

# 10 Questions To Validate Your Detection & Monitoring Meets The Mark

**How well does your organization detect and monitor potential cyber threats?**

Malicious actors are constantly developing new forms of attack, so you must validate the extent of your detection and monitoring to ensure you are truly defending against cyber-attacks.

**Does your network monitor cyber threats 24 x 7 x 365?**

**01**

- 24x7 monitoring is critical as threat actors target organizations after working hours, and during weekends and holidays, because they know that organizations often do not monitor during these times. It only takes minutes to fully compromise an organization and exfiltrate data, and with hours of unmonitored time, the risk of a breach increases.

**What cyber threats are being monitored in your systems?**

**02**

- It is important to verify with your IT Team what type of threats they are detecting and responding to. IT organizations tend to focus on system health and uptime. It is usually not their priority to understand potential threats and develop up-to-date detection capabilities. At a minimum, you should be monitoring phishing reports, endpoint detection, anomalous user behavior & login activity, anomalous network & perimeter activity, and internal and external scanning.

**How are phishing events detected, reported, and responded to?**

**03**

- Phishing is the number one method for threat actors to compromise an organization. All organizations should have a system in place for users to report phishing emails and a response team should be ready to act on verified phishing threats, in near real time.

**Who is responsible for investigating cyber threats?**

**04**

- It is important to have clear accountability for investigating cyber threats. Cyber monitoring and investigation should be handled by trained individuals who prioritize reducing cyber risk. For IT, availability of systems is usually the priority, which means security monitoring tends to take a back seat.

**How long does it take to investigate cyber threats?**

**05**

- Responding to cyber threats is a race against time. All threat monitoring providers should provide metrics that indicate how long it takes to investigate detected threats. The longer it takes to investigate threats, the higher the risk of critical compromise.


**What percentage of detected threats are being responded to?**

**06**

-  Cyber alerts can get to extremely high volumes. Overwhelmed IT teams report that conflicting priorities often lead to missed and ignored alerts. To avoid a security breach, it is important that all alerts get investigated to identify risk and reduce false positives.


**If a cybersecurity breach is discovered, who is notified and how?**

**07**

-  To successfully combat threat actors, organizations should have an incident response plan with clear escalation and notification procedures. If monitoring is outsourced, vendors should have clear escalation and reporting SLAs to ensure that identified risk are responded to appropriately.


**Who is responsible for incident handling and remediation?**

**08**

-  When an incident does occur, organizations often struggle with what to do and who is in charge. It is important to know the extent of what your IT vendor will handle and what responsibilities fall on your team. The incident response plan should document clear roles and processes so that the organization is able to respond quickly and efficiently.


**Do you provide weekly security reporting?**

**09**

-  Security vendors should provide reporting to ensure that all alerts are responded to and investigated in a timely manner. Vendors should be held accountable to provide insight and transparency to investigation volume, response time, handling time, and outcomes.

**What standards are being used to measure your cybersecurity strength?**

**10**

-  For organizations that choose to outsource IT, it is important that vendors are working within the framework of security best practices. IT vendors should be able to provide answers to what security framework their people, process, and technology aligns to.

**Contact Us:**

 [www.cyberforceq.com](http://www.cyberforceq.com)

 [solutions@cyberforceq.com](mailto:solutions@cyberforceq.com)

 248.837.1400

