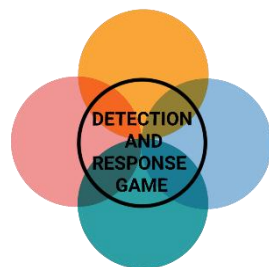
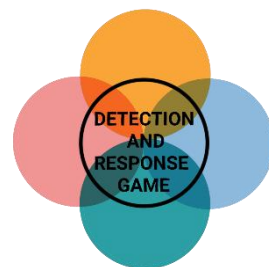


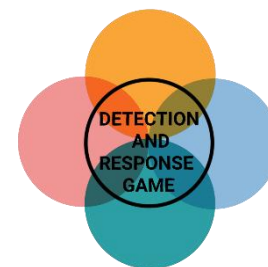
LATERAL
MOVEMENT, C2,
EXFILTRATION



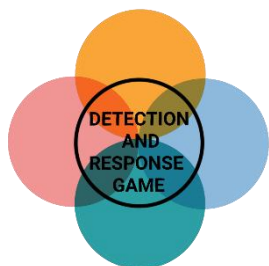
LATERAL
MOVEMENT, C2,
EXFILTRATION



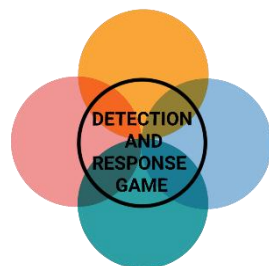
LATERAL
MOVEMENT, C2,
EXFILTRATION



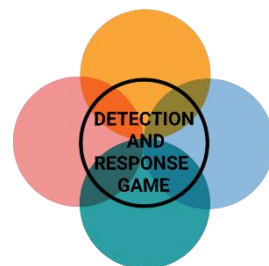
LATERAL
MOVEMENT, C2,
EXFILTRATION



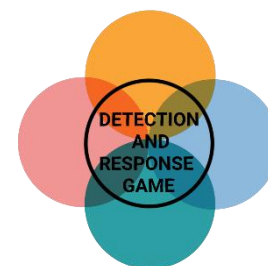
LATERAL
MOVEMENT, C2,
EXFILTRATION



LATERAL
MOVEMENT, C2,
EXFILTRATION



LATERAL
MOVEMENT, C2,
EXFILTRATION



LATERAL
MOVEMENT, C2,
EXFILTRATION

SSH HIJACKING

The hacker hijacks a legitimate user's SSH session to move laterally within an environment.

PREVENTION

Disable agent forwarding

DETECTION

Monitor user SSH-agent socket files

PASS THE HASH

The hacker uses Mimikatz to authenticate himself as a user without having the clear text password.

PREVENTION

Enable pass the hash mitigations

DETECTION

Monitor for lsass.exe

EXFILTRATION OVER USB

The hacker tries to move data between two disconnected networks using a USB device.

PREVENTION

Limit the use of USB devices

DETECTION

Monitor file access on removable media

TRAFFIC DUPLICATION

The hacker uses traffic mirroring to exfiltrate data over an already compromised network.

PREVENTION

Encrypt sensitive information

DETECTION

Monitor network traffic for uncommon data flows

MAIL PROTOCOLS

The hacker uses electronic mail delivery for unnoticed communication such as SMTP or POP3.

PREVENTION

Network intrusion detection

DETECTION

Analyze network data for uncommon data flows

NON-STANDARD PORT

The hacker does not use conventional ports (port 587) to communicate via HTTPS.

PREVENTION

Network intrusion detection

DETECTION

Analyze packet contents

WEB PROTOCOLS

The hacker uses web traffic protocols for unnoticed communication such as HTTP or HTTPS.

PREVENTION

Network intrusion detection

DETECTION

Analyze network data for uncommon data flows

VBA STOMPING

The hacker hides Visual Basic for Application payloads within MS Office documents.

PREVENTION

Restrict access to unneeded VB components

DETECTION

Detection for p-code