GRAVOC

g³ gray™

THE POWER OF MORE

How Hackers Think: A Behind-the-Scenes Look at Penetration Testing

Presentation Deck

Date: August 12, 2025

Today’s Agenda

1. What is Pentesting & Why it Matters
2. The Defensive Lifecycle: From Test to Remediation
3. A New Frontier: Artificial Intelligence
4. AI Risk Management
5. Key Takeaways & Q&A

GRAVOC

What We Do:

Penetration Testing

- Active Directory Assessment
- Adversary Simulation
- Cloud Security Assessment
- External PenTest
- Internal PenTest
- Social Engineering Testing
- Web/Mobile App Testing

Governance, Risk, & Compliance (GRC)

- AI Governance Consulting
- Business Continuity Planning
- Disaster Recovery Planning
- Certification Gap Readiness
- Risk Assessment
- Security Awareness
- Tabletop Training
- Virtual vCiso

IT Audit

- IT Audit Services
- Compliance Gap Analysis
- Security Configuration Review

Additional Services:

→ Managed Security Services

→ White Label & Strategic Partnerships

Security Certifications:

AWS Certified Cloud Practitioner

C|EH
Certified Ethical Hacker

CCNA Security
Cisco Certified Network Associate Security

CISA
Certified Information Systems Auditor

CISM
Certified Information Security Manager

CISSP
Certified Information Systems Security Professional

CRISC
Certified in Risk & Information Systems Control

CRTP
Certified Red Team Professional

E|CIH
EC-Council Certified Incident Handler

OSCP
Offensive Security Certified Professional

PCI QSA
PCI Qualified Security Assessor

PenTest+
CompTIA PenTest+

The Modern Threat:

What is PenTesting & Why it Matters

What is a Penetration Test?

A controlled, authorized, simulated cyberattack to evaluate your security.

External

Firewalls, routers, VPNs, applications, IoT devices, etc.

Internal

Local Area Network (LAN)

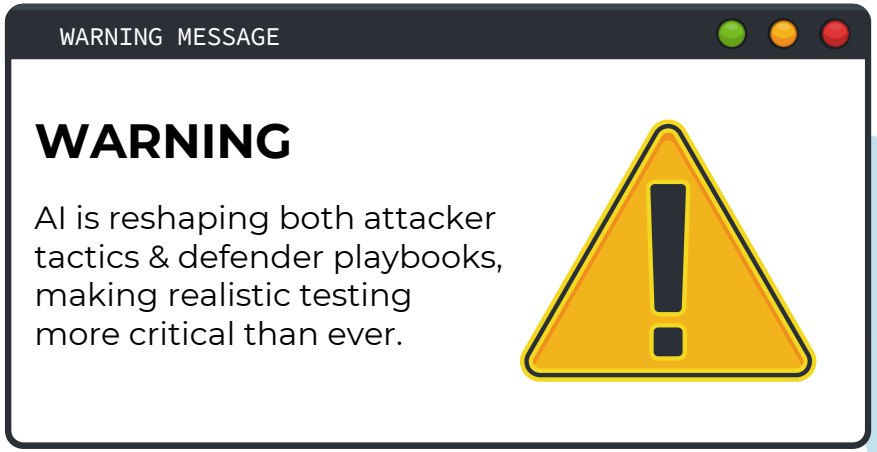
Web & Applications

Websites, mobile applications, integrations, API

Social Engineering

Phishing, Spear Phishing, Vishing, Impersonation, Pretext Calling & Mailer.

The goal:
Find weaknesses before real adversaries do.



Common PenTest Questions We Get:

How long does a typical PenTest take?

What are the differences between the various PenTesting methods?

How often should I perform a PenTest?

Are PenTests disruptive to our business operations?

How are PenTest results presented & what do I do with the results?

Penetration Testing Benefits:

- Find and fix the vulnerabilities that are exploitable.
- Proactively prevent expensive data breaches, fines, and recovery efforts.
- Satisfy requirements for regulations like PCI DSS, HIPAA, and SOC 2.
- Evaluate your team's ability to detect and respond to a real attack.
- Prove your commitment to protecting stakeholder and customer data.

PenTesting Compliance

HIPAA

Technical evaluations are required by the Security Rule and should be done annually or after major changes.

PCI

Mandated by 11.4Q; perform annually and after major changes.

