universidade de aveiro

Critical software

So far...

Robust Software – Nuno Silva

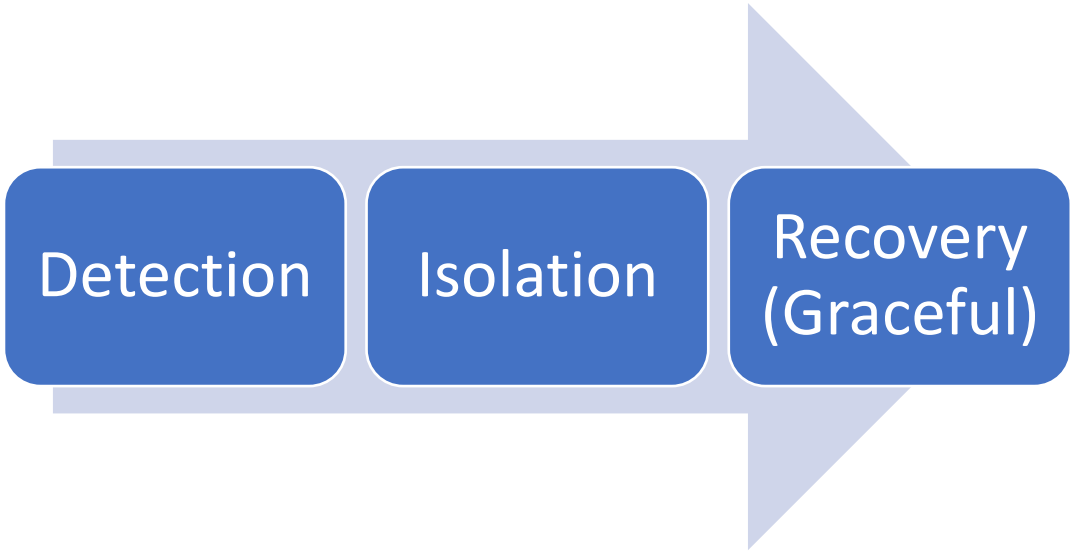
Mestrado em Cibersegurança

Knowledge

- Is key,
- So does awareness
- *“Conhecimento e*
- *Conscientização”*

Design Principles

1. Apply Defense in Depth
2. Use a Positive Security Model
3. Fail Securely
4. Run with Least Privilege
5. Avoid Security by Obscurity
6. Keep Security Simple
7. Detect Intrusions
    1. Log All Security-Relevant Information
    2. Ensure That the Logs Are Monitored Regularly
    3. Respond to Intrusions
8. Don’t Trust Infrastructure
9. Don’t Trust Services
10. Establish Secure Defaults



Secure SW Lifecycle

Phase	Microsoft SDL	McGraw Touchpoints	SAFECode
Education and awareness	Provide training		Planning the implementation and deployment of secure development
Project inception	Define metrics and compliance reporting Define and use cryptography standards Use approved tools		Planning the implementation and deployment of secure development
Analysis and requirements	Define security requirements Perform threat modelling	Abuse cases Security requirements	Application security control definition
Architectural and detailed design	Establish design requirements	Architectural risk analysis	Design
Implementation and testing	Perform static analysis security testing (SAST) Perform dynamic analysis security testing (DAST) Perform penetration testing Define and use cryptography standards Manage the risk of using third-party components	Code review (tools) Penetration testing Risk-based security testing	Secure coding practices Manage security risk inherent in the use of third-party components Testing and validation
Release, deployment, and support	Establish a standard incident response process	Security operations	Vulnerability response and disclosure

Software Quality Attributes

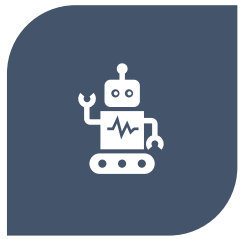
Source: ISO/IEC CD 25010 Software engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Quality model and guide, 2011.

Security Requirements

S – SPECIFIC

M – MEASURABLE

A – ACHIEVABLE / ATTAINABLE



R – RELEVANT

T – TIME-BOUND