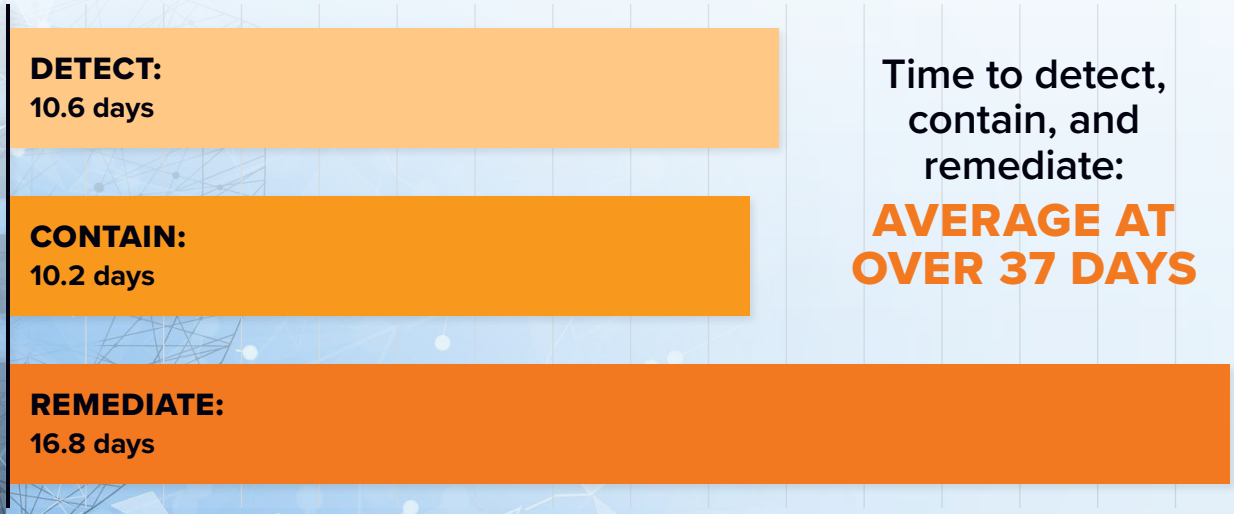
IDC ANALYZE THE FUTURE

Enabling Enterprise Resiliency Through Cyberthreat Detection

Utilizing predictive analytics, machine learning, anomaly detection, threat intelligence and threat hunting can enhance threat detection.

On average or from your most recent breach/incident, how long did it take your security service provider to detect, contain, and remediate?



Source: IDC, MSSP & MDR Survey, May 2020 | Base = respondents experienced a security breach in the last 12–24 months
Note: Managed by IDC's Quantitative Research Group | Note: data not weighted | n = 370; U.S. respondents only

Cyber-resilience is impossible to attain if attacks that are launched against an enterprise are not regularly detected in a timely manner. Unfortunately, the metric used for the length of time an attack can go without detection is not currently identified in seconds or minutes, but rather in days, weeks and even months.

A key aspect of cyber-resiliency is the timely identification, prioritization and remediation of threats, risks or even business adversity. An enterprise that has the capability to use modern technology (e.g., predictive analytics, AI and machine learning) to detect risk and threats to the business can better support an agile and adaptive enterprise resiliency approach.

As we look for ways to support a resilient enterprise approach, the combination of predictive analytics, machine learning and anomaly detection is a powerful new way where we are able to balance the human and machine relationship in order to drive better outcomes, such as reducing time to detect and respond to the threats. Gaining visibility into the various telemetry surfaces such as cloud, email, mobile and remote locations where data is produced and consumed is imperative to correlate any anomalies that might indicate an attack is underway.

Raise Enterprise Resiliency with Threat Hunting

Utilization of a complete threat intelligence program that provides a holistic view of potential, current, and prior adversaries is a key enabler of detecting and properly responding to cybercriminals. Understanding the historical and potential tactics as well as the likely threat vectors that the attacker might utilize is invaluable. This over-the-horizon view can help an enterprise identify what systems and assets are at the highest risk, driving the proactive responses such as determining which systems require immediate patching.

For those attacks that manage to slip through without detection, a strong threat hunting program can help raise enterprise resiliency by eliminating known and unknown threats that exist within the environment.

The term "threat hunting" is a combination of three different types of threat hunting:

Proactive
This approach is driven around a hypothetical analysis of the tactics, techniques, and procedures (TTPs) of a likely adversary and hunting around a likely area of compromise.

Targeted
This approach is focused on the high-value assets of an organization.

Reactive
By utilizing indicators of compromise (IOCs), security analysts will seek to eradicate identified malware and then search for additional remnants.

Of the three types of threat hunting, reactive hunting is the most heavily used when a threat is detected to ensure that the particular malware, email message, or other type of threat does not exist elsewhere within the organization. On the other hand, proactive and targeted hunting are used to uncover the threats that were able to get past the other frontline defenses.

Implementing the five key elements of cyberthreat detection — predictive analytics, machine learning, anomaly detection, threat intelligence and threat hunting — support organizations in becoming cyber-resilient. These key elements also support the overarching goal of the enterprise becoming more resilient as a whole.