@ChrFolini

Dr. Christian Folini

# Was IT-Sicherheit vom mittelalterlichen Burgenbau lernen kann

@ChrFolini

# Dr. Christian Folini

- Promovierter Mittelalterhistoriker mit einer Arbeit über die Sozialgeschichte der Deutschen Mystik

- Ehemaliger Präsident der Reenactment Gruppe Company of St. George

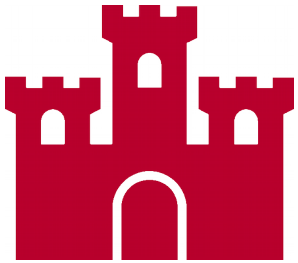
@ChrFolini

# Dr. Christian Folini

- Author des ModSecurity Handbuches, 2. Auflage
- Co-Lead des
  OWASP ModSecurity Core Rule Set Projekts
- Programmleiter Swiss Cyber Storm Konferenz
- Vize-Präsident Swiss Cyber Experts
- Über 10 Jahre Berufserfahrung in Cyber Security

# Programm

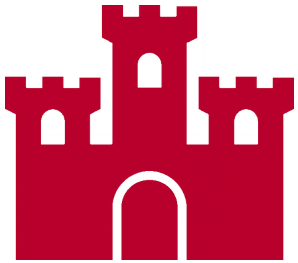
- 3 Probleme
- 3 Lösungen
- 3 sinnvolle Sicherheitspraktiken



@ChrFolini

# Problem 1

- Eine Schwachstelle genügt

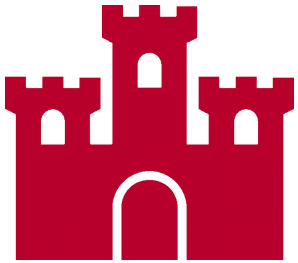


@ChrFolini

British Library
Royal 18 D II, f. 75r

# Problem 2

- Denial of Service

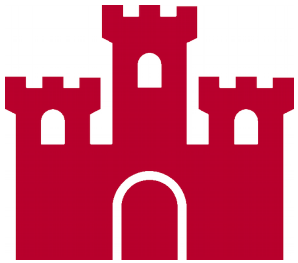


@ChrFolini

British Library
Royal 15 E I, f. 280v

# Problem 3

- Advanced Persistent Threat



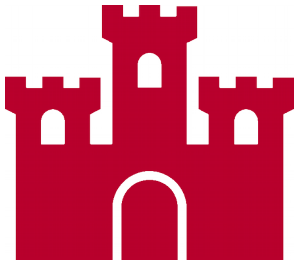
@ChrFolini

Victoria & Albert Museum
Miskina, Akbarnama

Victoria & Albert Museum
Miskina, Akbarnama, Detail

## Rob Joyce, NSA Tailored Access Operations

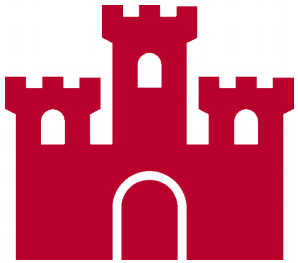
"The nation-state attackers? There's a reason it's called advanced persistent threats.
Because we'll poke and we'll poke. We'll wait and we'll wait and we'll wait, right? We're looking for that opportunity—that opening and that opportunity, to finish the mission."



@ChrFolini

# Lösung 1

- Flexibilität



@ChrFolini

Deutsche Schaller, um 1480

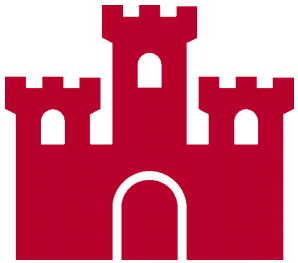
Deutsche Schaller, um 1480, Company of St. George

# Lösung 2

- Verteidigung in der Tiefe

  respektive:

- mehrere gestaffelte Verteidigungslinien
- unterschiedliche Sicherheitszonen



@ChrFolini

Burg Hochosterwitz, Kärnten
Südosten

Burg Hochosterwitz, Kärnten
Osten

Burg Hochosterwitz, Kärnten, Norden

Burg Hochosterwitz, Kärnten, Süden

Schloss Hallwyl, Aargau

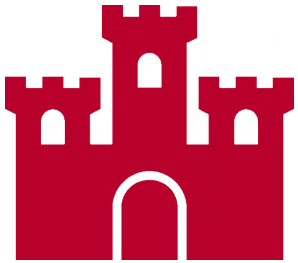
Schloss Chillon, Genfersee

# Lösung 3

- Whitelisting

  respektive:

- Positive Sicherheit
- Least Privilege Principle
- Positive Input Validation
- Reduction of Attack Surface



