Executive Leadership & Board Questions Regarding CYBER SECURITY

ABOUT THIS PRESENTATION

SAT IN ON MANY BOARD MEETINGS

QUESTIONS ASKED AFTER A BREACH

I BECAME A BOARD MEMBER

QUESTIONS ARE OFTEN NEVER ASKED?

EXEC LEADERSHIP ASSUMES I.T. IS FINE

EXEC LEADERSHIP GETS LOST IN THE TECH SPEAK

EXEC LEADERSHIP INTIMIDATED BY TECHNOLOGY

GOVERNANCE
&
LEADERSHIP OVERSIGHT

GOVERNANCE & LEADERSHIP OVERSIGHT

MAKE SURE CYBER SECURITY IS VEIWED AS…

1. VIEW AS AN ENTERPRISE RISK
2. HAVE IT COVERED AT BOARD MEETINGS
3. PROVIDE THE CISO/EXEC & BOARD VISIBILITY
4. CYBER SECURITY RESPONSIBILITIES ASSIGNED
5. POLICIES ARE REVIEWED & ACKNOWLEDGED

INCIDENT RESPONSE
&
RESILIENCE

INCIDENT RESPONSE & RESILIENCE

MAKE SURE YOU BRING UP THE FOLLOWING…

1. MAKE SURE A PLAN EXISTS AND MAINTAINED
2. LEADERSHIP PARTICIPATES IN EXERCISES
3. PERFORM A RANSOMWARE SCENARIO
4. BACKUPS ENCRYPTED & IMMUTABLE
5. PERFORM A DISASTER RECOVERY TEST

DATA PROTECTION & PRIVACY

DATA PROTECTION & PRIVACY

MAKE SURE YOU BRING UP THE FOLLOWING…

1. IS SENSITIVE DATA CLASSIFIED AND PROTECTED
2. ARE WE ENCRYPTING DATA (AT REST & TRANSIT)
3. DATA RETENTION REQUIREMENTS DEFINED
4. BREACH NOTIFICATION PROCEDURES

HUMAN RISK
&
SECURITY CULTURE

HUMAN RISK AND SECURITY CULTURE

MAKE SURE YOU BRING UP THE FOLLOWING…

1. TRAIN EMPLOYEES AND MAKE IT RELEVANT
2. USE SIMULATIONS AND/OR LIVE SESSIONS
3. PROVIDE EXECS WITH SPECIALIZED TRAINING
4. TRAINING EMPLOYEES ON HOW TO REPORT
5. INSIDER THREATS ARE MONITORED

METRICS & REPORTING

METRICS AND REPORTING

MAKE SURE YOU PROVIDE…

1. MEANINGFUL CYBER SECURITY METRICS
2. VULNERABILTIES ARE TRACKED TO REPAIR
3. INCIDENT REPONSE READINESS IS MEASURED
4. BACKUP RECOVERY TESTING IS MEASURED
5. INDEPENDENT SECURITY TESTING PERFORMED

SECURITY OPERATIONS
&
TECHNICAL CONTROLS

SECURITY OPERATIONS & TECH. CONTROLS

MAKE SURE THE FOLLOWING ARE COVERED...

1. CRITICAL SYSTEMS & CRITICAL DATA IDENTIFIED
2. CYBER RISKS ARE PRIORITIZED BY BUSINESS
3. RISK ACCEEPTANCE DECISIONS DOCUMENTED
4. THIRD PARTY VENDOR RISKS ARE ACCESSED
5. REVIEW AND UPDATE CYBER INSURANCE / YR

SECURITY OPERATIONS & TECHNICAL CONTROLS

The Granular Questions That Speak the Truth

SECURITY OPERATIONS & TECH. CONTROLS

QUESTION WILL EXPOSE A POSSIBLE CONCERN

Microsoft Active Directory

IS ACTIVE DIRECTORY CLEANED UP?

SECURITY OPERATIONS & TECH. CONTROLS

RESPONSES WILL PROVIDE A PULSE ON SECURITY HARDNESS ...

