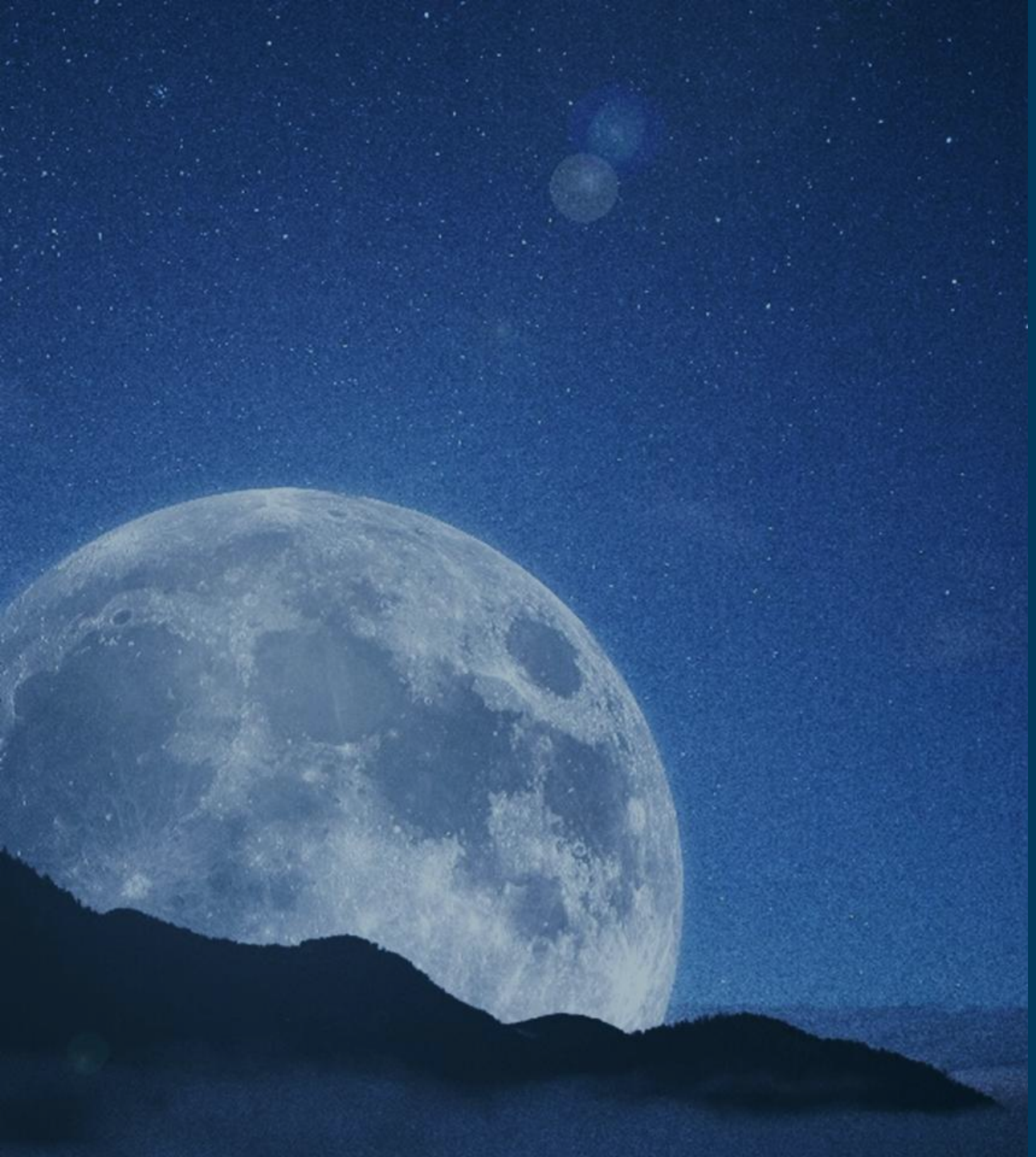
LUNARIS
Digital Solutions

SECURITY BY DESIGN

Sicherheit als integraler Bestandteil

Florian Bader



MIT WEM HABT IHR ES ZU TUN?