SOC 2

Regular risk assessments required; annual/biannual PenTesting supports Trust Criteria.

GDPR

Article 32 requires testing; PenTesting shows data protection by design.

ISO/IEC 27001

Annex A.12.6.1 recommends regular technical vulnerability assessments.

NIST

Recommended to be done annually as part of continuous monitoring.

FFIEC

Strongly recommended to be performed annually.

FTC

Without continuous monitoring: annual PenTests and scans every 6 months required.

NERC

Critical Infrastructure Protection Standards

Vulnerability assessments every 15 months.

Common Vulnerabilities Discovered During PenTesting:

Misconfiguration

Improper server, software, or cloud settings; use of default credentials.

Unpatched Vulnerabilities

Outdated software or operating systems with known, exploitable flaws.

Injection Attacks

Attackers inserting malicious code (SQL, command) to access or corrupt data.

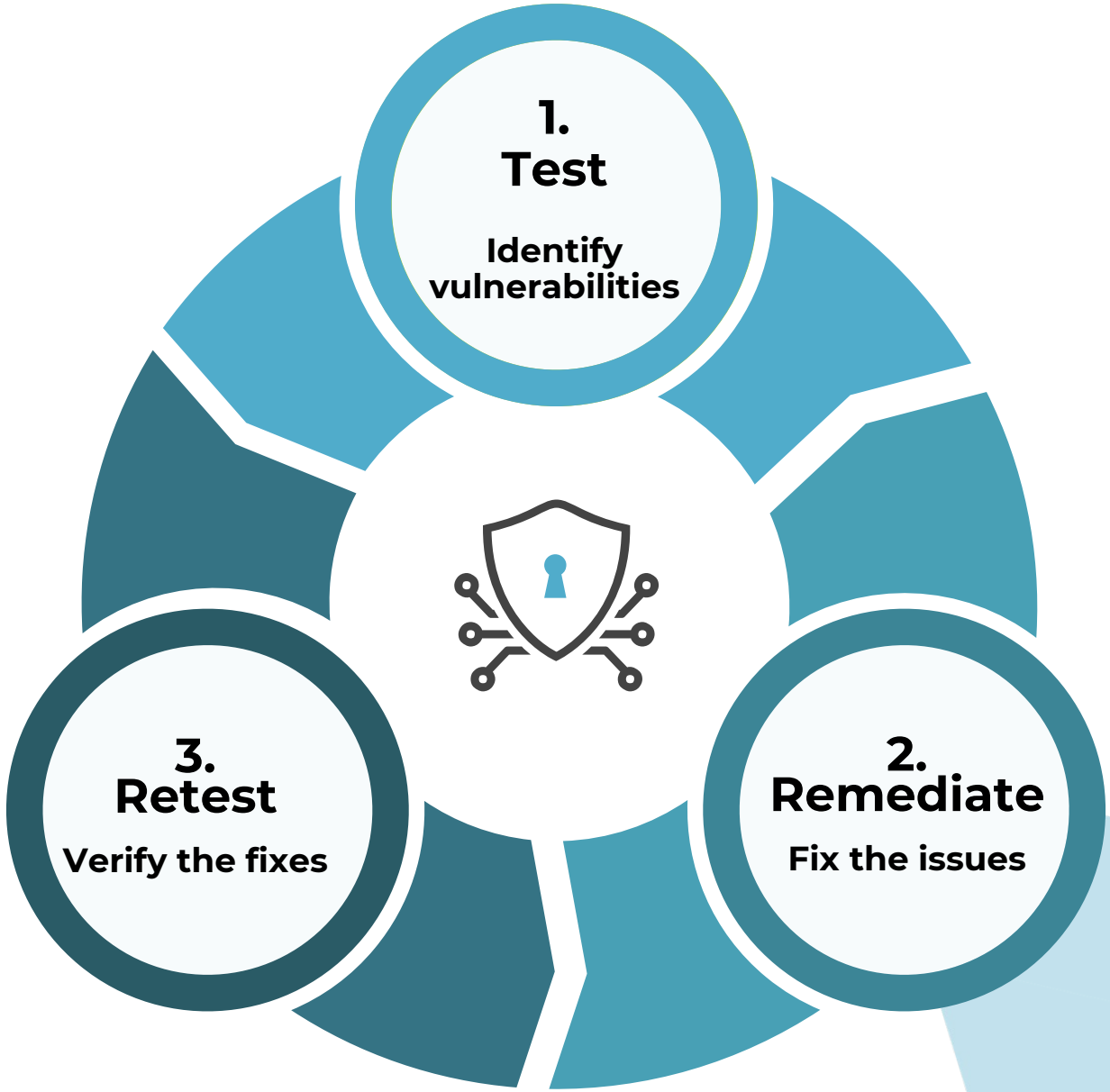
Privilege Escalation

Users gaining access to data or functions beyond their permissions.