Microsoft Active Directory

REMOVE OLD ACCOUNTS

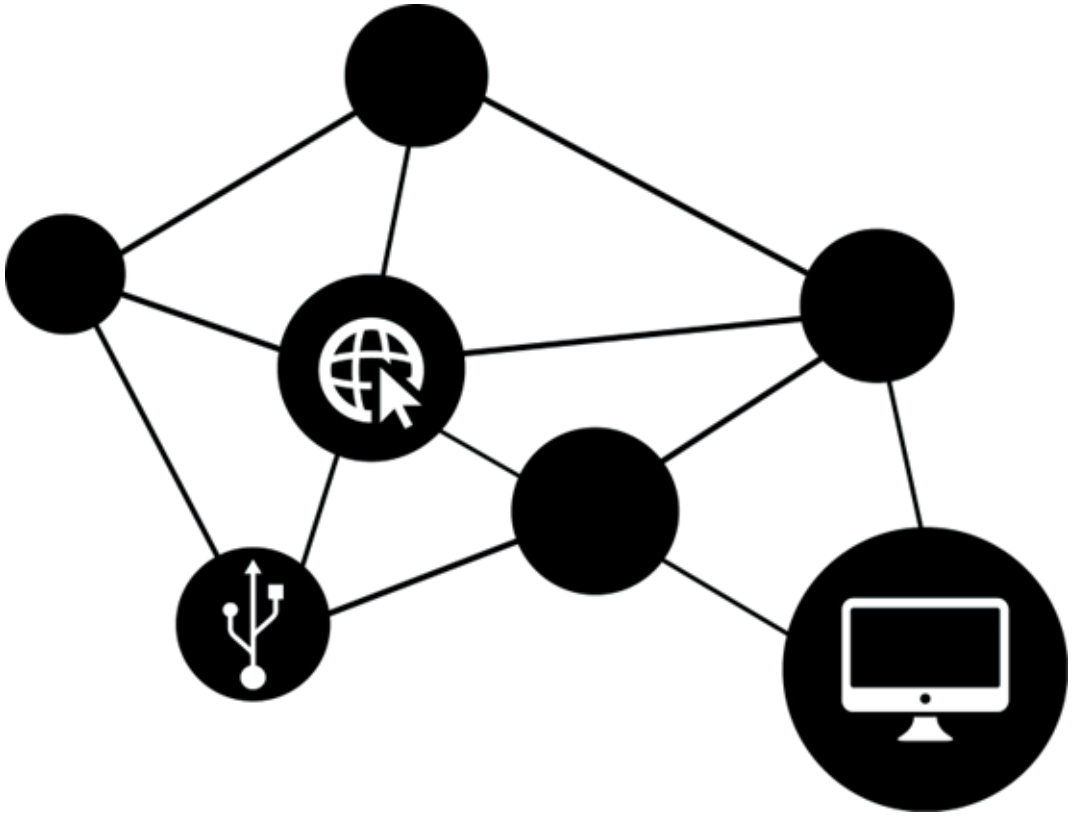
ENFORCE LEAST PRIVLEDGES

POLICE DOMAIN ACCOUNTS

ARE WE STAYING ON TOP OF THIS

SECURITY OPERATIONS & TECH. CONTROLS

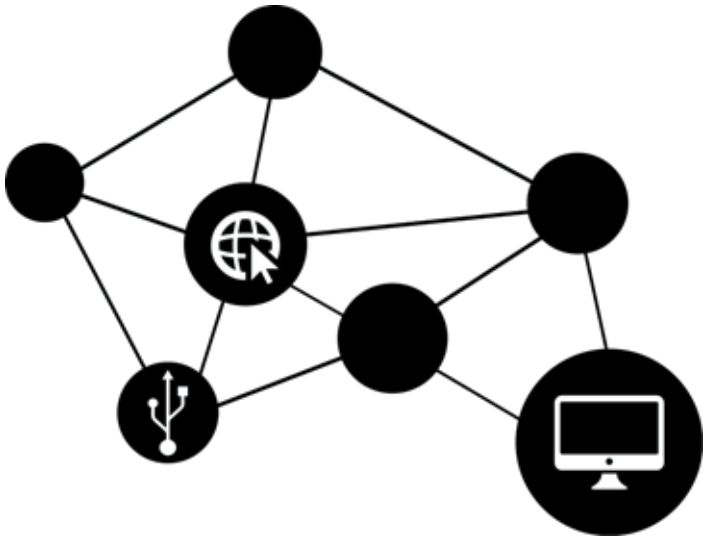
QUESTION WILL EXPOSE A POSSIBLE CONCERN



DID WE SEGMENT THE NETWORK?