Florian Bader

Solution Architect | CTO

Florian.Bader@lunaris.digital

https://lunaris.digital
https://github.com/florianbader

LUNARIS
Digital Solutions

SECURITY BY DESIGN

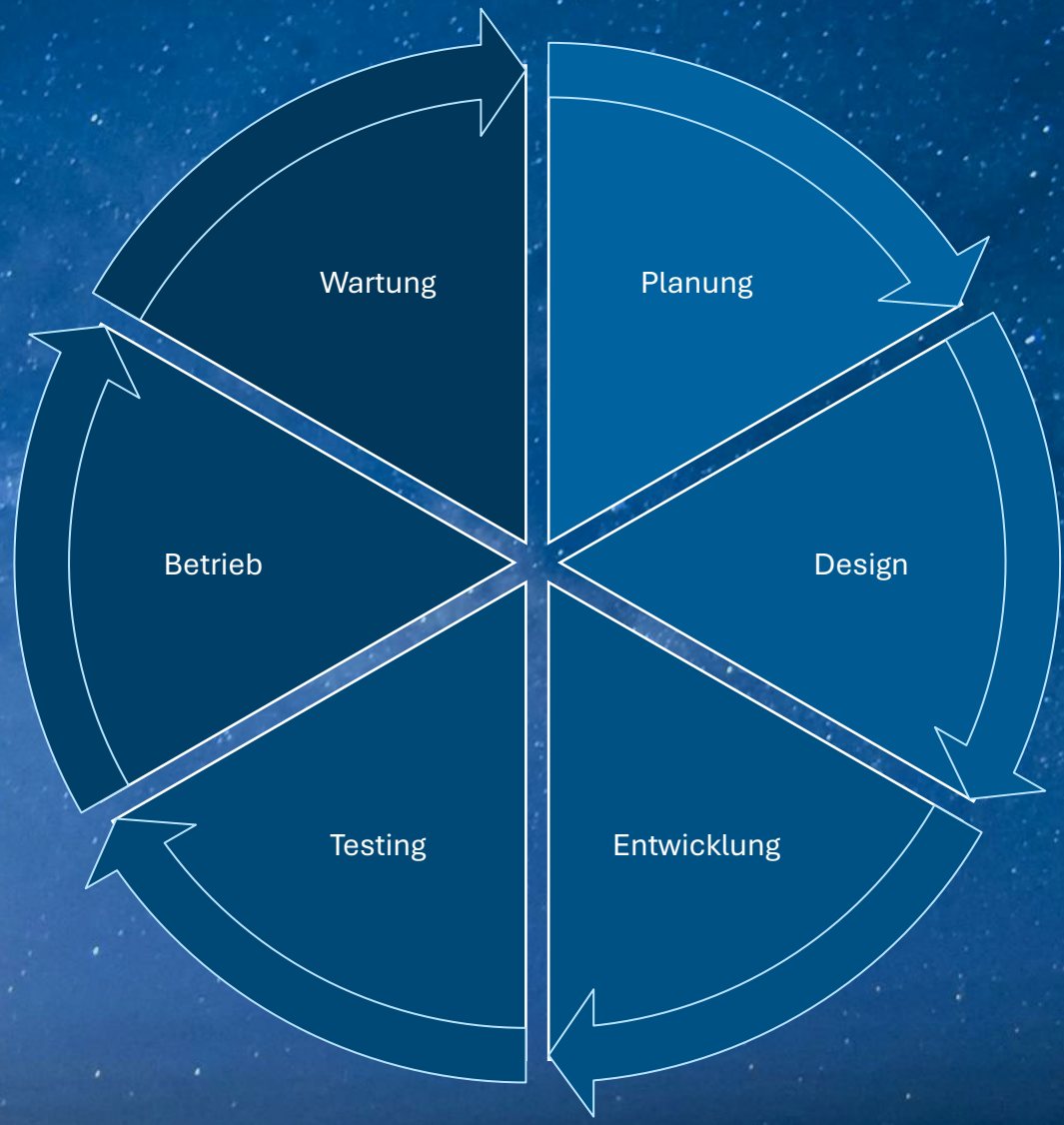
Warum?

- Shift Left: Günstiger in Planung als in Produktion
- Angriffsfläche wächst mit Cloud, Technologien, Tools, Abhängigkeiten
- Standards (ISO27001), Regulatorien (CRA, NIS2, GDPR)

Wie?

