SECURITY ADVANCED

PXL DIGITAL

WHITE TEAM

Contains elements of **Compliance, Management, Analysts, Logistics** and more.

These are all-knowing, neutral, 3rd parties who:

- Draft the rules
- Organise teams
- Make plans
- Follow up on progress

Essential for every organisation, but are far removed from the technical/practical part of the business and are therefore not always seen as an advantage -> need input from the workfield.

SECURITY STANDARDS

Setup rules based on standards.

ISO 27001

ISO 27001 is an international standard that defines how to manage information security in a company.

PXL DIGITAL

SECURITY STANDARDS

ISO 27001 Controls (Annex A)

A.5 **Information security policies** – controls on how the policies are written and reviewed

A.6 **Organization of information security** – controls on how the responsibilities are assigned; also includes the controls for mobile devices and teleworking

A.7 **Human resources security** – controls prior to employment, during, and after the employment

A.8 **Asset management** – controls related to inventory of assets and acceptable use, also for information classification and media handling

https://advisera.com/27001academy/knowledgebase/overview-of-iso-270012013-annex-a/

SECURITY STANDARDS

ISO 27001 Controls (Annex A)

A.9 **Access control** – controls for Access control policy, user access management, system and application access control, and user responsibilities

A.10 **Cryptography** – controls related to encryption and key management

A.11 **Physical and environmental security** – controls defining secure areas, entry controls, protection against threats, equipment security, secure disposal, clear desk and clear screen policy, etc.

A.12 **Operational security** – lots of controls related to management of IT production: change management, capacity management, malware, backup, logging, monitoring, installation, vulnerabilities, etc.

https://advisera.com/27001academy/knowledgebase/overview-of-iso-270012013-annex-a/

SECURITY STANDARDS

ISO 27001 Controls (Annex A)

A.13 **Communications security** – controls related to network security, segregation, network services, transfer of information, messaging, etc.

A.14 **System acquisition, development and maintenance** – controls defining security requirements and security in development and support processes

A.15 **Supplier relationships** – controls on what to include in agreements, and how to monitor the suppliers

A.16 **Information security incident management** – controls for reporting events and weaknesses, defining responsibilities, response procedures, and collection of evidence

https://advisera.com/27001academy/knowledgebase/overview-of-iso-270012013-annex-a/

SECURITY STANDARDS

ISO 27001 Controls (Annex A)

A.17 **Information security aspects of business continuity management** – controls requiring the planning of business continuity, procedures, verification and reviewing, and IT redundancy

A.18 **Compliance** – controls requiring the identification of applicable laws and regulations, intellectual property protection, personal data protection, and reviews of information security

[...] while IT is certainly important, IT alone cannot protect information. Physical security, legal protection, human resources management, organizational issues – all of them together are required to secure the information.

https://advisera.com/27001academy/knowledgebase/overview-of-iso-270012013-annex-a/

THREAT MODELLING

Threat modeling is a **process by which potential threats**, such as structural vulnerabilities **can be identified, enumerated, and prioritized** – all from a hypothetical attacker's point of view.

The purpose of threat modeling is to **provide defenders with a systematic analysis of the probable attacker's profile, the most likely attack vectors, and the assets most desired by an attacker.**

Threat modeling answers questions like:

"Where are the high-value assets?"

"Where am I most vulnerable to attack?"

"What are the most relevant threats?",

"Is there an attack vector that might go unnoticed?"

https://en.wikipedia.org/wiki/Threat_model

PXL DIGITAL

THREAT MODEL?

Find Security Bugs Early

- Help you find design issues even before you've written a line of code
- Once you've chosen, changes will be expensive

THREAT MODEL?

Understand Your Security Requirements

- Good threat models can help you ask "Is that really a requirement?"
- Interplay between requirements, threats, and mitigations
  - Some threats don't line up with your business requirements, and as such may not be worth addressing
  - Your requirements may not be complete
  - Other threats might be too complex or expensive to address

THREAT MODEL?

Engineer and Deliver Better Products

- Considering your requirements and design early in the process
- Dramatically lower the odds that you'll be
  - re-designing,
  - re-factoring,
  - or facing a constant stream of security bugs
- Deliver a better product on a more predictable schedule

THREAT MODEL?

Address Issues Other Techniques Won’t

- Threat modeling will lead you to categories of issues that other tools won’t find
- Models of what goes wrong, by abstracting away details, will help you see analogies and similarities to problems that have been discovered in other systems
- Threat modeling should not focus on issues that your other safety and security engineering is likely to find

