Best Practices for Security Monitoring During a Crisis
The COVID-19 outbreak has forced many organizations around the world to transition portions of their staff to work remotely. This presents a huge challenge to security and infrastructure teams to enable a remote work force while maintaining their cybersecurity posture.

As your security partner, LogRhythm assembled a series of best practices you can use to improve your security monitoring during a crisis.
Secure Your Users

- Collect and monitor the following log sources: Active Directory, endpoint security, virtual private network (VPN), multi-factor authentication, SSO, email, cloud services, and infrastructure.
- Perform 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 your current security use cases to ensure you address new business processes and trends (e.g., remote workforce).
Business Continuity and Productivity

- Enable operational monitoring of critical services and applications to ensure timely alerts are raised if critical services stop.
- Utilize 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 and Physical Security Monitoring

- Monitor new cloud-based services that are deployed to enable remote working, and 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 VPN logs for impossible travel.
- Understand your users’ geographic location and monitor for authentication from unexpected locations.
- Look out for port changes on the firewalls, especially around remote access secure shell (SSH) protocol, virtual network computing (N+VNC), and remote desktop protocol (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.
Often the challenges faced curing a crisis are extensions of those you face with every day. Through your LogRhythm Platform, you already have the tools and content necessary to meet the challenges head-on. If you have questions about the information in this e-Book, or if you need help implementing these tips, please get in touch. LogRhythm and your customer care team is 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 behavior analytics (UEBA); network detection and response (NDR); and security orchestration, automation, and response (SOAR) within a single, integrated platform for rapid detection, response, and neutralization of threats.

Built by security professionals for security professionals, LogRhythm enables security professionals at leading organizations like Cargill, NASA, and XcelEnergy to promote visibility for their cybersecurity program and reduce risk to their organization 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.