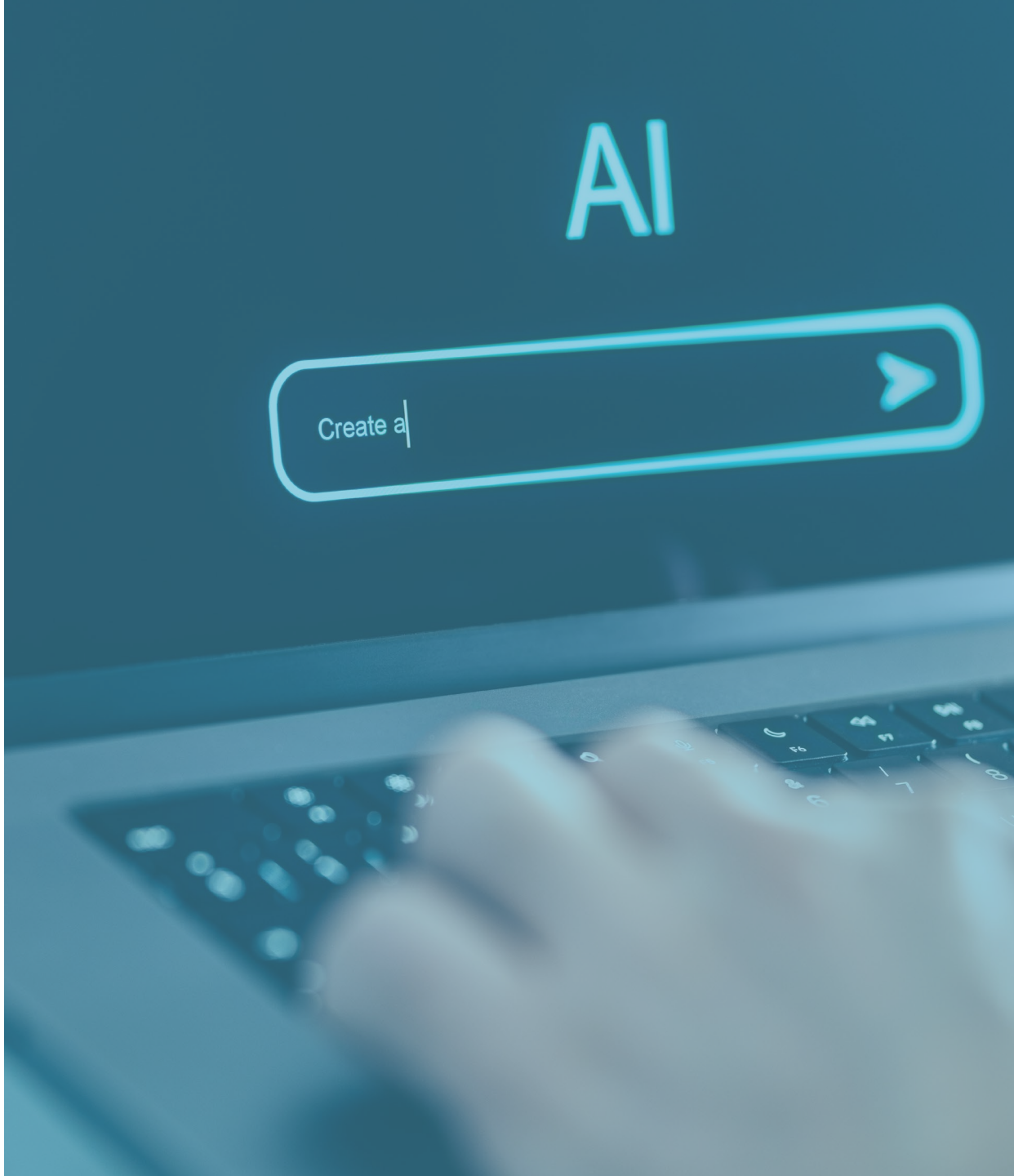
Social Engineering

Successful phishing or vishing attacks that exploit human error.