SECURITY OPERATIONS & TECH. CONTROLS

RESPONSES WILL PROVIDE A PULSE ON SECURITY HARDNESS …



SILO SENSITIVE AREAS

LIMIT PRIVILEDGE TO THEM

ENABLE NAC IF POSSIBLE

MONITOR THE SEGMENTS

SECURITY OPERATIONS & TECH. CONTROLS

QUESTION WILL EXPOSE A POSSIBLE CONCERN

LOCATE & HARDEN ALL DATA STORES

SECURITY OPERATIONS & TECH. CONTROLS

RESPONSES WILL PROVIDE A PULSE ON SECURITY HARDNESS …

LOCATE WHATS IMPORTANT

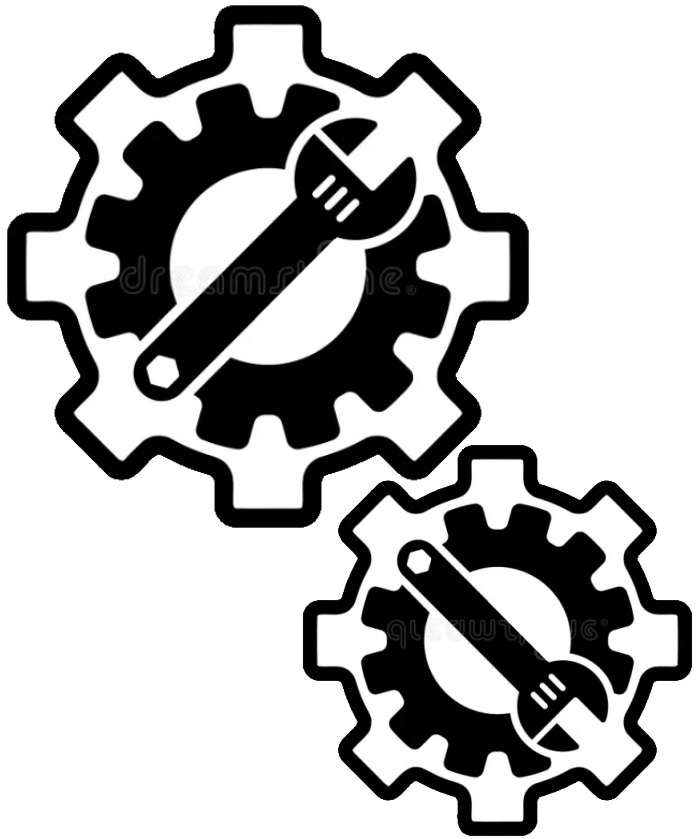
LOCKDOWN ACCESS TO IT

ENCRYPT IF POSSIBLE

POLICE BAD PRACTICES

SECURITY OPERATIONS & TECH. CONTROLS

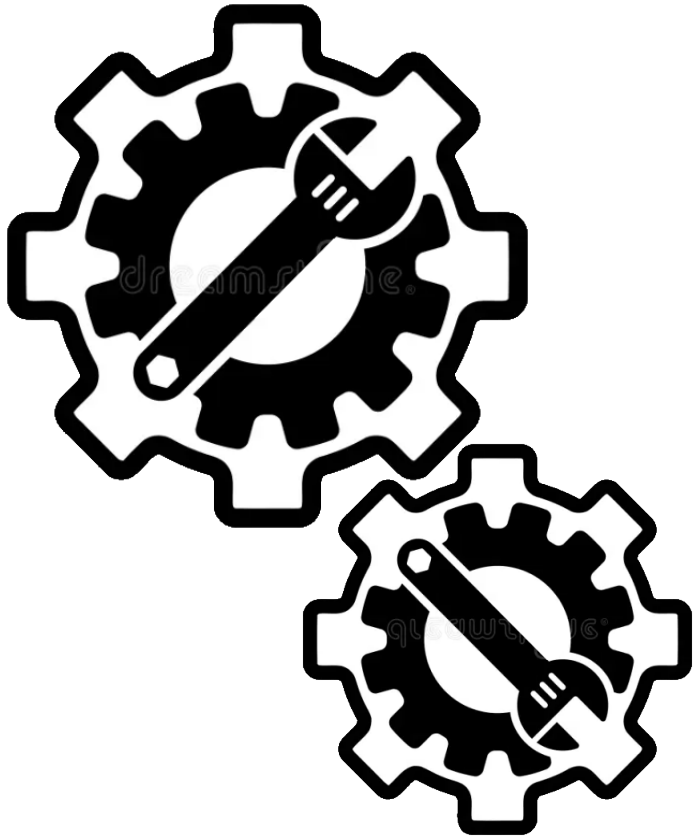
QUESTION WILL EXPOSE A POSSIBLE CONCERN



STRIP DEVICES OF ALL DEFAULT CONFIGS

SECURITY OPERATIONS & TECH. CONTROLS

RESPONSES WILL PROVIDE A PULSE ON SECURITY HARDNESS …



LOCATE WHATS IMPORTANT

LOCKDOWN ACCESS TO IT

ENCRYPT IF POSSIBLE

POLICE BAD PRACTICES

SECURITY OPERATIONS & TECH. CONTROLS

QUESTION WILL EXPOSE A POSSIBLE CONCERN

HAVE WE TESTED ENDPOINT DETECTION

SECURITY OPERATIONS & TECH. CONTROLS

RESPONSES WILL PROVIDE A PULSE ON SECURITY HARDNESS ...