@ChrFolini

Metnitz, Kärnten

Metnitz, Kärnten

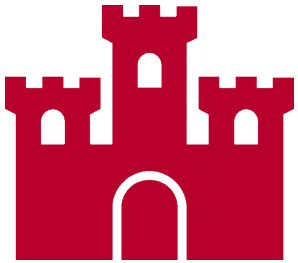
Waffentor, Hochosterwitz, Kärnten


# Nauders, Tirol

# Tower of London

# Sinnvolle Sicherheitspraxis 1

- Einspielen von Sicherheitsupdates



@ChrFolini

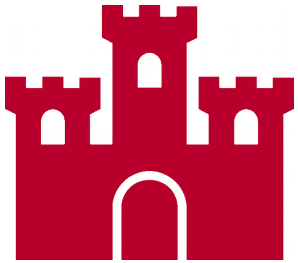
Castel de Pioz, Guadalajara

# Sinnvolle Sicherheitspraxis 2

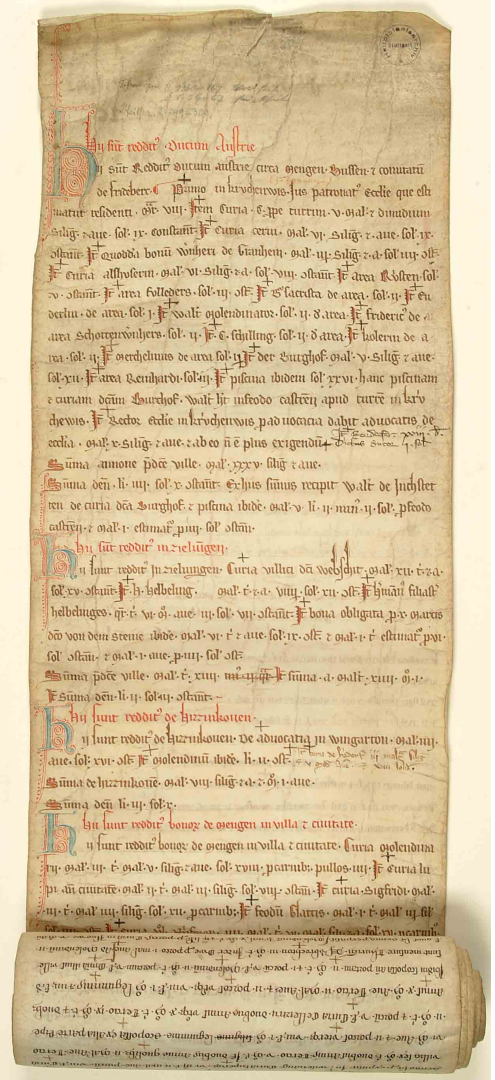
- Detailliertes Inventar

Respektive:

- Software Bill of Materials
- Dependency Tracking
- Exakte Netzwerkdiagramme

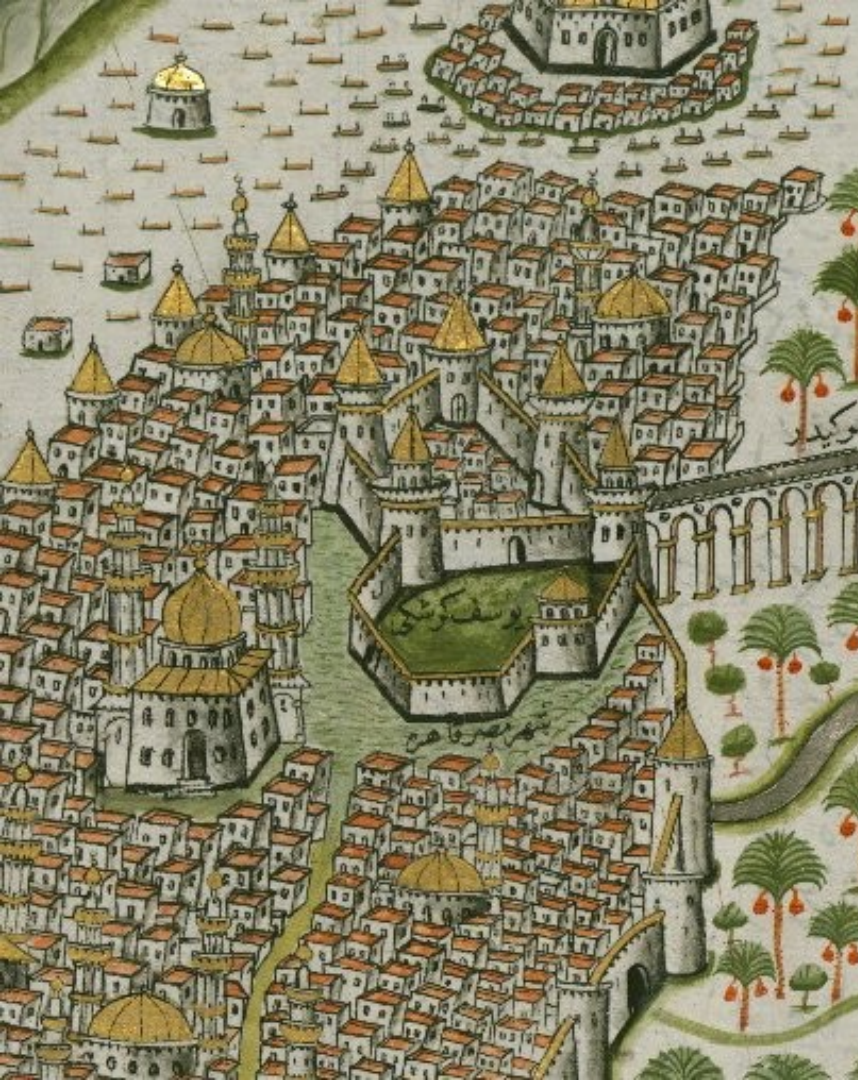


@ChrFolini



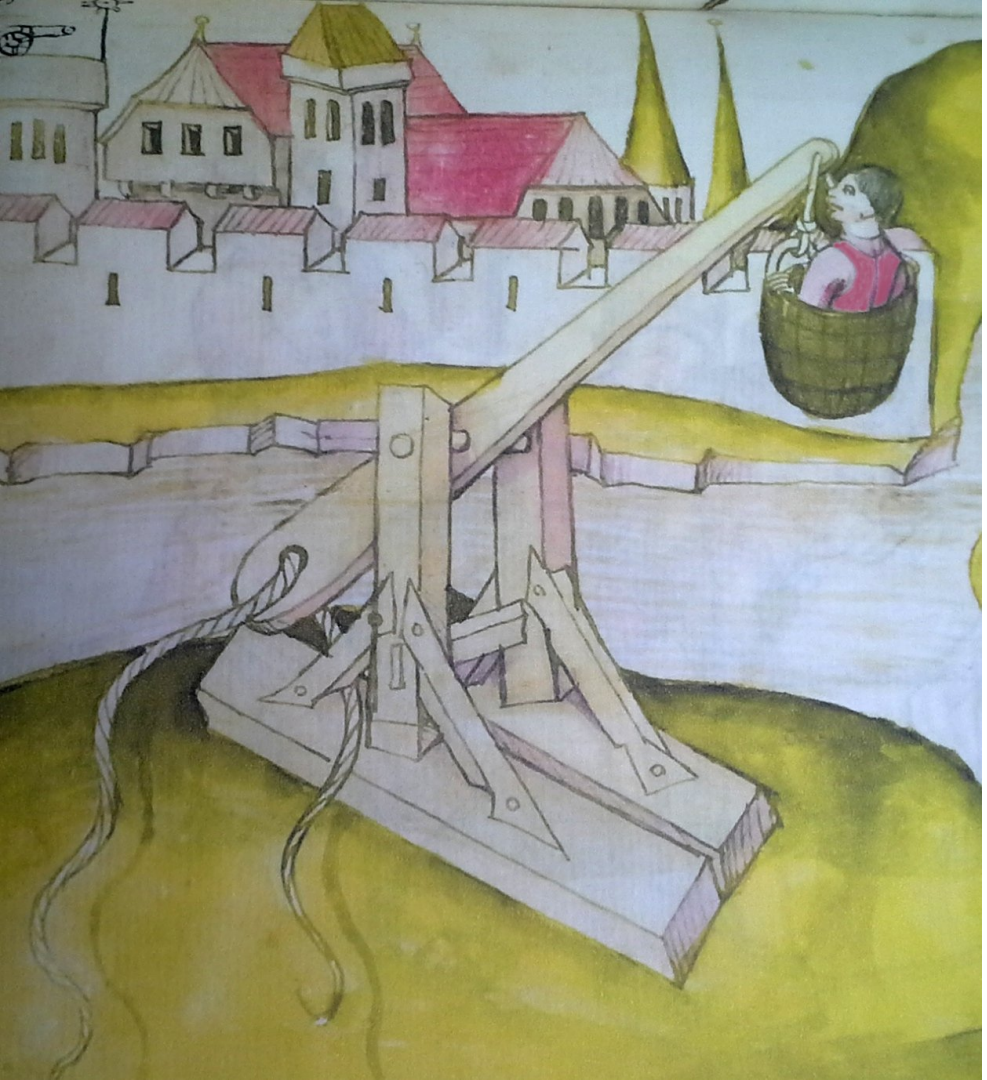
Habsburger Rotulus, um 1290
Hautpstaatsarchiv Stuttgart
H 162 Nr. 1


# Kairo, Karte des Piri Reis



Kairo, Karte des Piri Reis, Detail

Bellifortis, UB Frankfurt a.M.
Ms. germ. qu. 15, fol 61r



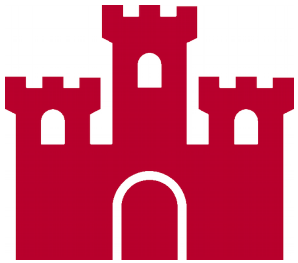
Bellifortis,
Det Kongelige Bibliotek
Copenhagen
MS Thott.290.2º, fol 22v

# Zusammenfassung

- Eine Schwachstelle genügt
- Denial of Service Attacken
- Advanced Persistent Threats

- Flexibilität
- Verteidigung in der Tiefe
- Whitelisting

- Einspielen von Sicherheitsupdates
- Detailliertes Inventar
- Bug Bounty Programme



@ChrFolini

@ChrFolini

# Dr. Christian Folini

- christian.folini@netnea.com
- @ChrFolini
- https://www.christian-folini.ch