- **Planung**: Threat Modeling, Security Requirements, Risikoanalyse
- **Entwicklung**: Analyzer, Secrets Scanner, SBOM, Security Header
- **Testing**: OWASP ZAP, SAST/DAST, Dependency Scans
- **Betrieb**: Managed Identities, Key Vault, Defender for Cloud
- **Wartung**: Patch-Management, Monitoring, Incident Response

SECURE SOFTWARE DEVELOPMENT LIFECYCLE (SSDLC)



OWASP TOP 10

A01:2025 - Broken Access Control

- Fehlende Berechtigungsprüfung, CORS, Elevation of Priviledge

A02:2025 - Security Misconfiguration

- Test Mode in Production, Default Credentials, Log Configuration

A03:2025 - Software Supply Chain Failures

- Vulnerabilities

A04:2025 - Cryptographic Failures

- Weak Hashing, Fehlende Verschlüsselung, Self Signed Certificates

A05:2025 – Injection

- SQL, XML, Command Line, LDAP

A06:2025 - Insecure Design

- Threat Modeling

A07:2025 - Authentication Failures

- Session Hijack, Bruteforce, Fehlendes oder unsicheres MFA,

A08:2025 - Software or Data Integrity Failures

- Trusted Repos, Digital Signatures

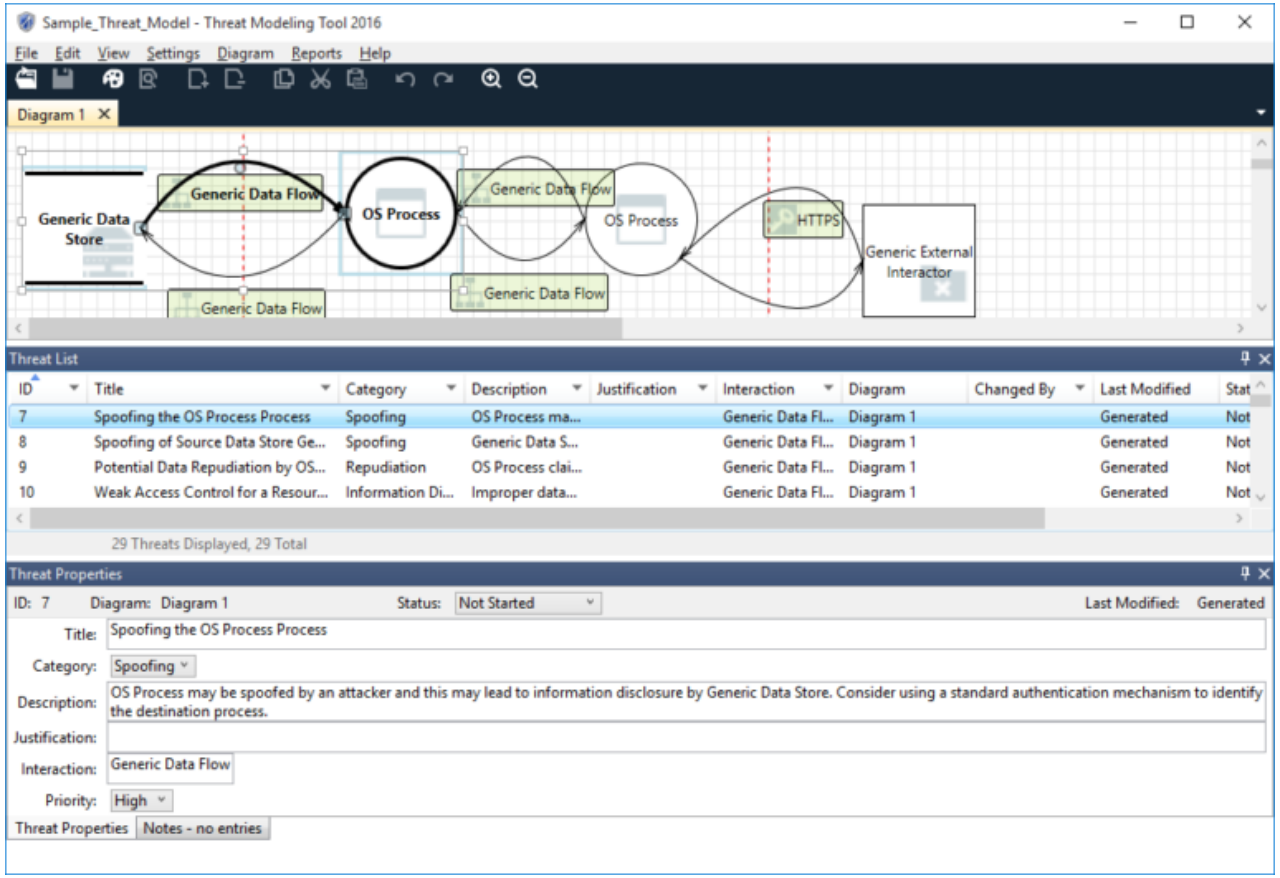
A09:2025 - Logging & Alerting Failures

- Sensitive Daten in Logs, Keine Logs für verdächtige Aktivitäten

A10:2025 - Mishandling of Exceptional Conditions

- Sensitive Daten in Exceptions, Denial of Service, Fehlender Rollback

PLANUNG



Microsoft Threat Modeling Tool overview - Azure | Microsoft Learn

Threat Modeling

- PlantUML/Markdown, Microsoft Threat Modeling Tool, OWASP Threat Dragon, IriusRisk

Non-Functional Requirements

- AuthN /AuthZ, Verschlüsselung, Logging/Monitoring, Datenschutz, Verfügbarkeit, ...

STRIDE

- Spoofing (Identitätsbetrug)
- Tampering (Manipulation)
- Repudiation (Abstreitbarkeit)
- Information Disclosure (Informations-Leaks)
- Denial of Service (Unverfügbarkeit)
- Elevation of Priviledge (Rechteausweitung)

Alternativen: PASTA, AttackTrees, FMEA

ENTWICKLUNG

Statische Codeanalyse (SAST)

- Static Application Security Testing
- .NET Analyzer, ESLint, Sonar, Astrée ...
- Secret Scanner (GitLeaks, Trufflehog, ...)

Software Supply Chain

