FORTRA™

Cybersecurity Week

Proactive Cybersecurity

The One Place Where “You’re Being Offensive” Is a Compliment

Your Presenter

Pablo Zurro

Cybersecurity Product Manager

pablo.zurro@fortra.com

Today’s Session

1. What Is Proactive Security?
2. The Journey Towards Proactive Security
3. 6 Tips for a Proactive Mindset

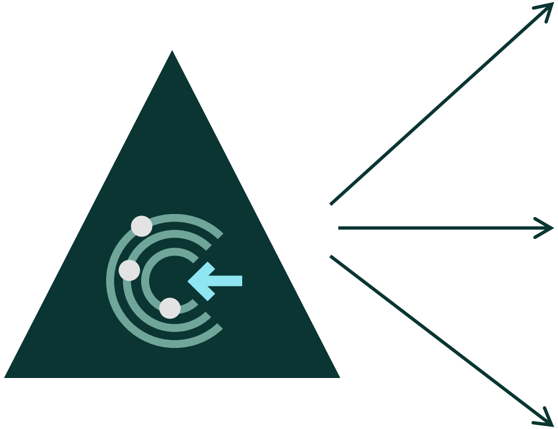
Proactive Security

Proactive: Serving to prepare for, intervene in, or control an expected occurrence or situation, especially a negative or challenging one; anticipatory

Dictionary.com

Offensive Security

Safely test your environment using the same techniques as today’s attackers



Offensive security exercises help organizations identify security weaknesses and exploitable vulnerabilities across an environment. Simply put, offensive security solutions help streamline testing to better prioritize and reduce risk exposure within the organization.

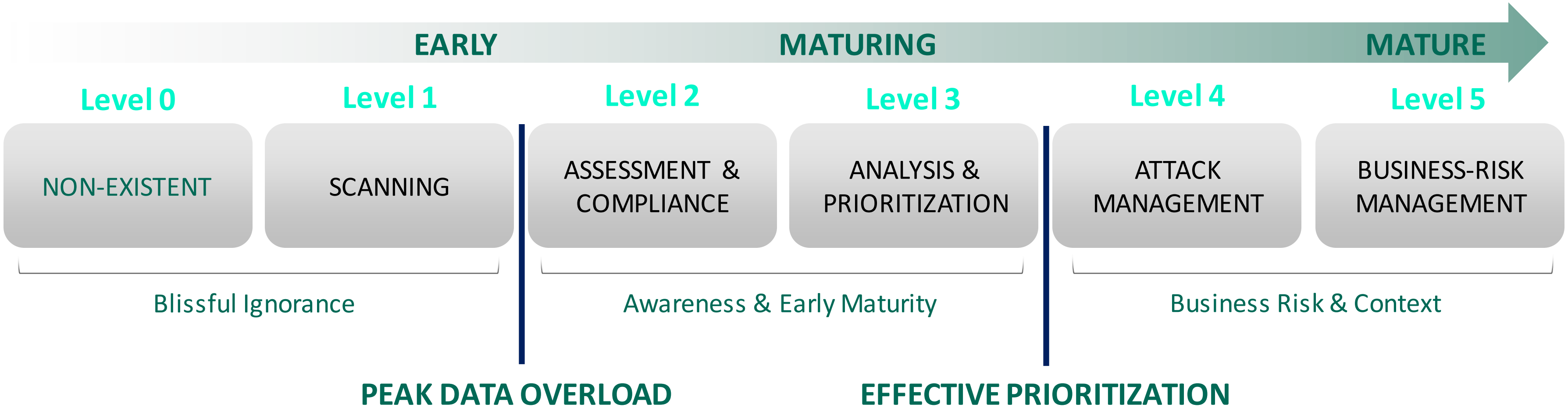
Fortra provides tools and services to help proactively protect your critical systems and data by anticipating attacks before they happen. Our offensive security solutions allow you to ***gain actionable insight into and prioritize your greatest risks to efficiently close security gaps***.

These tools and services include penetration testing, red teaming, and adversary simulation.

How do you know where you fit and what you need?

	EARLY	MATURING	MATURE
Team Attributes	• Small team, part of larger IT organization • Reactive, not proactive focus on security • Worried about keeping the lights on	• Small to mid-sized team • Starting to take proactive steps to reduce risk	• Large team • Fostered culture of security learning • Experts on staff
Company Attributes	• Limited security awareness from executives • No sustained companywide security focus	• Security team developing influence within organization • Meeting compliance requirements • Security-focused leadership is emerging	• Risk awareness is pervasive • Security is a part of day to-day life
Team Member Specialization	• Generalists managing IT and security • Little if any expert knowledge	• Starting to specialize on areas of security (i.e., network only security admin)	• Specialists, highly skilled individuals in key roles (SIEM admin, pen testers, red teamers, etc.)
Types of Solutions in place	• Firewall / Antivirus • Spam filter / Web proxy • Vulnerability management	• Log management • Security awareness training	• Covering most if not all the top-10 critical controls • External threat intelligence
Retained Services	• Managed application security	• MSSP • Training • Penetration testing	• Cyber Maturity Assessment • Red teaming
Recommended Areas of Focus	• Vulnerability Scanning • SIEM • Server-Level Protection/ Antivirus • Security Awareness Training	Same as early + • Penetration Testing Software • Penetration Testing Services • Web Application Scanning • Data Loss Prevention	Same as maturing + • Adversary Simulation • Red Teaming • Threat Intelligence Based Ethical Red Teaming

