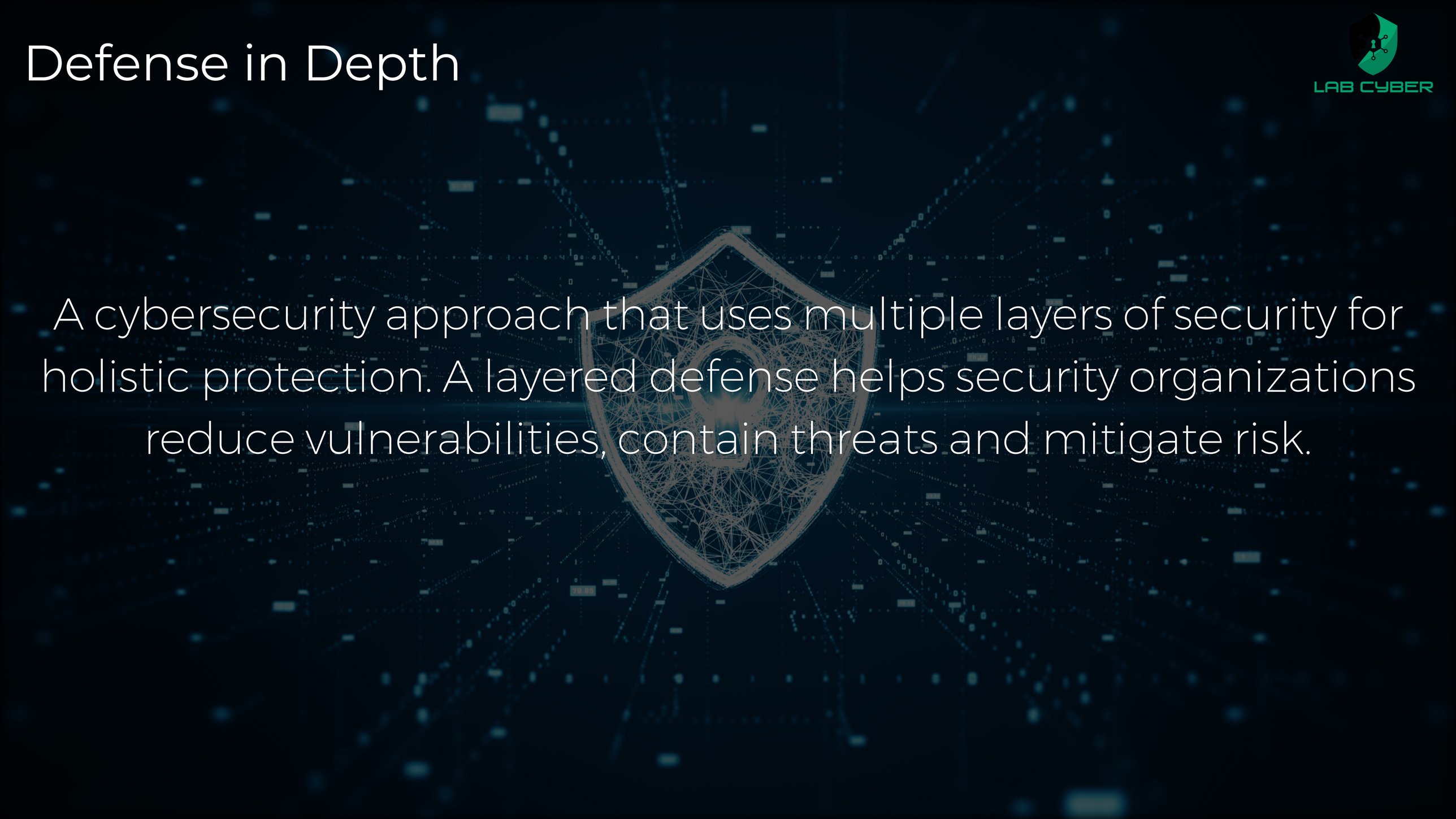
SECURITY CONTROLS IMPLEMENTATION

Security Controls

There should be several layers of protection and multiple security controls used

Defense in Depth

LAB CYBER