Identify & Exploit Vulnerabilities



The New Frontier: Artificial Intelligence



Understanding AI

Broadly, Artificial Intelligence (AI) is technology that enables computers and machines to simulate human learning, comprehension, problem solving, decision making, creativity and autonomy.

Generative AI

Describes algorithms that can be used to create new content, including audio, code, images, text, simulations and videos.

When you hear ChatGPT, CoPilot, etc. think Generative AI

Open-source AI

Offers publicly available code that allows for anyone to access and modify the AI models and underlying code.

Transparency, collaboration and cost efficiency are some of the biggest pros with open-source AI.

However, data security, lack of vendor support and higher costs are the drawbacks.

Closed-source AI

Offers improved confidentiality of data, vendor support, consistent updates and a better level of quality assurance.

However, higher costs when it comes to licensing fees, constraints on customization, and limited visibility into algorithms are drawbacks.

Generative AI

Broadly, Artificial Intelligence (AI) is technology that enables computers and machines to simulate human learning, comprehension, problem solving, decision making, creativity and autonomy.

Notice for Attorneys:

American Bar Association (ABA) guidance on using GenAI emphasizes that lawyers must understand their ethical obligations.

Attorneys should consider including confidentiality provisions in discovery agreements to protect confidentiality.

Artificial Intelligence: Risk Management

Laying the Groundwork for an AI Risk Governance Program: *How Will You Use It?*

Enterprise AI Strategy& Scope

Define purpose, data sources, system access and intended users at the Enterprise Level.

Identify the areas of your Organization that you want to start with AI adoption.

Data Sensitivity & Security Considerations

Will you be inputting sensitive, confidential, and or public data into your chosen platform?

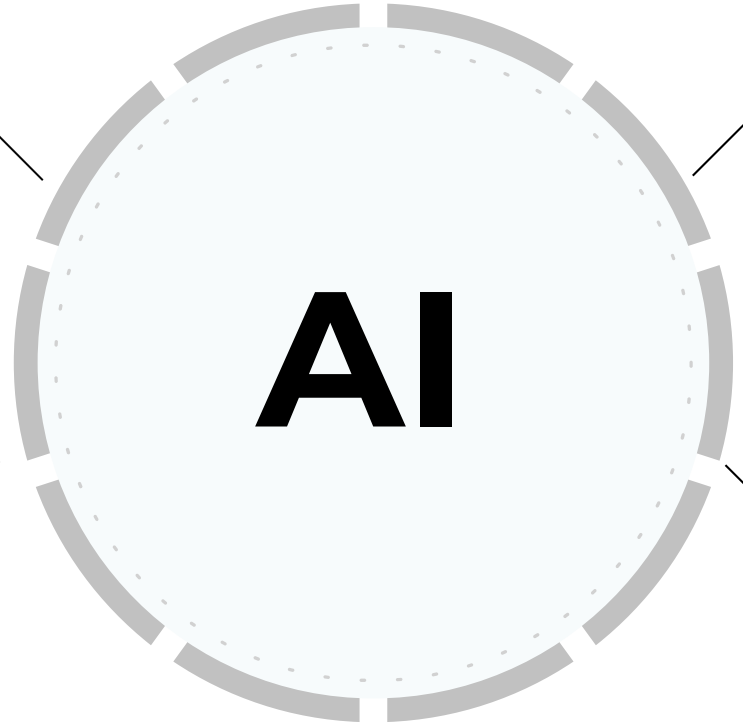
As we mentioned earlier, if you're going to use opensource AI, data security should be of paramount concern. Closed-source allows more control over data security.

AI Use Case Alignment with Strategic Goals

Are you looking for automation, problem solving, decision making, enhanced customer satisfaction, etc.?

We recommend starting with your organization's strategic initiatives and identifying what initiatives you want to start supporting with AI.

AI Risks: External



Reconnaissance

AI agents scour social media, code repos, and dark web data at massive scale.

Scanning & Weaponization

AI-powered tools adaptively 'fuzz' applications to find novel vulnerabilities.

Social Engineering

Deepfake voice and video are used for hyper-realistic phishing and fraud.

