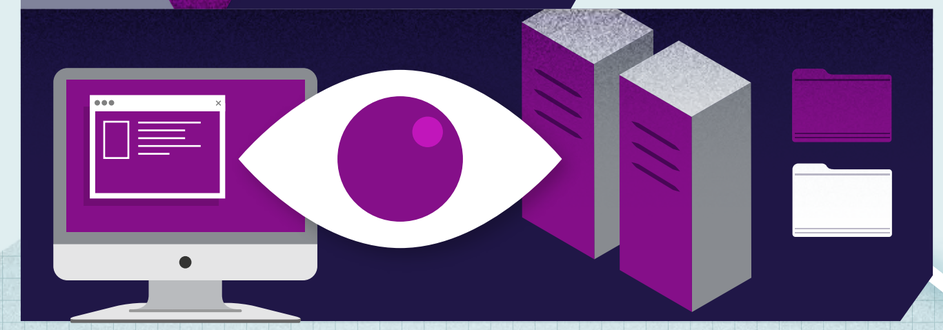
leidos

NIST Cybersecurity Framework

1 IDENTIFY

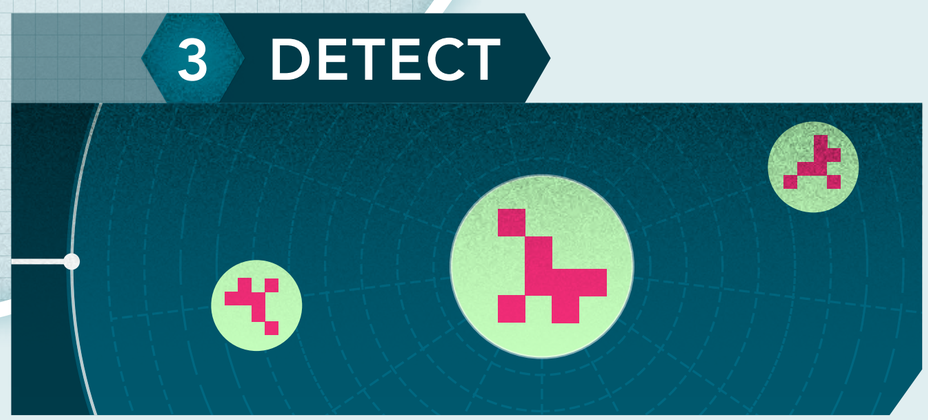


Identification forms the basis for understanding an organization's infrastructure. When the organization IDs how systems and infrastructure align to business objectives, risk decisions have more positive impact.

2 PROTECT

Protection against cyberattacks includes traditional forms of information assurance capabilities, along with training, policies and procedures.

3 DETECT

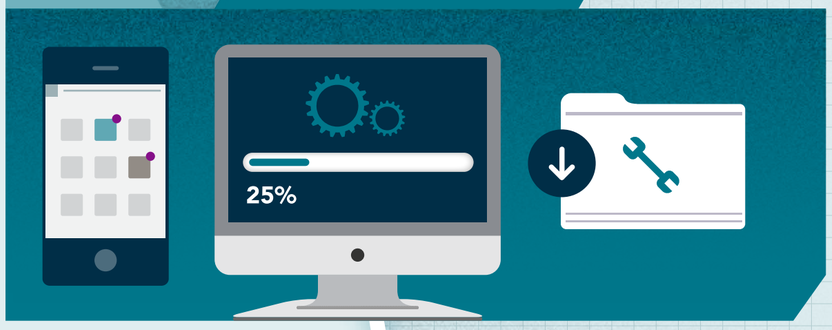


Detection focuses on rapid discovery of cyber incidents and is most effective when utilizing advanced analytical techniques. Done right, it helps fight cyberattacks by anticipating them before they start.

4 RESPOND

Response is triggered when a cyber incident is imminent or active. The ability to continue operations uninterrupted during a cyber event is a key performance indicator for success.

5 RECOVER



Recovery requires determining what's needed to support a return to normal operations, including disaster recovery, continuity of operations and effective communications.