EXAMINE EDR CONFIGS

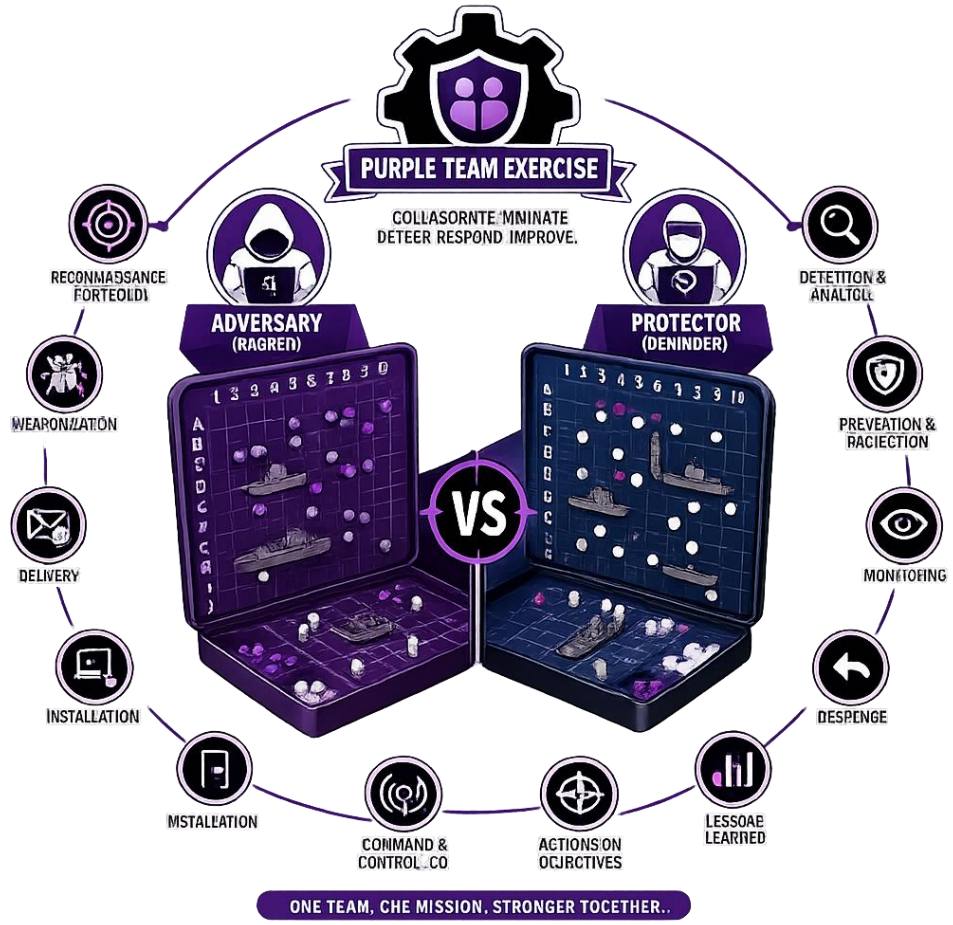
TEST TO BYPASS EDR

REMEDIATE ASAP

HAVE WE TESTED THE MSP

SECURITY OPERATIONS & TECH. CONTROLS

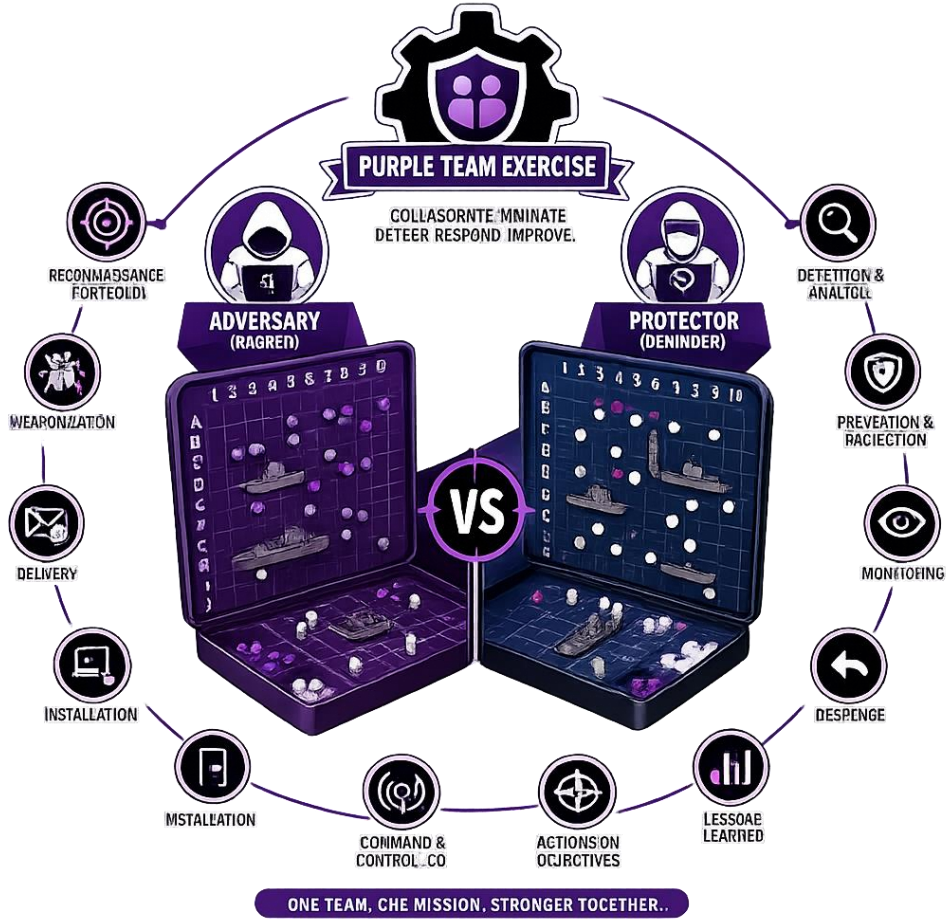
QUESTION WILL EXPOSE A POSSIBLE CONCERN



HAVE WE PERFORMED A PURPLE TEAM EXERCISE

SECURITY OPERATIONS & TECH. CONTROLS

RESPONSES WILL PROVIDE A PULSE ON SECURITY HARDNESS ...