- Vulnerabilities
- Lizenzen
- Software Bill of Materials (SBOM)

Web App Security

- Rate Limiting
- Security Headers

Logging

- Compliance Redaction

Dependency-Track | Software Bill of Materials (SBOM) Analysis | OWASP

```
PASS: Server Side Code Injection [90019]
PASS: Remote OS Command Injection [90020]
PASS: XPath Injection [90021]
PASS: Application Error Disclosure [90022]
PASS: XML External Entity Attack [90023]
PASS: Generic Padding Oracle [90024]
PASS: Expression Language Injection [90025]
PASS: SOAP Action Spoofing [90026]
PASS: Cookie Slack Detector [90027]
PASS: Insecure HTTP Method [90028]
PASS: SOAP XML Injection [90029]
PASS: WSDL File Detection [90030]
PASS: Loosely Scoped Cookie [90033]
PASS: Cloud Metadata Potentially Exposed [90034]
PASS: Server Side Template Injection [90035]
PASS: Server Side Template Injection (Blind) [90036]
WARN-NEW: Missing Anti-clickjacking Header [10020] x 11
        https://lunaris.digital/ (200 OK)
        https://lunaris.digital (200 OK)
        https://lunaris.digital/blog (200 OK)
        https://lunaris.digital/portfolio/trainings (200 OK)
        https://lunaris.digital/blog/articles/2025-04-23_pragmaticpm-issue-08-kanban-vs-scrum (
WARN-NEW: Strict-Transport-Security Header Not Set [10035] x 11
        https://lunaris.digital/ (200 OK)
        https://lunaris.digital/robots.txt (200 OK)
        https://lunaris.digital (200 OK)
        https://lunaris.digital/sitemap.xml (404 Not Found)
        https://lunaris.digital/portfolio/trainings (200 OK)
WARN-NEW: Content Security Policy (CSP) Header Not Set [10038] x 11
        https://lunaris.digital/ (200 OK)
        https://lunaris.digital (200 OK)
        https://lunaris.digital/sitemap.xml (404 Not Found)
        https://lunaris.digital/portfolio/trainings (200 OK)
        https://lunaris.digital/blog (200 OK)
```

OWASP ZAP

TESTING

Dynamisches Testen (DAST)

- Dynamic Application Security Testing
- OWASP ZAP, Burpsuite, Aikido, ...
- MITRE Caldera, MITRE ATT&CK

Security Tests

- Input Validation (NaughtyStrings)

