order to address complaints from employees regarding controls, processes, and technology limitations that are preventing them from working remotely.

Equip Your SOC with SOAR Tool

Recently, a 2020 State of Security Operations Report is published by Micro Focus, in partnership with CyberEdge Group. The report findings show that 89% of the respondents expect to use a Security Orchestration, Automation, and Response (SOAR) tool within the next twelve (12) months.

The findings in the report explicitly indicate that SOCs need to be matured and, to this end, they require to deploy next-gen tools, such as **Logsign SIEM** and **SOAR**, at an unprecedented rate to address security gaps in security.

The Final Word

The world has been quarantined in the aftermath of the COVID-19 pandemic. Not only the health sector has been paralyzed but also the cybersecurity arena is on the verge of destruction. More and more people are working remotely. The in-house SOCs are also functioning remotely and cybersecurity is also requiring a new direction to survive and thrive in the quarantined world. In this whitepaper, we have shed light on various cybersecurity issues that are hindering remote security operations today. Besides, we have also discussed numerous security solutions that can ease the situation if security operations teams such as SecOps, security managers, CISOs, SOC analysts, and so forth, can follow and implement them.

References

1. https://healthitsecurity.com/news/new-covid-19-phishing-campaigns-target-zoom-skype-user-credentials
2. https://www.pcmag.com/news/phishing-attacks-increase-350-percent-amid-covid-19-quarantine
3. https://www.itgovernance.co.uk/blog/the-cyber-security-risks-of-working-from-home
4. https://www.itsecurityguru.org/2020/08/11/remote-workers-at-increased-risk-from-ddos-attacks/
5. https://securitybrief.eu/story/ddos-attacks-doubled-in-q1-2020-as-attackers-target-remote-workers
6. https://medium.com/@emmaaajohnson21/how-to-use-2fa-for-rdp-e4ff10e9e783
7. https://blog.techinline.com/2019/08/07/two-factor-authentication-remote-support/
8. https://www.cybersecurity-insiders.com/how-to-overcome-cybersecurity-challenges-for-remote-workers/
9. https://www.itgovernance.co.uk/blog/the-cyber-security-risks-of-working-from-home
10. https://www.pandasecurity.com/en/mediacenter/mobile-news/tips-browsing-safer/
11. https://cybersecurityventures.com/12-tips-for-safer-browsing/#:~:text=1%20Use%20a%20VPN%20to%20hide%20your%20IP.,authentication.%20Most%20secure%20sites%20will%20have%20two-factor%20authentication.
12. https://alvcoaching.com/cybersecurity-and-remote-work/
13. https://www.cisecurity.org/blog/cybersecurity-challenges-of-a-remote-workforce/
14. https://searchitoperations.techtarget.com/news/252481738/COVID-19-remote-work-forces-shift-on-SecOps-strategy
15. https://www.channelfutures.com/channel-research/work-from-home-remote-access-challenges-netops-secops
16. https://www.pwc.com.pk/en/assets/document/Impacts%20of%20COVID-19%20on%20Organisations%20-%20Cyber%20Security%20Considerations.pdf
17. https://thehackernews.com/2020/09/covid-cybersecurity-report.html
18. https://us.norton.com/internetsecurity-privacy-safe-vpn.html
19. https://resources.infosecinstitute.com/topic/top-10-anti-phishing-best-practices/
20. https://www.computerweekly.com/opinion/A-view-from-the-SOC-Maintaining-security-capabilities-during-the-pandemic
21. https://nationalcybersecuritynews.today/cybersecurity-comptia-info-introducing-a-technical-guide-to-remote-security-operations/
22. https://securityboulevard.com/2020/06/8-best-practices-for-secure-remote-work-access/
23. https://www.weforum.org/agenda/2020/08/covid-19-future-of-work-employees/
24. https://execed.economist.com/blog/industry-trends/successfully-leading-distributed-workforce
25. https://www.bbc.com/worklife/article/20201023-coronavirus-how-will-the-pandemic-change-the-way-we-work
26. https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/the-bedrock-of-a-post-covid-19-security-operations-center
27. https://constanttech.com/cyber-security-operations-centers-the-response-to-covid-19/
28. https://www.securitymagazine.com/articles/93779-of-security-operations-center-employing-ai-and-machine-learning-tools-to-detect-advanced-threats

About Us

Logsign was established in 2010 to enable cyber security practitioners to work more efficiently with smart, clutter-free and next-generation softwares. Securing the IT systems and managing cyber security operations should not be so complex, time consuming and over-priced. This is why we developed our smart and simple-to-use SIEM and SOAR softwares considering the market's current and future needs. Automation starts the new era in cybersecurity. We believe with this era, automation handles the manual workload of humans upto 98%. Thus, efficiency in cybersecurity operations is not a dream anymore. SOAR software is in the heart of operations enhancing security teams work in a smart, collaborative and effective environment. You can't protect before you see and detect. Collecting any data, visualizing and turning into actionable intelligence are possible via our infinitely scalable and cluster SIEM. With 10 years of experience, Logsign is a sincere team player for all internal & external parties, trusted by more than 500 enterprises, ministries and state agencies.

www.logsign.com | support.logsign.net | 0 850 660 0 850