I.T. VS THE AGGRESSOR

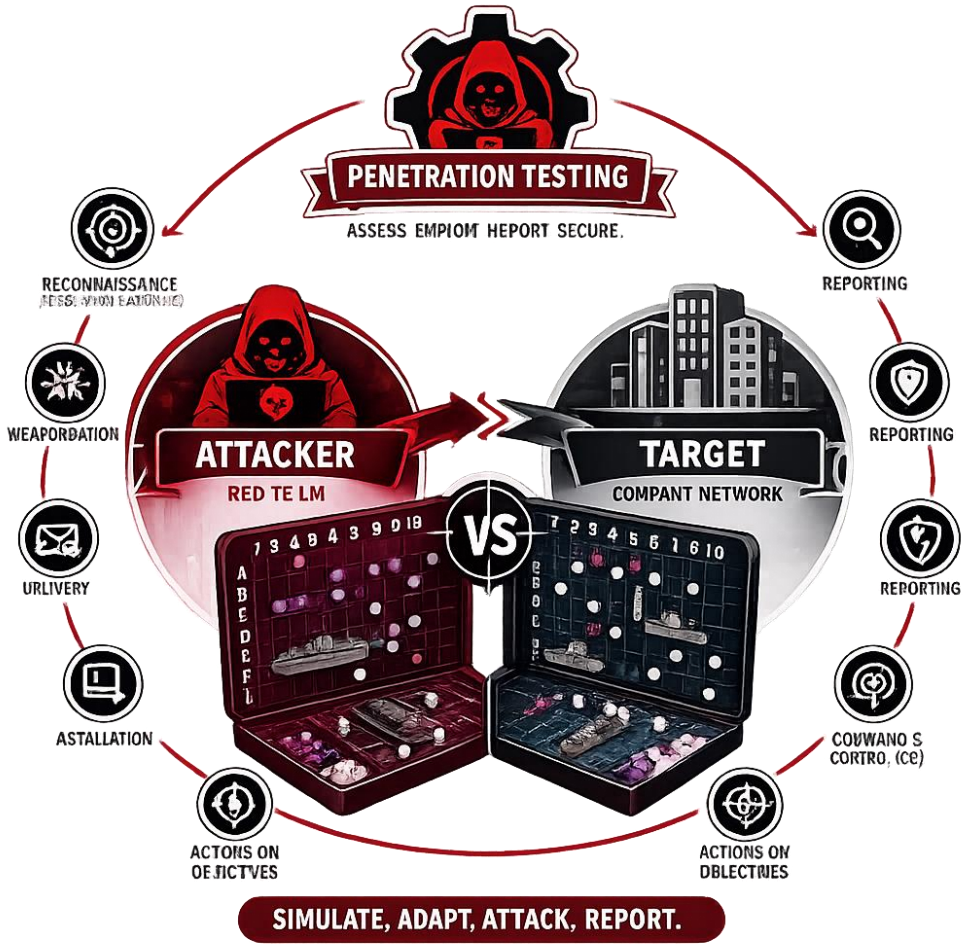
CYBER SEVICES ALTERING

THWARTING ATTACKS

HAVE WE TESTED THE MSP

SECURITY OPERATIONS & TECH. CONTROLS

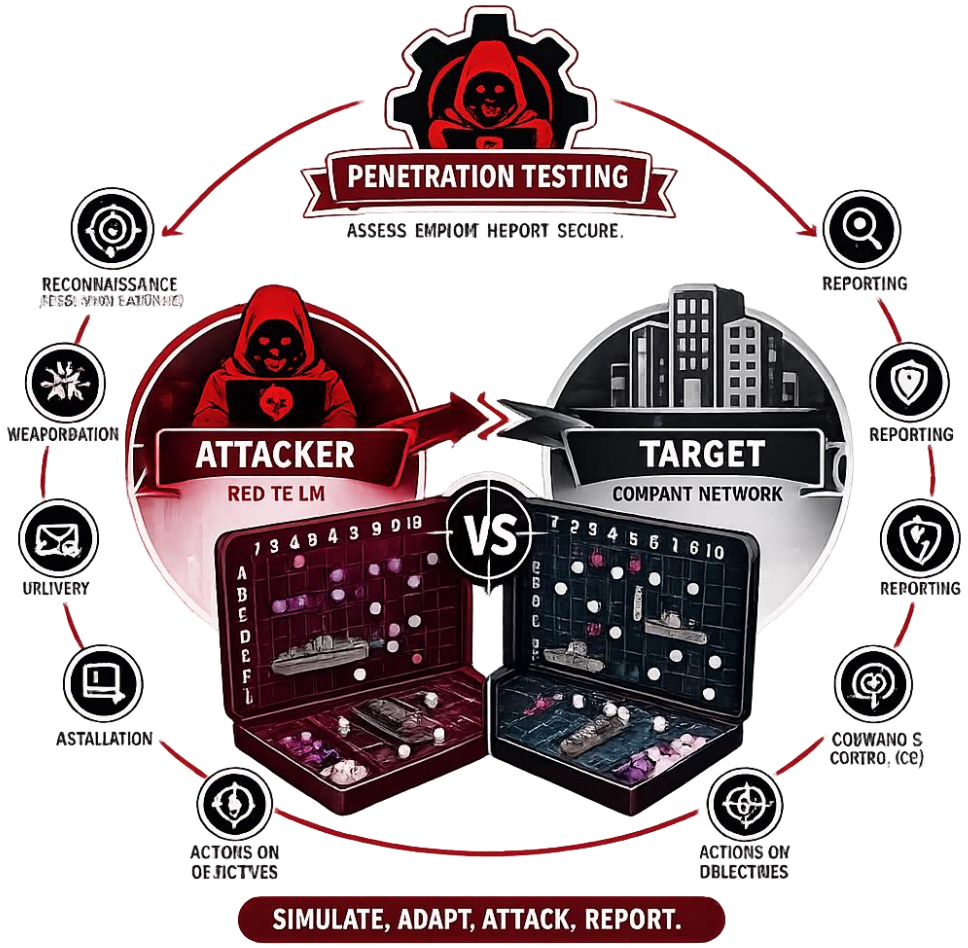
QUESTION WILL EXPOSE A POSSIBLE CONCERN



HAVE WE PERFORMED "REAL" PENETRATION TESTING?

SECURITY OPERATIONS & TECH. CONTROLS

RESPONSES WILL PROVIDE A PULSE ON SECURITY HARDNESS ...



