

SPYDERISK

Automated Cyber Risk Assessment for Compliance Certification

The Problem

The hardest part of compliance is the asset risk assessment process, which is:





- ◆ Time consuming
- ◆ Error prone
- ◆ Difficult to repeat reliably
- ◆ Expensive

The Solution

Modelling and semi-automatic risk analysis for complex IT systems:





- ◆ Threat identification
- ◆ Risk calculation
- ◆ Mitigation plan
- ◆ Compliance reporting

SPYDERISK Automation

-  Attack paths are identified
-  Threat cascades are computed
-  Mitigations are proposed from a detailed knowledgebase
-  Risks are computed from the threat likelihood and business impact



Data Input

-  Draw the model with our intuitive drag-and-drop interface
-  Import data through the API*
-  Integration with Terraform, Nessus and popular CMDBs*
-  Select existing mitigations from SOC-2 and ISO 27k controls

Analysis & Export

-  Explore the threats and their causes
-  Implement suggested controls to lower risk levels
-  Export full technical assessment
-  Create the reports required for SOC-2 and ISO 27001*

SPYDERISK

Asset Palette

Threat Explorer

Modelling Canvas

Key Issues

The screenshot displays the SPYDERISK interface with several key components:

- Asset Palette:** Located on the left, it lists asset categories like CellularNetwork, Internet, MobileHost, and HostedAsset.
- Threat Explorer:** A central window showing a threat model. It includes a description of a 'Remote Client Exploit (Phishing)', a likelihood of 'Medium' and risk of 'High', and a list of control strategies such as 'OneTimeKeyAuthentication' and 'OneTimeKeyGenerator at ClientBrowser'.
- Modelling Canvas:** A central diagram showing relationships between assets like Website, ClientDB, Webserver, MachineRoom, DBServer, and ShopLAN. Relationships include 'amends', 'reads', 'uses', 'hosts', 'connectedTo', and 'subjectTo'.
- Key Issues:** A table on the right showing a summary of assets, controls, and misbehaviours. It includes a table of threats with columns for Name, Asset, Impact, Likelihood, and Risk.

| Name | Asset | Impact | Likelihood | Risk |
|-------------------------|---------------|----------|------------|----------|
| Loss of Confidentiality | ClientProfile | High | Medium | High |
| Loss of Integrity | ClientProfile | High | Medium | High |
| Loss of Availability | Website | Medium | Medium | Medium |
| Infected by Malware | ShopRouter | Very Low | Very Low | Very Low |
| Infected by Malware | Webserver | Very Low | Very Low | Very Low |
| Infected by Malware | DBServer | Very Low | Very Low | Very Low |
| Infected by Malware | ClientPC | Very Low | Low | Very Low |

| Threat | Asset | Likelihood | Risk |
|---|--------------------|------------|--------|
| Remote Host Exploit (OWASP A9) (a4a3) | ClientPC | Medium | High |
| Remote Host Exploit (OWASP A6) (927a) | ClientPC | Medium | High |
| Remote Host Exploit (OWASP A6) (c339) | ClientPC | Medium | High |
| Remote Client Exploit (Phishing) (1324) | ServiceChannel-... | Medium | High |
| Access to Comms via Compromised Subnet (ca6e) | ServiceChannel-... | Medium | High |
| Remote Host Exploit (OWASP A9) (8482) | ClientPC | Medium | Medium |
| Remote Host Exploit (2e25) | Interface-Clie... | Very High | Low |

Selected Mitigations

All Threats