KPMG

Cybersecurity during Covid-19

Recalibrating your security operations

May 2020

When Covid-19 broke out, SecOps teams faced a perfect storm of constraints on their working practices, reduced access to operational tools, and a threat landscape in which criminals are exploiting the fear and doubts around Covid-19. How do organizations adapt?

Running a SecOps function under the working conditions that have arisen from COVID-19 measures is a challenge. There is some practical advice we can offer, and some areas for consideration.

Not everything can be done remotely

Security Operations Centre's (SOC) may be a physical site that can't be easily or fully virtualized to allow SOC engineers remote access to SIEM tooling and ticketing systems.

Given the criticality of the SecOps function, access to the SOC may be arranged with the help by local authorities, with some limitations potentially placed on the number of staff allowed on site at any given time.

The need to adapt shift schedules to protect employees' health, and also provide them with appropriate letters of authority to confirm their need to travel, may be required.

This requirement also assumes risk acceptance in relying on a subset of the usual tooling. Make sure the second line risk function is aware of this and work together to prioritize your SecOps capabilities.

Enable the team to work securely

Reiterate the need for SecOps employees to maintain secure working practices, and help employees self-assess their physical security at home. If they live with roommates/flatmates, parents or teenage children, it may not be suitable to have sensitive discussions in their home environments where they may be overheard.

If employees aren't able to secure their remote working environment, put in place guidelines and procedures to assist them. Privacy screens are helpful, as is the use of headsets and protocols around only sharing sensitive information in writing rather than having it announced on calls. Also, consider flexibility in shift schedules to allow employees to work at times when privacy can be assured.

Recreate their workstations

The team is used to working with several monitors and with a specific keyboard. These pieces of hardware aren't just preferences; they enable SecOps analysts and engineers to work quickly, efficiently and accurately.

It's not possible to generate the same productivity working from home with just a laptop. If employees need additional monitors, cables and keyboards, be prepared to fund their needs. The expenditure will increase productivity and may offer longer-term flexibility in working practices.

Widescreen monitors with split-screen options are excellent for enabling multi-tasking across multiple systems and tools.

Communication is key

The ability to collaborate in a distributed environment may be a challenge for analysts who are used to face to face problem solving. They'll need the ability to communicate securely during this period, with the ability to share pictures, screenshots and videos. Access to a company phone or a personal phone with a mobile device management solution is essential.

It may help to consider a fallback communication mechanism if an incident compromises the organization's network. Cloud-based video conferencing and collaboration platforms may offer a quick solution, but be aware of the security challenges these may present the team.

Protect the SOC infrastructure

Keep the systems used by the SOC well secured from the broader enterprise network. It's worth checking that the firewalls are appropriately configured to protect these systems from any compromise of the enterprise network.

Provisioning an alternative VPN access to critical SOC systems should also be considered, to allow fallback mechanisms if the infrastructure is compromised.

Adapt resourcing models

Be aware of the heightened risk of analysts and engineers becoming ill during the pandemic period, as well as the impact on them as they look after children and others who rely on them.

Implement a good resourcing tool that allows employees to flag capacity challenges. Also, examine the length of shifts, and the impact it will have on employee well being, and consider scheduling in time for employees to "switch off" from their work environments.

Lastly, consider building additional redundancy into your shift patterns, further overlapping shifts or placing additional people on call to allow for overage at short notice.

Pay attention to local conditions

Many SOC teams have members based in different regions with different curfew hours and distinct local policies relating to Covid-19. Pay attention to guidance and restrictions in Saudi Arabia, regional and city-wide level where employees are based, and make sure shift rota reflects team member's conditions. Some may only be able to visit shops in specific time windows, collect medication or leave the house at all.

Gear your tools to the threat landscape

The new threat landscape under Covid-19 consists of a variety of consumer and employee targeted phishing campaigns, as well as a higher frequency of enterprise-level cyber attacks. These include ransomware, crypto-mining operations, and privilege escalation attacks.

SIEM tooling may be configured to mark levels of activity suspicious under normal circumstances. Be prepared for those levels to change. Joiners, movers and leavers processes may be more frequent due to the high turnover of staff.

Review SIEM systems and make sure they reflect the new threat landscape and consider how to automate detection and remediation processes to handle a higher frequency of attacks and reduced staffing. You may have limited visibility of BYOD and other home working solutions, implementing workarounds.

Assess your End-Point Security

- Assess remote work station security controls and features including overall desktop controls such as BIOS, prevention of booting, checking of controls such as logs, Antivirus, patches, anti theft measures, user authentication, secure network communication agent (corporate VPN or zero trust), and enforcement of Multi Factor Authentication (MFA).
- Assess security controls and features on mobile devices including the usage of mobile device management solution (MDM), user authentication, storage encryption, enforcement of security updates configuration
- Assess cloud security controls including Identity Access Management (IAM) multi factor authentication and privileged access, Data Leakage Prevention, cloud data encryption, network segregation, and advanced threat protection.

Assume the long game

Restrictions relating to Covid-19 may recur if countries experience further spikes in infection rates, or if another pandemic arises. The lessons learned during this time are valuable — document the changes made; keep relevant hardware, software and incident response playbooks; and be prepared to deploy this working model again should the need arise. Aspects of this new way of working may even become the new norm.

Contacts

Tariq Dreiza
Head of Technology
KPMG in Saudi Arabia
E: tdreiza@kpmg.com
T: +966 55 388 9928

Ton Diemont
Head of Cybersecurity
KPMG in Saudi Arabia
E: antondiemont@kpmg.com
T: +966 56 860 8393