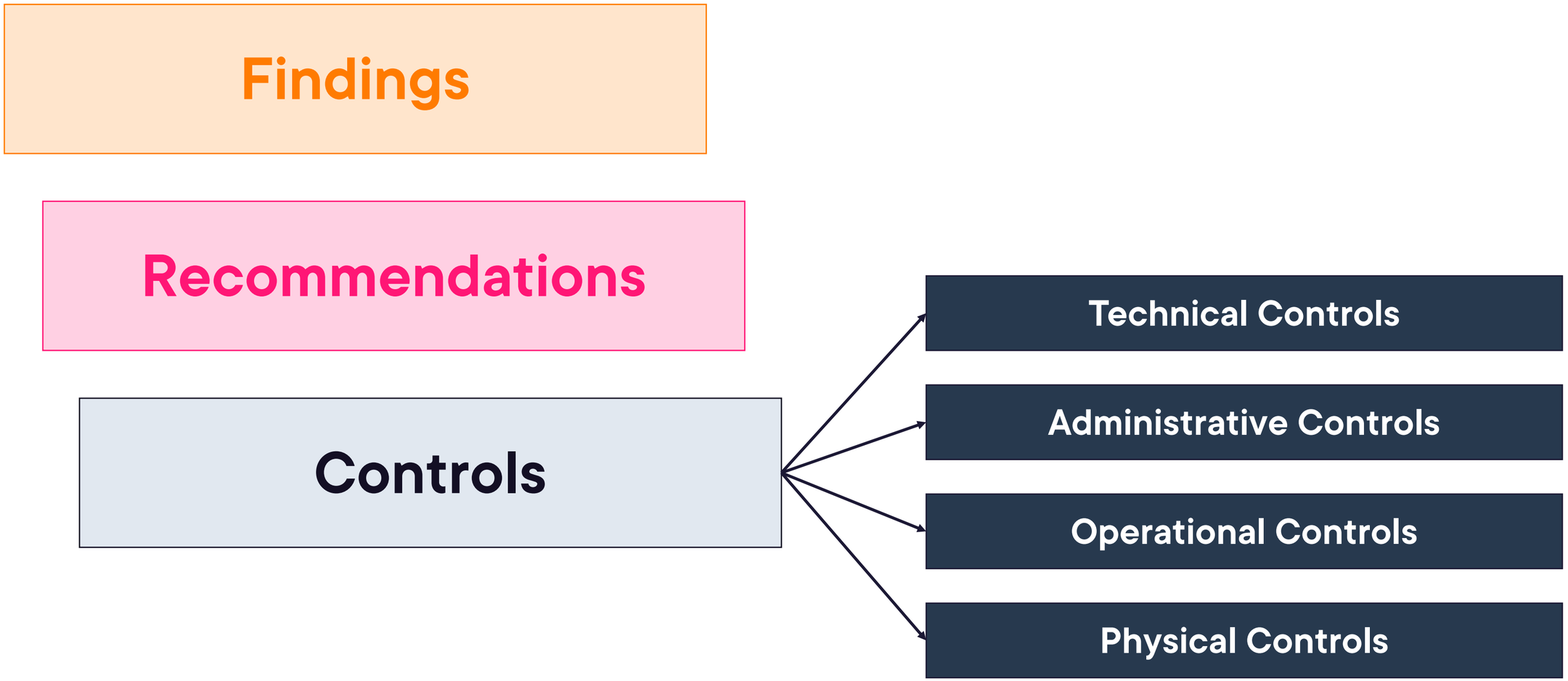
Remediations and Recommendations

Ricardo Reimao, OSCP, CISSP
Cybersecurity Consultant

Understanding the Basics



Technical Controls – Part 1

System Hardening

Parametrized Queries and User Input Sanitization

Multi-factor Authentication

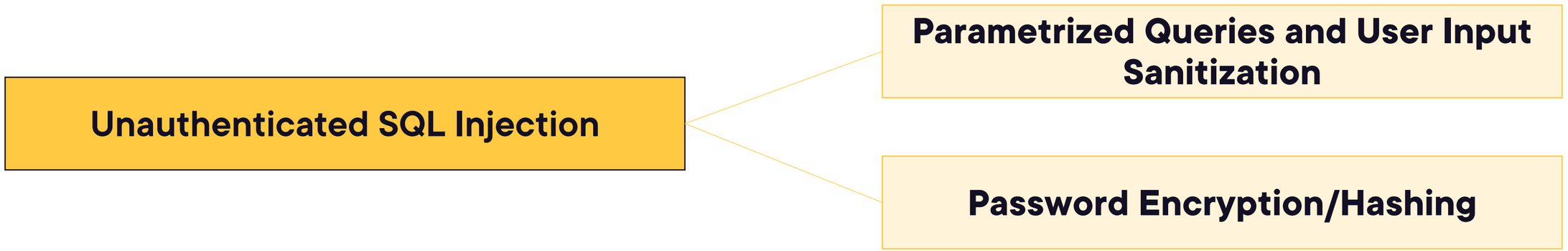
Password Encryption/Hashing

Process-level Remediation

Technical Controls – Part 2

Patch Management	Key Rotation	Certificate Management
Secrets Management Solution	Network Segmentation	Infrastructure Security Controls

Suggested Technical Controls - Globomantics



Common Administrative Controls

Main Administrative Controls

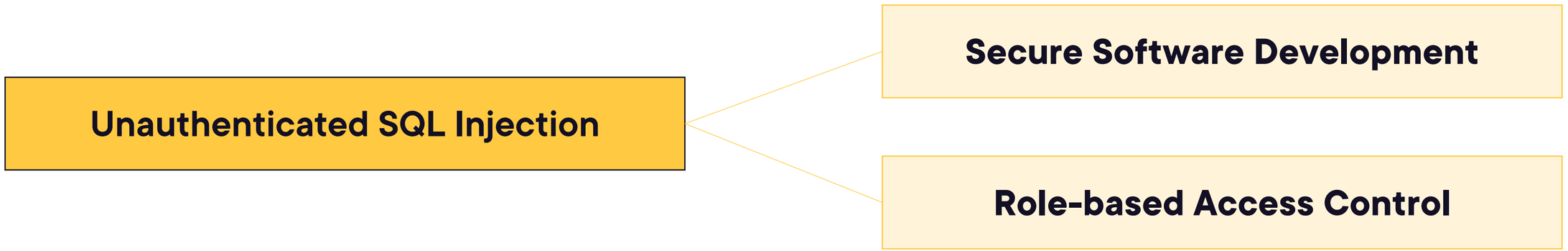
Role-based Access Control (RBAC)

Secure Software Development Lifecycle

Minimum Password Requirements

Adequate Policies and Procedures

Globomantics
Suggested Administrative Controls



Common Operational and Physical Controls

What Are Operational and Physical Controls?

Operational controls are related to day-to-day activities of the company and employees

Physical controls are related to the physical security of the environment

Operational Controls

Job Rotation

Mandatory Vacations

Time-of-day Restrictions

User Training

Physical Controls

Access Control Vestibule

Biometric Controls

Video Surveillance

Domain Summary

What You Learned

Pre-engagement tasks