NOT JUST PERIMETER

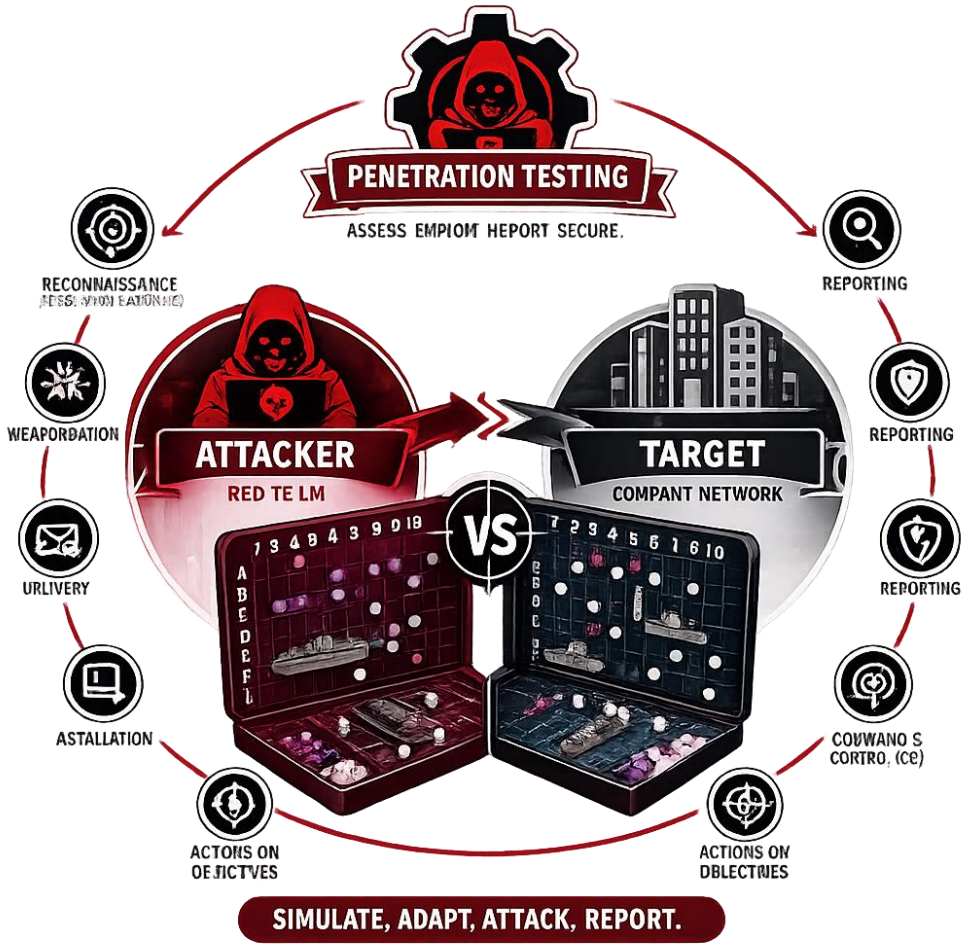
INTERNAL TESTING

NOT JUST A SCAN

ADVERSARY SCENARIOS

SECURITY OPERATIONS & TECH. CONTROLS

RESPONSES WILL PROVIDE A PULSE ON SECURITY HARDNESS ...



HAVE YOU REMEDIATED

HAVE YOU RETESTED

ARTIFICIAL INTELLIGENCE
&
CYBER SECURITY

Ai GOVERNANCE
&
STRATEGIC DIRECTION

Ai Governance & Strategic Direction

RESPONSES WILL PROVIDE A PULSE ON Ai READINESS

Do we have an Ai strategy?

Who owns Ai governance inside the organization

Do we have an Ai acceptable use policy?

DATA PROTECTION
&
INFORMATION LEAKAGE

Ai DATA PROTECTION AND LEAKAGE

Are employees entering sensitive company data into Ai systems?

What types of company data are prohibited from Ai platforms?

Can Ai vendors retain or train on our data?

CYBERSECURITY
&
THREAT LANDSCAPE

Ai CYBER SECURITY AND THREAT LANDSCAPE

How are threat actors using Ai against us?

Could someone convincingly impersonate our executives using Ai?

Are we using AI securely within cybersecurity operations?

REGULATORY, LEGAL & COMPLIANCE RISK

Ai LEGAL AND COMPLIANCE RISKS

Are there legal or regulatory risks tied to our Ai usage?

Are we prepared for future Ai regulations?

Who reviews Ai generated content before it is trusted or released?

BUSINESS CONTINUITY
&
OPERATIONAL RISK

Ai BUSINESS CONTINUITY OPERATIONAL RISK

What happens if our Ai dependent systems fail?

Are employees becoming overly dependent on Ai?

Could Ai create reputational risk for the company?

THIRD PARTY
&
VENDOR RISK

Ai THIRD PARTY & VENDOR RISK