Security Header Test

(External) Penetration Tests

BETRIEB

Secrets & Identity Management

- Secret Rotation
- Azure Key Vault
- Managed Identities

Monitoring & Threat Protection

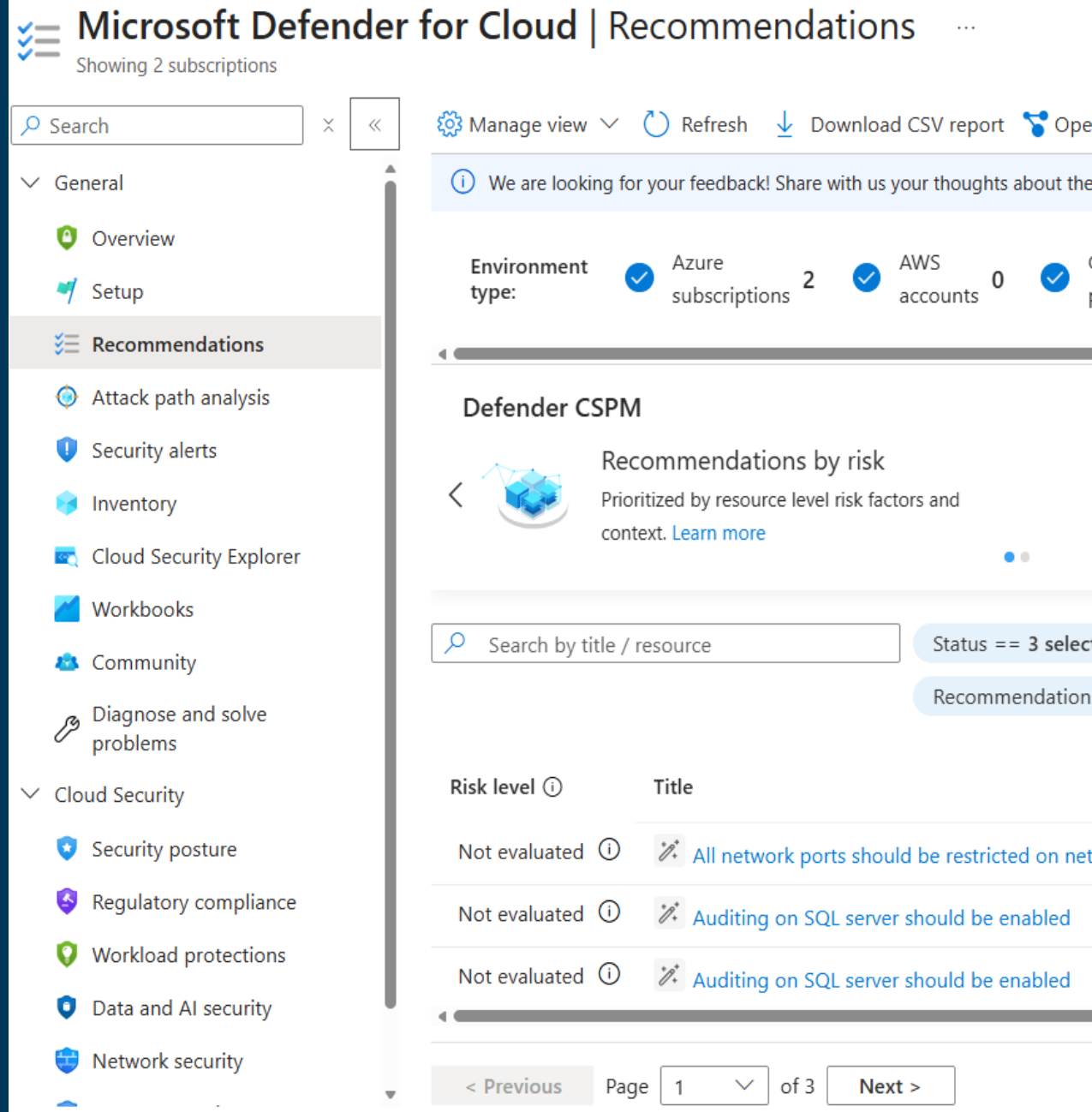
- Microsoft Defender for Cloud
- Microsoft Sentinel

Compliance & Governance

- Azure Policy
- Azure Log Analytics
- Data Masking & Encryption

Infrastruktur- & Netzwerk-Sicherheit

- Patch Management (VM, Container)
- Netzwerksegmentierung
- Customer Managed Keys




LUNARIS
Digital Solutions