Best practices for security monitoring during a crisis
The COVID-19 outbreak has forced the hands of many organisations around the world to have their workforce switch to remote working. This presents a huge challenge to security and infrastructure teams to enable remote working at scale whilst maintaining their cybersecurity posture.

Teams should be continuously educating users about policies, guidelines and best practices. At times like these, it’s important to up the ante and increase communications, re-enforce training, and distribute corporate announcements, etc.

Staying on top of day-to-day security operations at a time like this is paramount. Following are some important tips for a SOC team to consider.
Secure your users

- Ensure you are collecting and monitoring from the following: Active Directory, endpoint security, VPN, multi-factor authentication, SSO, email, cloud services, and infrastructure.
- Run analytics on email logs for subjects related to the crisis.
- Run analytics on web proxy or firewall logs for domain names and URLs related to the crisis.
- Hunt for young domain names related to the crisis.
- Review current use cases in the light of any changes in business processes based on remote working.
● Enable operational monitoring of critical services and applications to ensure timely alerts are raised if critical services stop.

● Utilise automation to restart services should they unexpectedly stop.

● Generate alerts if systems go down and do not come up within a defined period.

● Monitor and alert on CPU/memory/storage anomalies (e.g., if your VPN appliance fails due to overheating).

● Ensure all critical services and applications are being monitored for availability.
Infrastructure & physical security monitoring

- Monitor any new cloud-based services that are deployed to enable remote working, ensure that data isn’t exposed by misconfiguration.
- Create a list of users permitted to be physically present in the office and raise alerts for non-approved users badging in.
- Monitor door/badge entry systems and correlate users against the VPN for impossible travel.
- Understand geographically where your users are and monitor access from unexpected geographies.
- Look out for port changes on the firewalls, especially around remote access protocols (SSH, VNC, RDP).
- Baseline network traffic to detect possible exfiltration — particularly because remote working and changed practices will present attackers with the opportunity to exploit the network.
Conclusion

Often the challenges associated with working from home are extensions of those linked with office-based workers. It’s ten-fold when the entire organisation is working from home.

Ensuring you have the basics in place as well as enhanced monitoring, additional automations, extra education and robust security policies, most SOCs will be more than up to the task of maintaining business continuity, securing the infrastructure and remote workforce.

If you have questions about the information in this e-Book, or have concerns about securing a remote workforce, please get in touch. We are here to help.
About LogRhythm

LogRhythm empowers more than 4,000 customers across the globe to measurably mature their security operations program. LogRhythm’s award-winning NextGen SIEM Platform delivers comprehensive security analytics; user and entity behaviour analytics (UEBA); network detection and response (NDR); and security orchestration, automation, and response (SOAR) within a single, integrated platform for rapid detection, response, and neutralisation of threats.

Built by security professionals for security professionals, LogRhythm enables security professionals at leading organisations like Cargill, NASA, and XcelEnergy to promote visibility for their cybersecurity program and reduce risk to their organisation each and every day. LogRhythm is the only provider to earn the Gartner Peer Insights’ Customer Choice for SIEM designation three years in a row. To learn more, please visit logrhythm.com.