Assessment types, contracts, agreements, rules of engagement and target selection

Assessment frameworks

PTES, CREST, MITRE ATT&CK, OWASP, etc.

Communication and Reporting

Sections of a report, executive summary, writing findings, determining impact, etc.

Recommendations and Technical Controls

Technical, administrative, operational and physical controls

Things to Remember

The Pentest Process

Pre-Engagement → Intelligence Gathering → Threat Modelling → Vulnerability Analysis → Exploitation → Post Exploitation → Reporting

Main Agreements

Master Service Agreement (MSA) → Non-Disclosure Agreement (NDA) → Statement of Work (SOW) → Terms of Service (ToS) → Rules of Engagement (RoE)

Main Compliance Standards

- PCI-DSS
- GDPR
- Local Restrictions

Things to Remember – Part 2

Pentest Frameworks

- PTES
- OSSTMM
- MITRE ATT&CK
- CREST
- OWASP
- PURDUE

Risk Calculation

Impact × Likelihood = Risk

Report Sections

Technical Controls

Next Courses

- Engagement Management for CompTIA Pentest+
- Reconnaissance and Enumeration for CompTIA Pentest+
- Vulnerability Discovery and Analysis for CompTIA Pentest+
- Attacks and Exploits: Network and Application Attacks for CompTIA Pentest+
- Attacks and Exploits: Specialized Attacks for CompTIA Pentest+
- Post-exploitation and Lateral Movements for CompTIA Pentest+
- Exam Review and Tips for CompTIA Pentest+

Thank you!