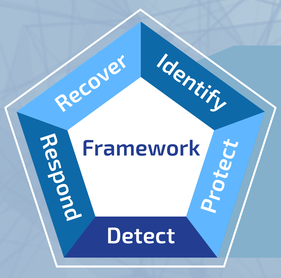
LMNTRIX
BE THE HUNTER I NOT THE PREY

How Cybersecurity Works



Modern Cybersecurity Framework

Modern cybersecurity frameworks consist of five concurrent and continuous Functions that define how your defenses against cyber threats work. Such a framework comprises best practices, standards and recommendations for an organization to improve its cybersecurity practices. When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk.

Identify and Protect

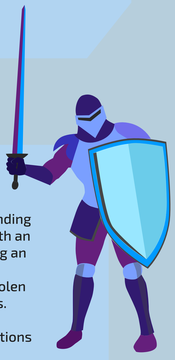
In this step, you try to identify and protect your digital assets against all known and unknown threats. Measures include not only AV software and firewalls but also anti-spam and anti-phishing protection as well as identity management to prevent unauthorized access.

Researchers find 350,000 new pieces of malware each day with 10 billion attacks a year being reported by companies worldwide.

Detect

Detection finds malware and attackers that penetrate your perimeter controls or hide in your network. The use of advanced techniques such as Threat Intelligence, Adversary Hunting, Adaptive Response, Analytic Monitoring, and Deceptions requires collaborating with an advanced Managed Detection & Response (MDR) vendor such as LMNTRIX. Detecting ransomware early with help from an MDR vendor can save you millions.

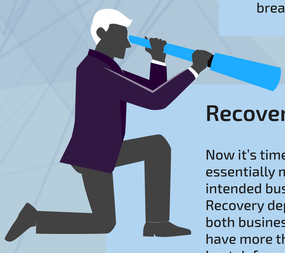
Ransomware payments are totaling around $1 billion a year and also rank as the malware that is detected too late by in-house security teams.



Respond

An effective response strategy usually involves spending millions building internal capability or partnering with an advanced MDR vendor like LMNTRIX, since containing an attack within your network, containing the threat, preventing the spread of malware and recovering stolen data is an overwhelming task for most organizations. Response also includes actions to identify what the attacker did while inside your perimeter and notifications to affected parties.

An IBM reports reveals that the average time to identify a breach in 2019 was 206 days.



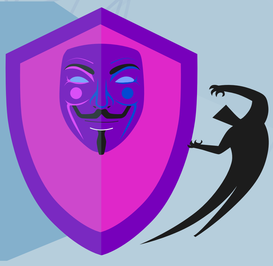
Recover

Now it's time to get your business cyber resilient. This essentially means your ability to continuously deliver the intended business outcomes, despite adverse cyber events. Recovery depends largely on your approach to backing up both business-critical data and operational data as well as to have more than one data backup option. For instance, the sole best defense against ransomware is up to date data backup along with early detection. Recovery is the main component of any business continuity plan.

The average cost of a data breach stands at $3.92 million in 2019.

Be The Threat Actor

Although not part of any framework, agile cybersecurity functions employ real-world scenarios to augment standard controls testing. Unannounced red teaming (not penetration testing) focused on gaining an understanding of the real state of cybersecurity readiness is a common method. As organizations begin to think like a threat actor, they may do a more effective job designing defenses, prioritizing their deployment and devising test activities to assess the effectiveness of those defenses against the real-world threats.



The number of malware detections by businesses worldwide grows by 13% in 2019.

Holistic Approach

Modern cybersecurity requires a holistic approach where all IT security concepts and steps blend together to produce viable results. The nature of today's cyber threats does not allow for omitting a single step or thinking that you will not be a target because your business is too small or very well protected.

LMNTRIX
BE THE HUNTER I NOT THE PREY