Threat & Vulnerability Management Maturity Model



EARLY — MATURING — MATURE

Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
NON-EXISTENT	SCANNING	ASSESSMENT & COMPLIANCE	ANALYSIS & PRIORITIZATION	ATTACK MANAGEMENT	BUSINESS-RISK MANAGEMENT

Blissful Ignorance

Awareness & Early Maturity

Business Risk & Context

PEAK DATA OVERLOAD

EFFECTIVE PRIORITIZATION

Tips for a Successful Proactive Security Program

01 Understand What You Are Protecting

02 Understand Your Third-Party Ecosystem

03 Understand Your People and Processes

04 Think Like an Attacker

05 Invest in Vulnerability Assessments, Pen Testing, and Adversary Simulation

06 TEST, TEST, and TEST Again

The Benefits of a Proactive Security Program

Total Vulnerability Management

Vulnerability management programs aim to reduce risk and continually elevate the security of an IT environment by creating robust processes for identifying, classifying, remediating, and mitigating weaknesses.

Adherence to Regulatory Requirements

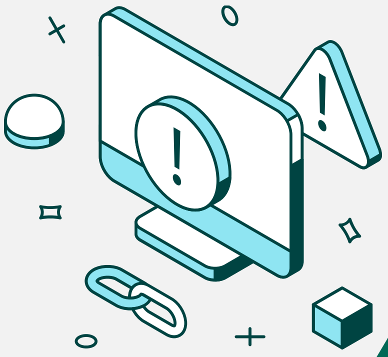
Penetration testing helps organizations address regulatory requirements. The reports illustrate ongoing due diligence to assessors, avoiding significant fines for non-compliance.

Avoiding the Costs of a Breach

Financially, organizations can end up paying millions of dollars to return to equilibrium. Operationally, a breach can halt the flow of business and recovery doesn't always repair a damaged reputation.