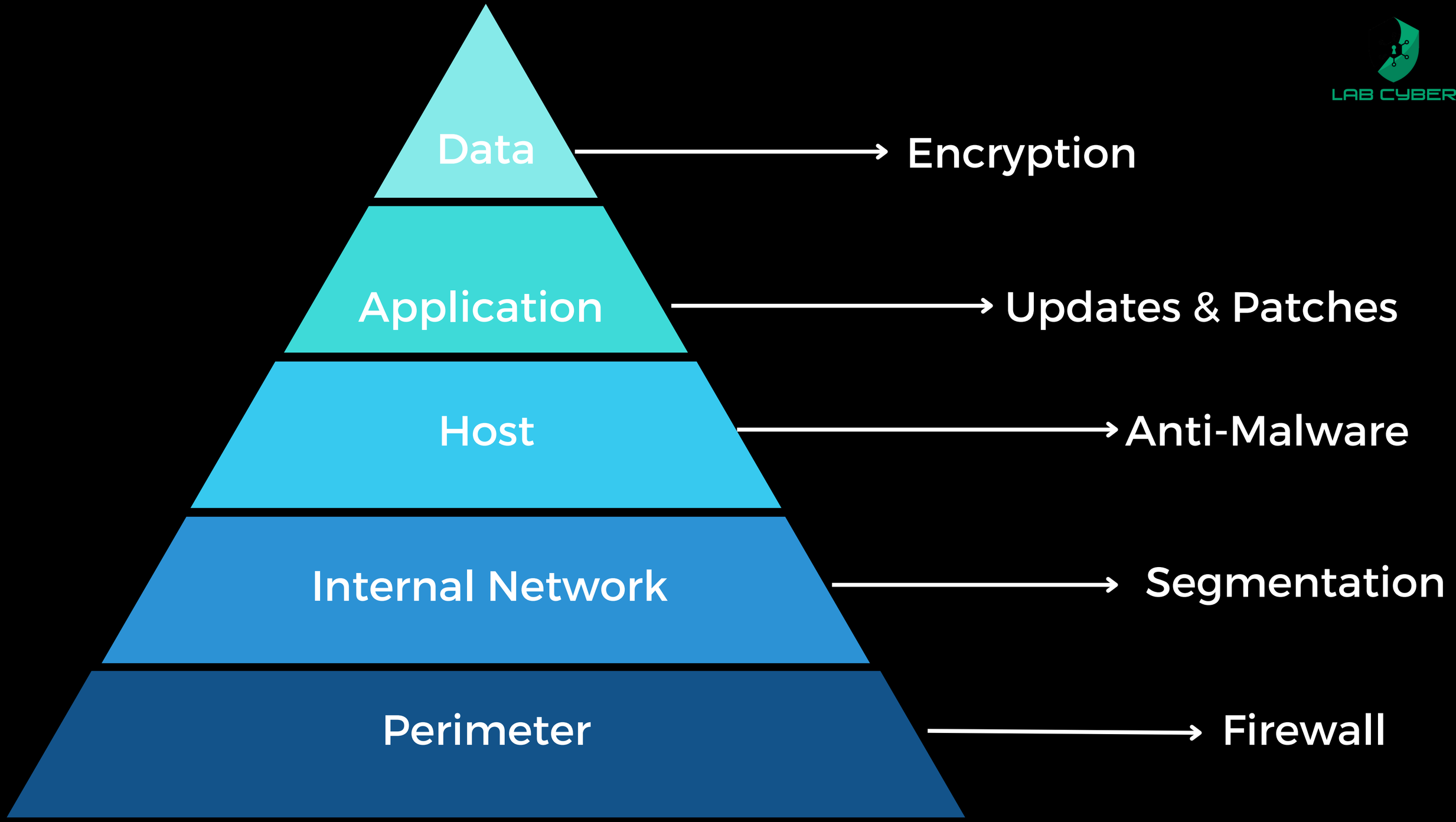
A cybersecurity approach that uses multiple layers of security for holistic protection. A layered defense helps security organizations reduce vulnerabilities, contain threats and mitigate risk.