AI Vendors

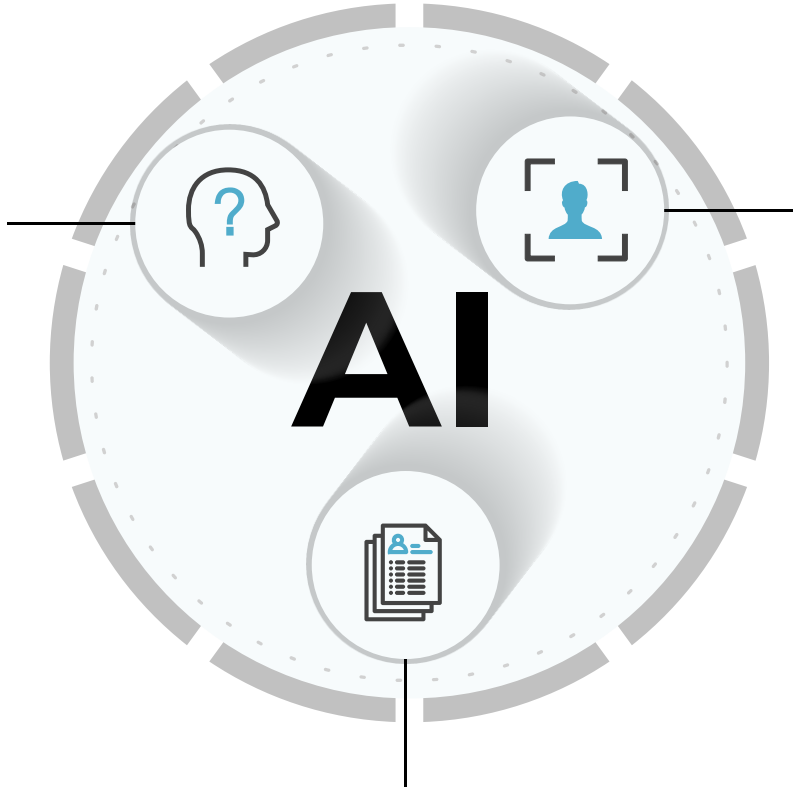
Ensure third parties providing AI services to your Organization have adequate due diligence performed prior to usage.

AI Risks: Internal

Blindly Trusting AI?

Will the AI product/service be autonomous or will it make decisions without any manual verification/authorization?

Knowing the difference is key in proper risk mitigation.



Lack of Data Confidentiality

Define the data types that are permitted to be inputted into AI technologies. Avoid inputting non-public/confidential data!

Lack of Defined Acceptable Use Standards

Provide clear, documented acceptable use standards to staff to ensure they are using approved AI services safely.

Developing an AI Risk Management Program

Set Clear AI Usage Boundaries

Be crystal clear on whether AI can be used for business tasks. Put guard rails up before the car goes off the track!

Define AI Approval Authority

Define who can approve AI products within your organization and reinforce the chain of command with staff at all levels.

Mitigate AI Decision-Making Risks

Clearly outline controls to minimize privacy, ethical, and compliance risks when AI output is used for important decisions.

Leverage the NIST AI RMF

Build on the NIST AI Risk Management Framework to Govern, Map, Measure, and Manage AI risks

Form an AI Risk Committee

Consider an AI Risk Committee for AI usage oversight.

Case Study:
Deepfake Voice Phish at XYZ Corp

The Attack:

An attacker used an AI voice clone of the CEO to call an employee in finance, urgently requesting a wire transfer.

The Pentest Simulation:

We replicated this by training a voice model on public earnings calls and using it in a 'vishing' campaign.

The Remediation:

XYZ Corp implemented a multi-person approval process for out-of-band requests and trained employees to use a verbal codeword for verification.

Key Takeaways:

- Penetration testing remains your front-line assessment for real-world vulnerabilities
- AI is a 'force multiplier' for attackers, making traditional defenses insufficient on their own.
- Ongoing vulnerability management is key to ensuring your Organization’s security posture is adequate in the rapidly evolving threat landscape.
- Develop an AI Risk Management Program that formally governs AI usage Organization-wide.

GRAVOC

g³ gray™

THE POWER OF MORE

Questions

Paul Seekamp
pseekamp@gravoc.com

Patrick Avery
pavery@gravoc.com