Proactive Security Assessment

Vulnerability Management



Fortra's Digital Defense

Vulnerability Management and Penetration Testing Services

VULNERABILITY VALIDATION

Penetration Testing

Fortra's Core Security

Penetration Testing Software and Security Consulting Services

ADVANCED ADVERSARY SIMULATION

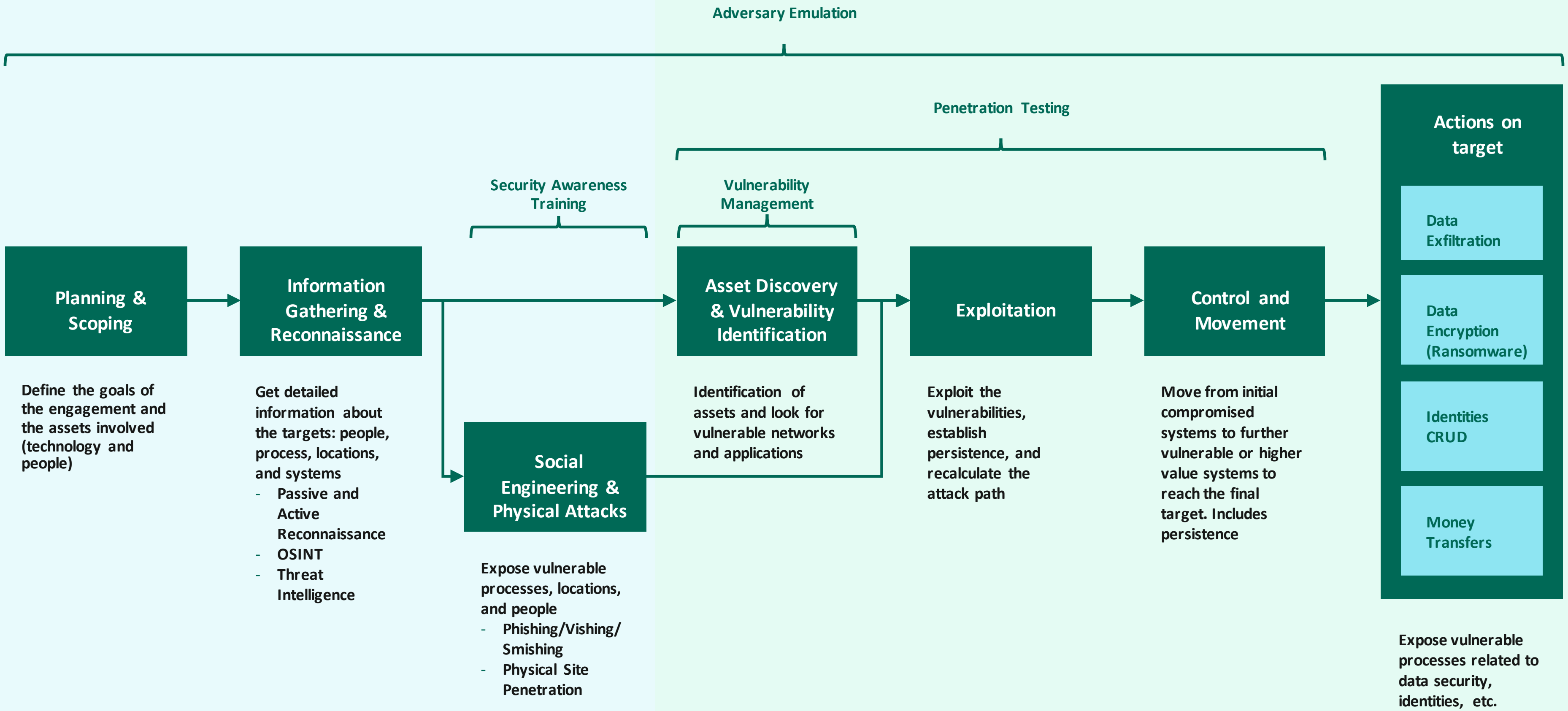
Red Teaming

Fortra's Cobalt Strike & Outflank OST

Adversary Simulations and Red Team Operations

FORTRA

Cybersecurity Week



Adversary Emulation

Penetration Testing

Security Awareness Training

Vulnerability Management

Planning & Scoping

Define the goals of the engagement and the assets involved (technology and people)

Information Gathering & Reconnaissance

Get detailed information about the targets: people, process, locations, and systems

- Passive and Active Reconnaissance
- OSINT
- Threat Intelligence

Social Engineering & Physical Attacks

Expose vulnerable processes, locations, and people

- Phishing/Vishing/ Smishing
- Physical Site Penetration

Asset Discovery & Vulnerability Identification

Identification of assets and look for vulnerable networks and applications

Exploitation

Exploit the vulnerabilities, establish persistence, and recalculate the attack path

Control and Movement

Move from initial compromised systems to further vulnerable or higher value systems to reach the final target. Includes persistence

Actions on target

- Data Exfiltration
- Data Encryption (Ransomware)
- Identities CRUD
- Money Transfers

Expose vulnerable processes related to data security, identities, etc.

Outside the organization

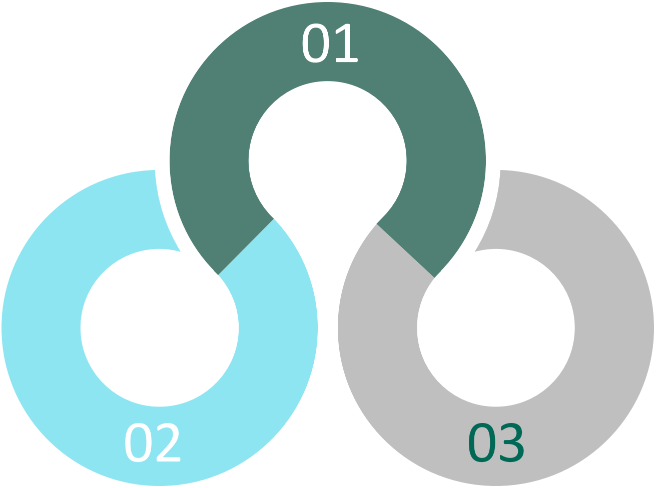
Inside the organization

Strengthen and Simplify Your Cybersecurity

Do more than just defend against cyber-attacks: Proactively **anticipate** attacks before they happen.

Continually **adapt** your cybersecurity strategy to address new attack vectors.

Improve security team efficiency for faster **remediation** times and timely protection.



Prioritize the Risks That Matter

Recent Technical Resources

INFRASTRUCTURE PROTECTION FOR PROACTIVE SECURITY

www.coresecurity.com/resources/datasheets/infrastructure-protection-proactive-security-datasheet

TAKING BACK CONTROL: A PROACTIVE APPROACH TO ADVANCE YOUR SECURITY MATURITY

www.coresecurity.com/resources/guides/taking-back-control-proactive-approach-advance-your-security-maturity

HOW DO YOU KNOW IF YOU'RE READY FOR A PEN TEST?

https://static.fortra.com/hs/pdfs/2022/datasheet/hs-security-maturity-matrix-ds.pdf

FORTRA™

Cybersecurity Week

Thank you

www.fortra.com

emails@fortra.com