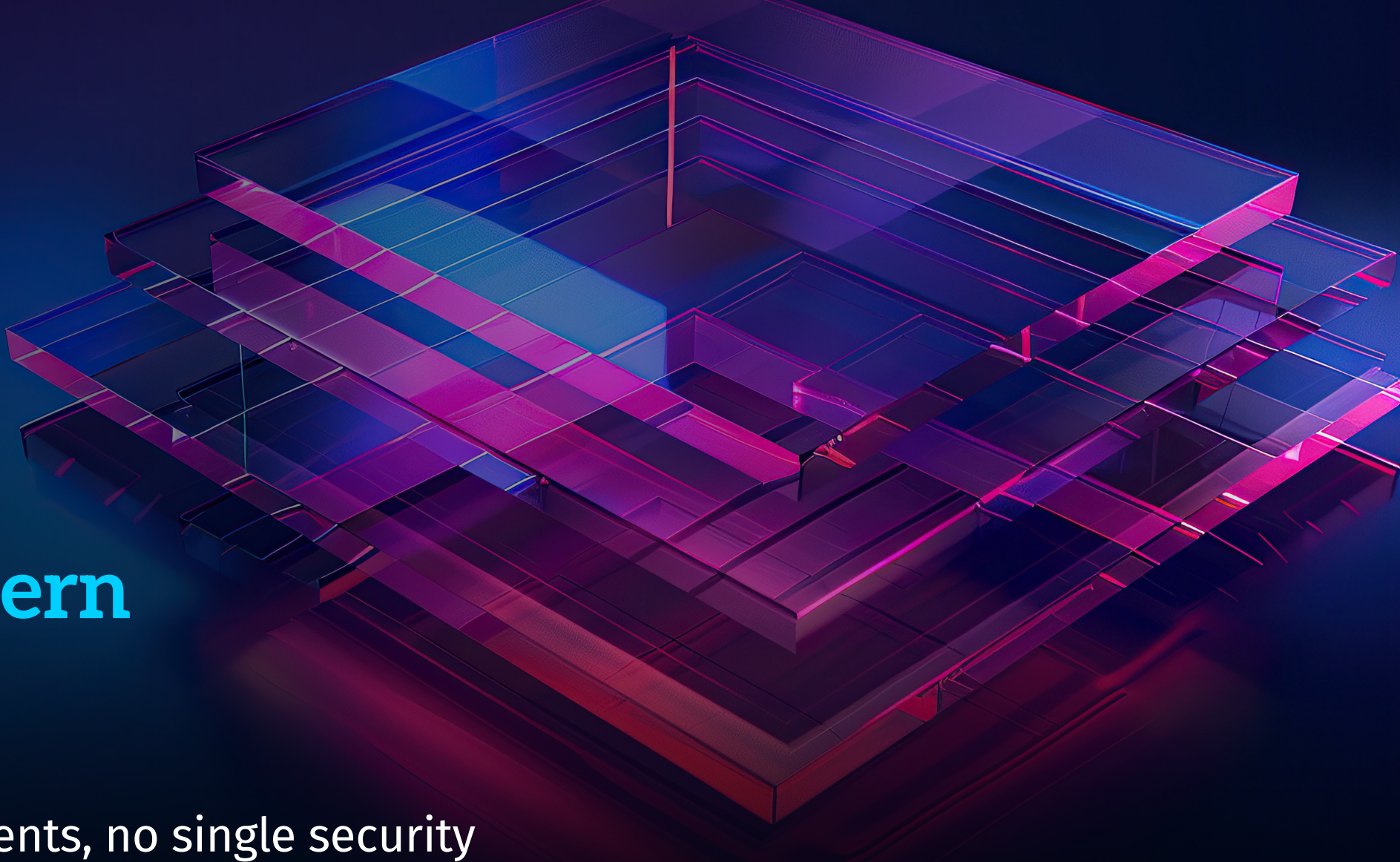




Defense in Depth—A Modern Cybersecurity Mandate

In a world of complex, distributed IT environments, no single security control is enough. Defense in Depth (DiD) applies multiple, overlapping layers of protection—from firewalls and identity management to monitoring and response—to reduce risk and improve resilience.

Key Topics



Why DiD Still Matters

Cyberattacks are a matter of when—not if. DiD ensures that if one layer fails, others are in place to prevent, detect, and respond to threats effectively. It turns reactive security into proactive resilience.



