cybereason

An Introduction to Cyber Hunting

10 Immediate Actions for a Post-Breach Reality

1 Accept that a breach is inevitable

No matter how well an organization is protected, a network breach will eventually occur. A talented, persistent group of hackers will eventually be able to bypass your prevention methods, given enough time.

2 Focus on the malicious operation (Malop) timeframe

Once inside the environment, hackers move slowly and methodically to gain access to critical assets while avoiding detection. It can take months for hackers to gain full access, but once they do, the damage is nearly instantaneous. This is why the Malop timeframe offers a key window of opportunity to intercept a cyber attack.

3 Follow the hackers' steps

No matter how hard attackers try to hide their tracks, they will always leave behind some faint traces that a proactive, well-trained security team can discover.

4 Shift to proactive hunting

Don't wait to discover a breach after the damage is done. Start searching for traces of malicious activity that hackers leave behind and link separate events to a broader attack picture.

5 Continuously collect and analyze data

Continuously collect every piece of information from your environment - from endpoints and the network - as it is essential for spotting malicious activities.

6 Leverage threat intelligence to hunt for known malicious activities

Run the collected data against threat feeds and blacklists to confirm the existence of known threats. Analyze this data in real time to be able to spot malicious behavior as it emerges.

7 Look beyond signatures and hashes

As most attacks use new malware and exploits, they can only be identified by looking for known malicious behavior, such as reconnaissance, network scanning, hacker communication with C&C servers, and data exfiltration.

8 Make judgements to eliminate false positives

Rule out normal user behavior and unsubstantiated suspicions that did not evolve into a larger malicious operation.

9 Put attacks in context to see the full threat picture

Connect separate pieces of evidence to form a coherent attack picture. This allows the team to connect seemingly unrelated threats and understand the full scope of an attack.

10 Finally: Consider an automated hunting platform

Increase your team's productivity: Use an automated solution that continuously scans your entire environment and syncs together all of its elements to identify emerging threats and eliminate false positives.

Cybereason.

Let the Hunt Begin.