THREAT DETECTION & RESPONSE

25 CRITICAL QUESTIONS YOU NEED TO BE ABLE TO ANSWER

Knowing your security posture from end-to-end can be a challenge. With siloed security solutions, it is hard to identify if there are blind spots that need to be resolved. Yet increasingly sophisticated attacks are growing by the year, forcing organizations to improve their threat detection and response capabilities.

The following are 25 questions you should be able to answer about your threat detection & response capabilities.

1. Can I identify the exact location, sensitivity, and relative value of all information in the organization that needs to be protected to adequately measure risk?
2. Do I have monitoring capabilities to the network, cloud, and endpoints?
3. Do I have deep observations of real-time endpoint data?
4. Can I monitor and observe the entire attack surface in my organization?
5. Is my network traffic meta-data, such as network flow data, ingested to detect malicious threats early on? And, does it follow attacker movement across the network?
6. Are User and Endpoint Behavior Analytics (UEBA) algorithms used to discover anomalous user behavior?
7. Can I track users to understand who logged on to a system, their location, what the host they connected to, and the specific actions taken?
8. Can I prioritize alerts based on rich data context (user identity, ITSM policy tags, etc.)?
9. Are my alerts enriched with links to broader threat intelligence?
10. Does my threat intelligence consist of third-party feeds such as industry related feeds from Information Sharing and Analysis Centers (ISACs)?
11. Do my monitoring processes use the latest Indicators of Compromise (IoCs)?

12. Are my logging mechanisms set at a sufficient level for IoCs to be recognized?
13. Can my team use automated remediation actions and rules based on previously detected threats?
14. Can I tell whether an endpoint is still sending logs to my console or SIEM?
15. Are my firewalls properly configured to utilize the security features which detect and alert on malicious activity?
16. Are my data pipelines tuned to accommodate security telemetry volumes?
17. Does my threat detection and response platform align with the MITRE ATT&CK Framework?
18. Are monitoring efforts backed by a 24/7 SOC?
19. Are my security analysts able to keep up with the volume of alerts presented to them?
20. Are reports available to various personas in my organization with KPIs they care about?
21. Is my organization's incident response plan reviewed on a regular basis?
22. Do I have sufficient IT resources to monitor and respond to a cybersecurity events?
23. Are call tree testing and table-top exercises performed?
24. Have I validated detection of high-risk events to check that alerts trigger properly and analysts react appropriately?
25. Does my organization participate in Red/Blue Team exercises or cyber-range events to test response times?

If you are struggling to answer any of these questions, you are not alone. Many organizations have some of the technologies to address these questions, but are still left trying to correlate insights for complete visibility and coordinated response for breaches that threaten their environments.

GET THE ANSWERS WITH CADRE INFORMATION SECURITY

For more than 25 years, Cadre Information Security has worked with companies to improve their security postures through technical expertise and guidance, and best of breed technologies. Working with our partner ecosystem, we can guide you in choosing the endpoint detection and response (EDR), network detection and response (NDR), managed detection and response (MDR), or extended detection and response (XDR) solution best suited to bolster your protection efforts.

IT'S EASY TO GET STARTED

Where are your gaps? We are here to help you navigate the challenges of threat detection and response. If you are looking to stand apart and improve your security posture, book a no-obligation consultation today to discuss your unique environment.

Contact us today at info@cadre.net