Core Principles

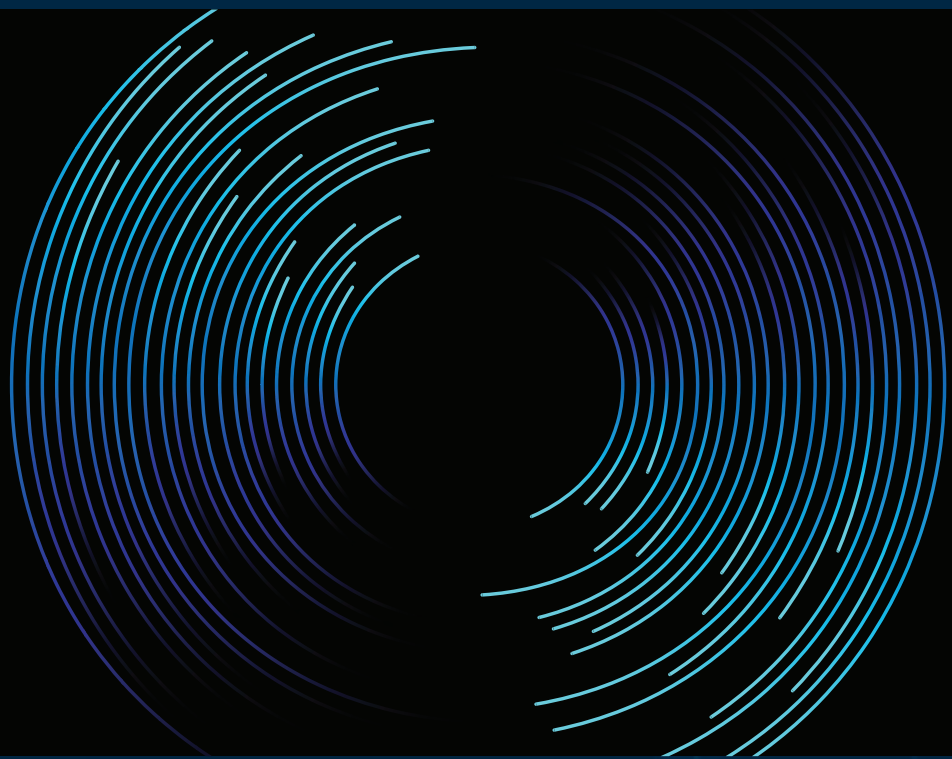


Strategic Implementation



Types of Security Controls

- Preventive**
Firewalls, encryption, access controls
- Detective**
SIEM, intrusion detection, audit logs
- Corrective**
EDR, SOAR, incident response plans



The Zero Trust Connection

Zero Trust builds on DiD: “Never trust, always verify.” Even internal users and devices must be authenticated and continuously monitored.

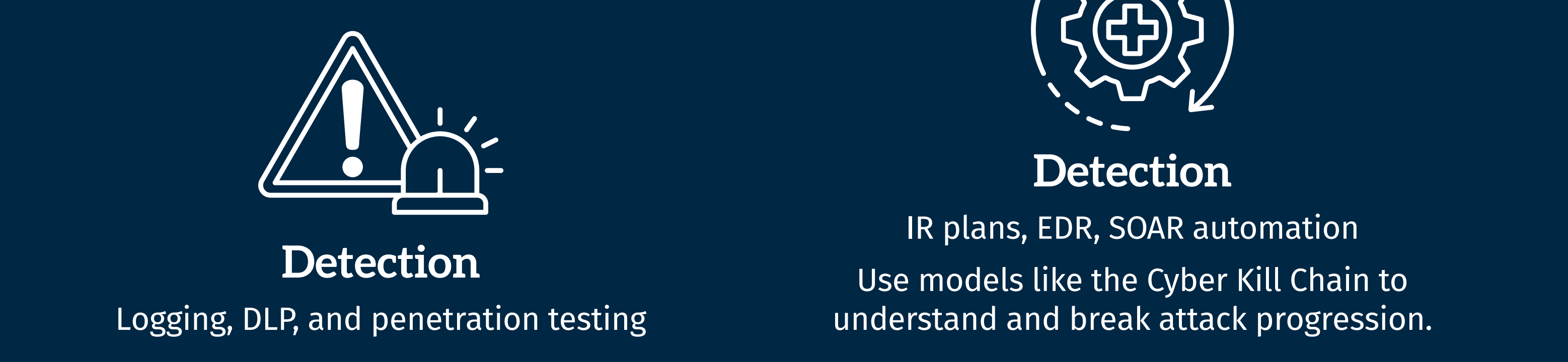
Cloud Considerations

- Shared Responsibility**
Define and manage roles clearly
- Identity as Perimeter**
Enforce authentication and MFA
- Cloud Logging**
Enable complete visibility
- Tools**
CASBs, Remote Browser Isolation, and native cloud security services

Endpoint Security



Detection & Response



Bottom Line for Executives

DiD is not about complexity—it’s about resilience. With layered protection across systems, cloud, and endpoints, DiD empowers organizations to reduce risk, protect assets, and respond with confidence.