Defense in Depth

The primary goal is to ensure that there is no single point of security failure

Defense in Depth

Make it as hard as possible to get hacked


Data
Encryption
Application
Updates & Patches
Host
Anti-Malware
Internal Network
Segmentation
Perimeter
Firewall

Defense in Depth

LAB CYBER

Even more defence

- Backups
- Data Access monitoring
- Security Policy

Defense in Depth Controls

LAB CYBER

1

PREVENTION/PROTECTION

2

DETECTION

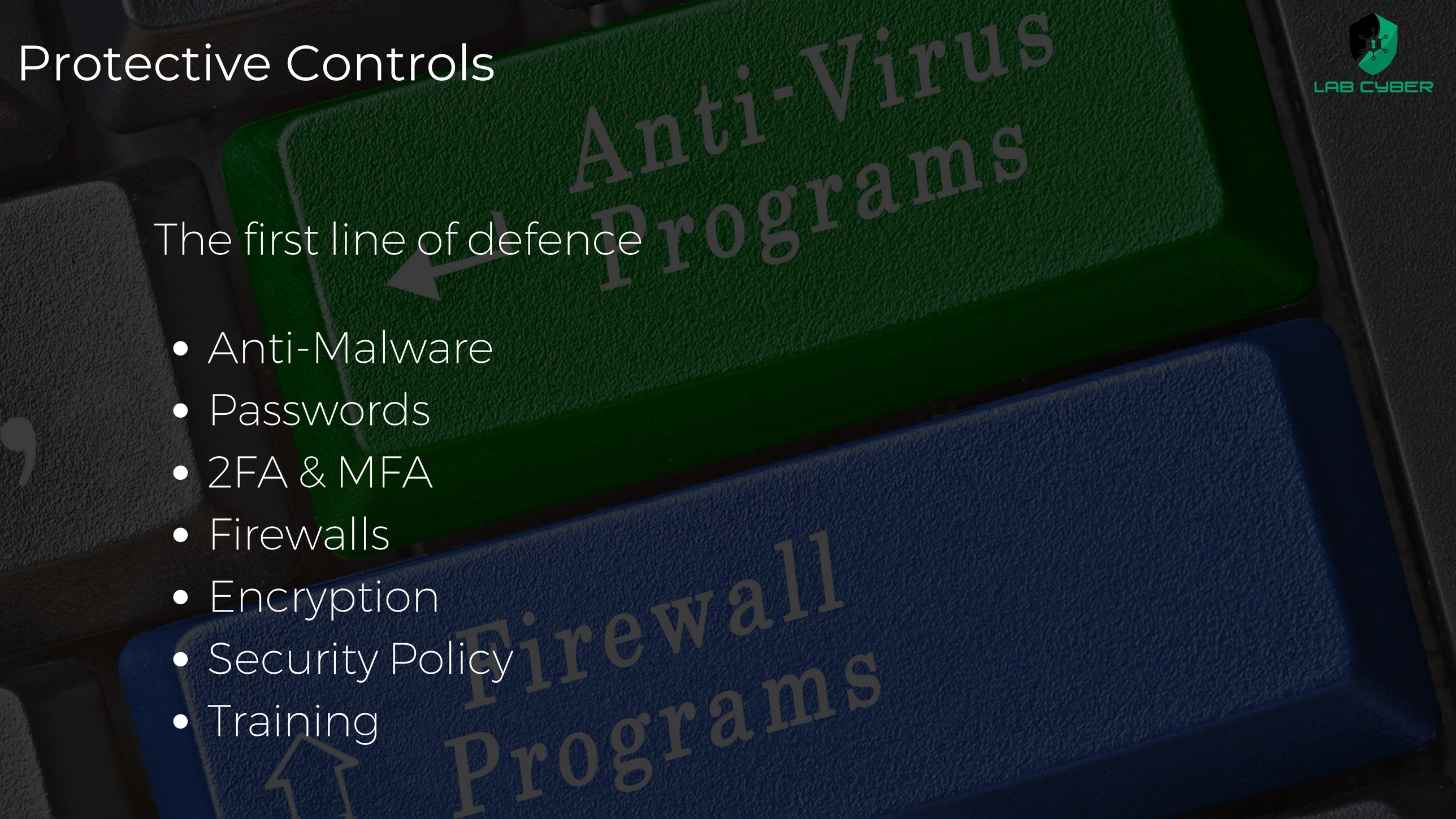
3

SLOW DOWNS

4

RECOVERY

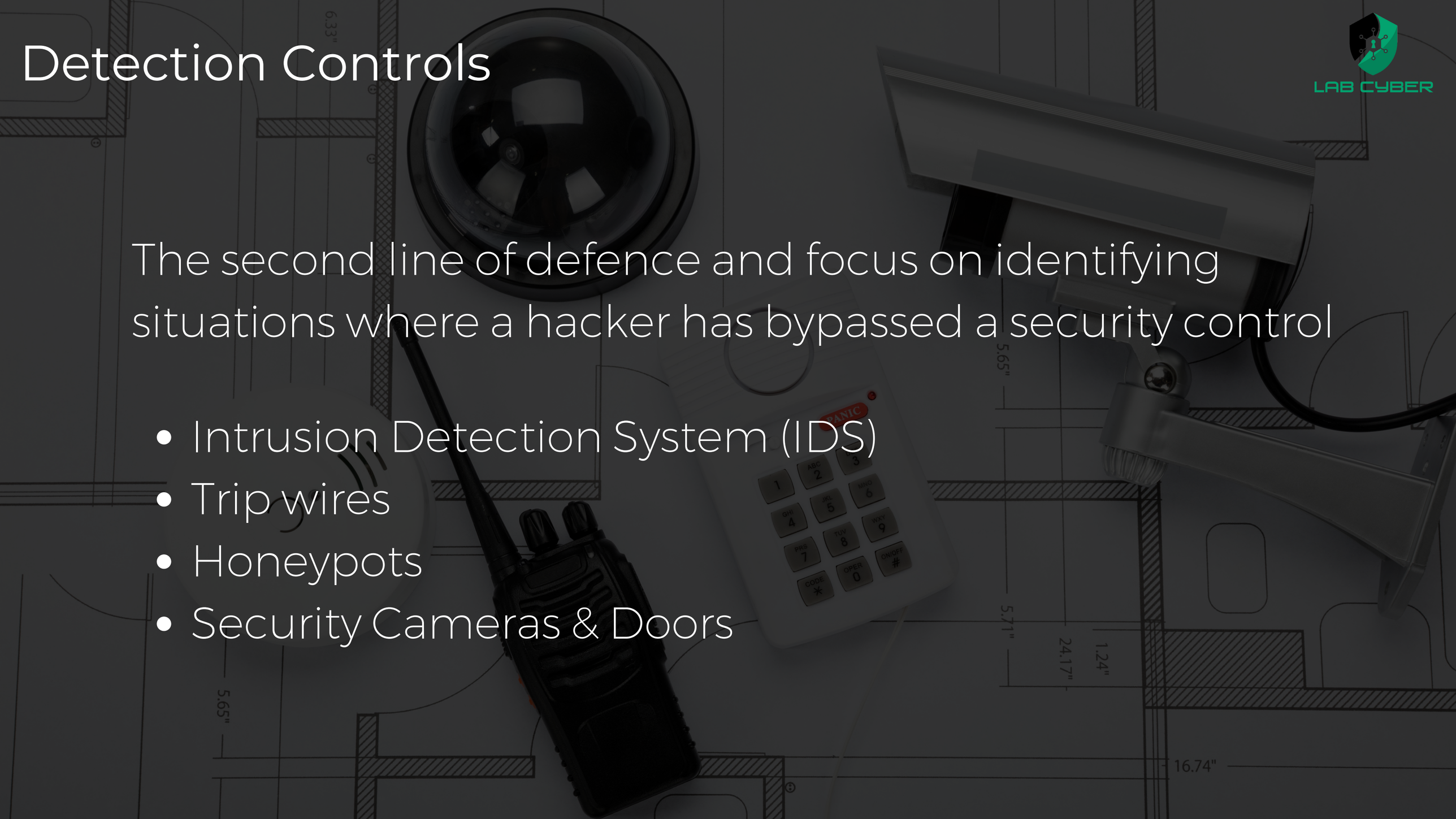
Protective Controls



The first line of defence

- Anti-Malware
- Passwords
- 2FA & MFA
- Firewalls
- Encryption
- Security Policy
- Training

Detection Controls



The second line of defence and focus on identifying situations where a hacker has bypassed a security control