Which Ai platforms are currently being used inside the company?

Have our vendors integrated Ai into products without our knowledge?

Are our contracts protecting us from Ai related vendor risk?

WORKFORCE
&
HUMAN IMPACT

Ai WORKFORCE AND HUMAN IMPACT

Which jobs or functions could Ai significantly change?

Are employees being trained on Ai risks and safe usage?

Are executives specifically being targeted with Ai enhanced fraud?

COMPETETIVE
&
STRATEGIC ADVANTAGE

Ai COMPLIANCE AND STRATEGIC ADVANTAGE

How are competitors using Ai?

Where could Ai provide us the greatest business advantage?

Are we adopting Ai too slowly or recklessly?

ARTIFICIAL INTELLIGENCE & SECURITY OPERATIONS

Ai CYBER SECURITY AND THREAT LANDSCAPE

Could Ai accidentally expose our internal infrastructure or security operations?

Are we validating Ai generated code before deployment?

Are we monitoring Ai usage within the organization?

Artificial Intelligence Questions CEOs Rarely Ask … But Should

Ai CYBER SECURITY AND THREAT LANDSCAPE

Could Ai increase the scale and speed of attacks against us?

Could our own employees unintentionally train attackers?

If we banned Ai tomorrow, could the organization still function competitively?

Ai CYBER SECURITY AND THREAT LANDSCAPE

"How could Ai realistically hurt this company financially, operationally, legally, or reputationally and are we prepared for it?"

36 Ai PROJECTS

30 WERE FAILED PROJECTS

83% FAILURE RATE

QUESTIONS?

STEVE STASIUKONIS
315.579-3373 | Office
315-440-9468 | Mobile
steve@securenetworkinc.com
www.securenetworkinc.com