4-STEP THREAT MODELLING FRAMEWORK

1. What are you building?

2. What can go wrong with it once it's built?

3. What should you do about those things that can go wrong?

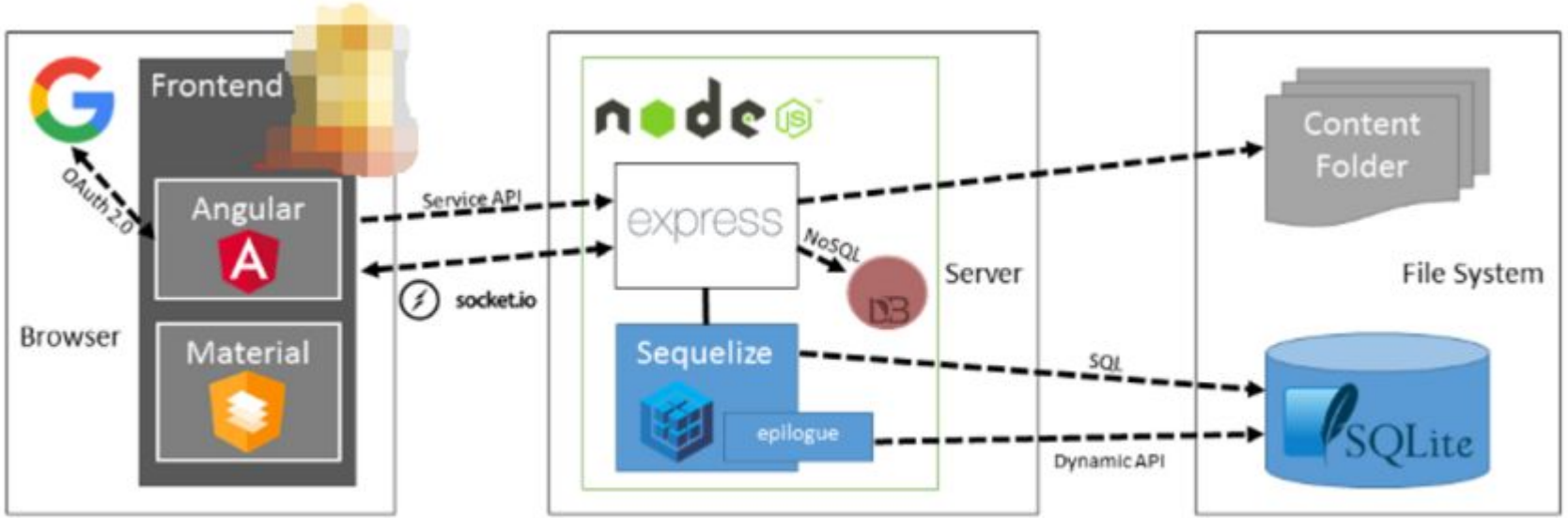
4. Did you do a decent job of analysis?

WHAT ARE YOU BUILDING?

- *"We are going live with our facelifted next-gen online shop next month and we will gain market share like 😜!"* (SVP Sales & Marketing)
- *"We will offer a dedicated next-gen B2B API to our customers using a RESTful endpoint supporting standard and custom data formats. We will ➡ SOON migrate our legacy-XML-integrated customers to this new interface."* (Team Lead EDI Services)
- *"Our new solution is no longer running natively on a classic VM but inside a single 🐳 container on any ☁ platform!"* (Datacenter Manager)
- *"We added secure authentication via Google OAuth 2.0!"* (CISO)
- *"In a future release we will of course add a Blockchain!"* (CIO)

WHAT ARE YOU BUILDING?

Data Flows in the sample application



TRUST BOUNDARIES

- Boundaries to show who controls what
- Threats that cross those boundaries are likely important ones
- Different people control different things

Good examples include: Accounts, Network Interfaces, Different physical computers, virtual machines or organizational boundaries.

STRIDE (What can go wrong)

Threat	Description
Spoofing	Pretending to be something or someone you're not
Tampering	Modifying something you're not supposed to modify. It can include packets on the wire (or wireless), bits on disk, or the bits in memory
Repudiation	Claiming you didn't do something (regardless of whether you did or not)
Information Disclosure	Exposing information to people who are not authorized to see it
Denial of Service	Attacks designed to prevent a system from providing service, including by crashing it, making it unusably slow, or filling all its storage
Elevation of Privilege	When a program or user is technically able to do things that they're not supposed to do

THREATS VS. SECURITY GOALS/PRINCIPLES

Threat	Security Goal/Principle
Spoofing	Authenticity
Tampering	Integrity
Repudiation	non-Repudiation
Information Disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

WHAT SHOULD YOU DO ABOUT IT?

Mitigate: Doing things to make it harder to take advantage of a threat

Eliminate: Almost always achieved by eliminating features

Transfer: Letting someone or something else handle the risk

Accept: Once you've accepted the risk, you shouldn't worry over it.

Sometimes worry is a sign that the risk hasn't been fully accepted, or that the risk acceptance was inappropriate

DID YOU DO A DECENT JOB?

Diagramming

1. Can we tell a story without changing the diagram?

2. Can we tell that story without using words such as “sometimes” or “also”?

3. Can we look at the diagram and see exactly where the software will make a security decision?

4. Does the diagram show all the trust boundaries, such as where different accounts interact? Do you cover all UIDs, all application roles, and all network interfaces?

DID YOU DO A DECENT JOB?

Diagramming (cont.)

5. Does the diagram reflect the current or planned reality of the software?

6. Can we see where all the data goes and who uses it?

7. Do we see the processes that move data from one data store to another?

Threats

1. Have we looked for each of the STRIDE threats?

2. Have we looked at each element of the diagram?

3. Have we looked at each data flow in the diagram?

Validating Threats

1. Have we written down or filed a bug for each threat?

2. Is there a proposed/planned/implemented way to address each threat?

3. Do we have a test case per threat?

4. Has the software passed the test?

PXL DIGITAL

PLURALSIGHT VIDEOS

Pluralsight video: link
Relevant : Introduction to Threat Intelligence

Pluralsight video: link
Relevant : ISO/IEC 27001 Information Security: The Big Picture

Pluralsight video: link
Relevant : Finding Threats Using STRIDE

Pluralsight video: link
Relevant : Risk Management