THE 5 KEY STEPS OF INCIDENT RESPONSE

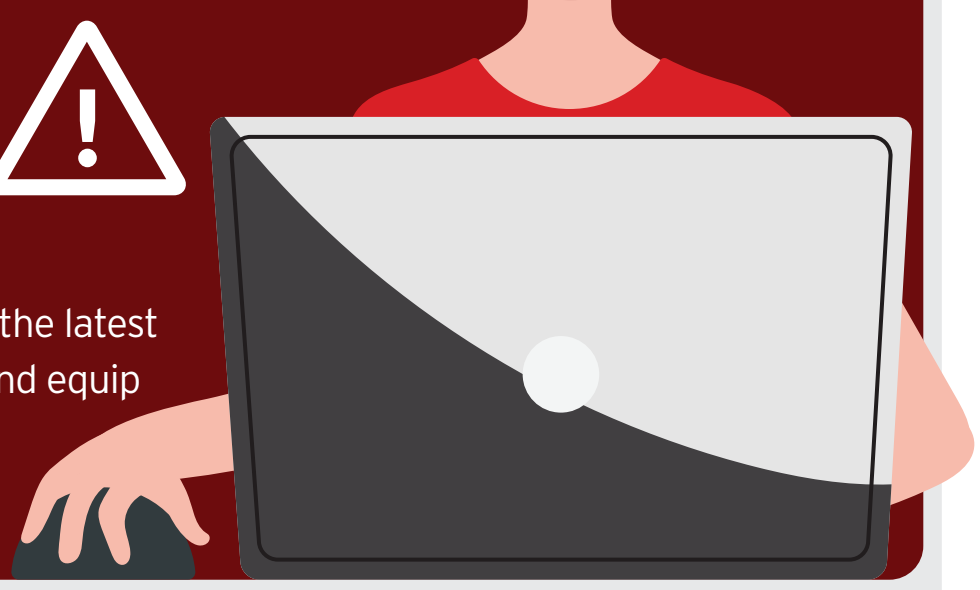
It's late at night and your phone is ringing. Your organization is experiencing a cybersecurity breach and you need to respond—fast.

As scary as this sounds, experts agree breaches are inevitable. But keeping your organization prepared, with both advanced defenses and a well-defined plan, can make all the difference.

1 THE ALERT

What started as an antivirus alert turned out to be much worse: remote management software has been installed in your network.

The right security vendor will warn you about the latest ransomware threats targeting your industry and equip you with the technology to quickly defend against them, like XDR.



2 SCOPING THE SPREAD

The attackers have already exfiltrated data from your network. After quickly taking the affected server offline, you need to judge the extent of the damage.

Pinpointing 'patient zero', the breach's point of entry, is just the beginning. You also need network and endpoint sensors to probe the full extent of the attack.

3 ROUNDING UP THE SUSPECTS

Every endpoint is a potential threat and must be treated as a suspect until the entire network can be scanned for indicators of compromise (IoC).

A zero trust approach limits the spread of the attack until every last trace of the breach has been identified. Studying the malware payload will narrow down your list of suspects.

4 SLAM EVERY DOOR

Now it's time to shut out the attackers. Uploading identified IoCs to the network firewall secures the perimeter. Next, network connections are reset and the entire system is scoured for lingering malware hash.

Compromised devices and users will need to be restricted until the breach is resolved. Studying firewall logs for mass data transfers can help identify the scale of data theft.

5 BE READY FOR THE NEXT BREACH

The attack is stopped! What's next?
Time to start preparing for the next one.

Breaches are inevitable, but you should still prepare your team and your cybersecurity solutions for the next attack. Study your response and identify areas for improvement. Next time, the rapid response enabled by an XDR platform and zero trust posture could make all the difference.

If you're ready to develop a comprehensive cyber incident response plan but don't know where rto start, there are experts who can help. **Trend Service One**™ augments your existing security teams with 24/7 managed detection, response, and support—including assistance from Trend Micro's global Incident Response Team.