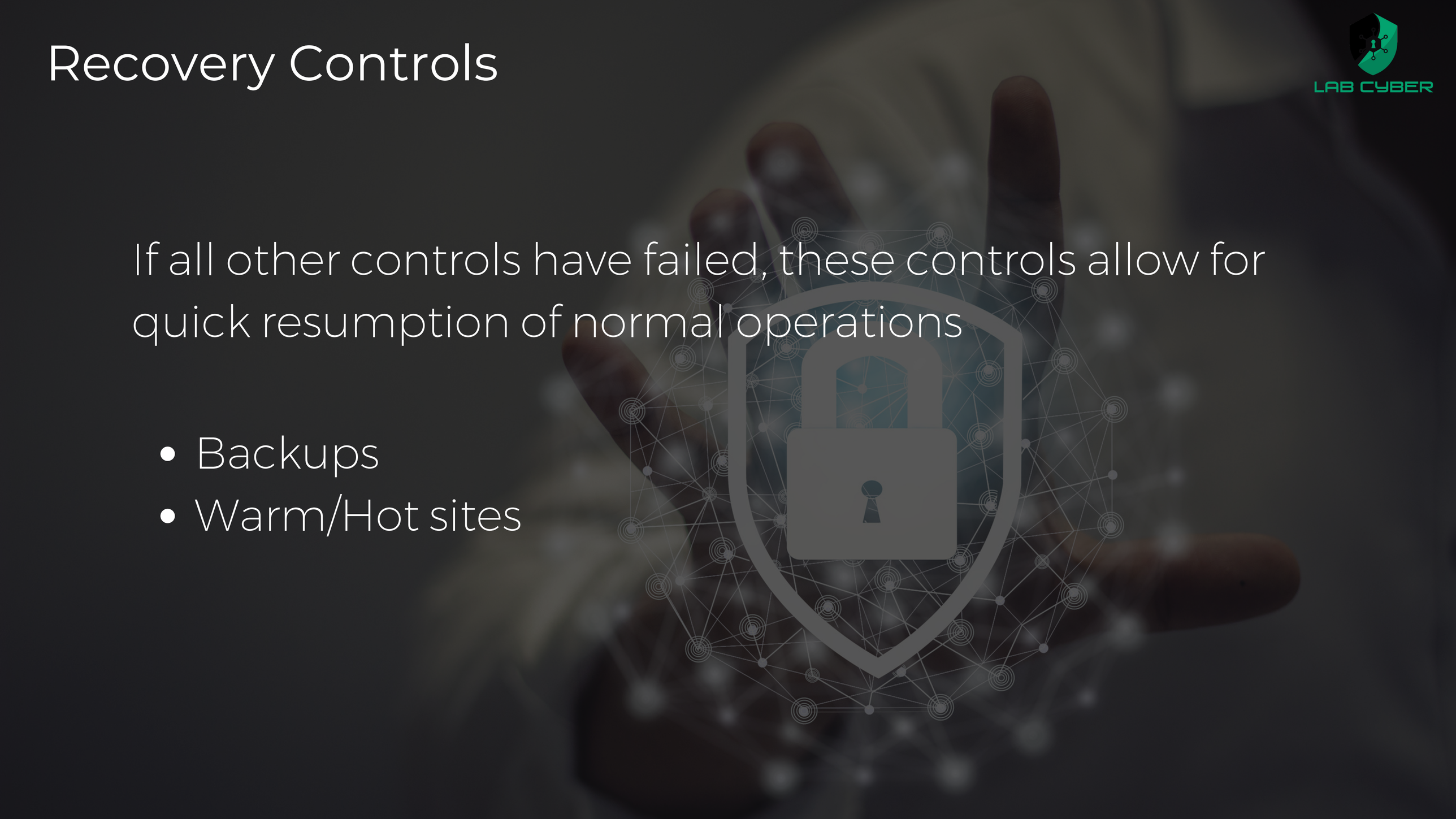
- Intrusion Detection System (IDS)
- Trip wires
- Honeypots
- Security Cameras & Doors

Slow Down Controls

Designed to impede the amount of damage a hacker can cause after successfully gaining entry

- Obfuscation (renaming important files)
- Time outs
- Large files transfer control

Recovery Controls



If all other controls have failed, these controls allow for quick resumption of normal operations

- Backups
- Warm/Hot sites