Castle Defense 101

(aka Threat Modeling)

Bärnau Motte, Germany

"Die slawische Frühmittelaltersiedlung im Geschichtspark Bärnau-Tachov mit der Motte im Vordergrund"
by Barbara Brunner, used under CC BY-SA 3.0/ Cropped from original
https://commons.wikimedia.org/wiki/File:Motte_mit_Dorf.jpg

“Geschichtspark Bärnau-Tachov im Jahr 2017” by Klaus Schicker, used under CC BY 4.0/ Cropped from original
https://commons.wikimedia.org/wiki/File:Geschichtspark-Baernau-Luftaufnahme.jpg

“Think like an attacker” considered harmful

Gravensteen, Belgium

“Gravensteen ("Castle of the Counts") during golden hour in Ghent” by Trougnouf (Benoit Brummer), used under CC BY 4.0/ Cropped from original
https://commons.wikimedia.org/wiki/File:Gravensteen,_Ghent_(DSCF0191).jpg

Alcatraz Island, US

“View of Alcatraz Island in August 2021” by Chris6d, used under CC BY-SA 4.0/ Cropped from original
https://commons.wikimedia.org/wiki/File:Alcatraz_2021.jpg

@OtherDevOpsGene #techbash

- What are we protecting?
- Why are we protecting it?
- How might it be compromised?
- What happens if we fail to protect it?
- How will we react/respond and move on?

Edinburgh Castle, Scotland

"Edinburgh Castle entraince" by Graham van der Wielen, used under CC BY 2.0/ Cropped from original
https://commons.wikimedia.org/wiki/File:Edinburgh_-_Old_City_-_Edinburgh_Castle_(2962379502).jpg

Shostack's 4 Question Frame for Threat Modeling

https://github.com/adamshostack/4QuestionFrame

1. What are we working on?
2. What can go wrong?
3. What are we going to do about it?
4. Did we do a good job?

Segovia Castle, Spain

"Fotografía nocturna del Alcázar de Segovia" by Ángel Sanz Andrés, used under CC BY-SA 4.0/ Cropped from original
https://commons.wikimedia.org/wiki/File:Fotograf%C3%ADa_nocturna_del_Alc%C3%A1zar_de_Segovia.jpg

“Clouds in Russia.” by Dmitry Makeev,
used under CC BY-SA 4.0
https://commons.wikimedia.org/wiki/File:Clouds_in_Russia._img_469.jpg

@OtherDevOpsGene #techbash
Castel del Monte, Italy
“Italy, Castel del Monte” by Berthold Werner, used under CC BY-SA 3.0/ Cropped from original
https://commons.wikimedia.org/wiki/File:Castel_del_Monte_BW_2016-10-14_13-15-58.jpg

Castel del Monte, Italy

“Castel del Monte fotografato con mavic mini 2” by D.belfiore, used under CC BY-SA 4.0/ Cropped from original
https://commons.wikimedia.org/wiki/File:Castel_del_monte_la_corona_di_Puglia.jpg

Zero trust assumptions

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

- The entire enterprise private network is not considered an implicit trust zone
- Devices on the network may not be owned or configurable by the enterprise
- No resource is inherently trusted
- Not all enterprise resources are on enterprise-owned infrastructure
- Remote enterprise subjects and assets cannot fully trust their local network connection
- Assets and workflows moving between enterprise and non-enterprise infrastructure should have a consistent security policy and posture

Ludlow Castle, England

"Ludlow Castle" by Philip Pankhurst, used under CC BY-SA 2.0/ Cropped and darkened from original
https://commons.wikimedia.org/wiki/File:Ludlow_Castle_-_geograph.org.uk_-_2445657.jpg

Krak des Chevaliers Castle, Syria

“Krak des Chevaliers Castle, Syria” by Vyacheslav Argenberg / http://www.vascoplanet.com/, used under CC BY 4.0
https://commons.wikimedia.org/wiki/File:Krak_des_Chevaliers_Castle,_Syria.jpg

@OtherDevOpsGene #techbash

Top 10 Ordered Ways of Attacking Strong Places

Vajdahunyad Castle, Hungary

"Vajdahunyad Castle in the City Park, Budapest" by Lessormore, used under CC BY 4.0 / Darkened from original
https://commons.wikimedia.org/wiki/File:Vajdahunyad_castle_40.jpg

Rousanou Monastery, Greece

"Rousanou Monastery" by Paul Stephenson, used under CC BY 2.0/ Cropped from original
https://commons.wikimedia.org/wiki/File:Rousanou_Monastery,_Meteora,_Greece_(15148627963).jpg

Impact vs. Likelihood

Impact	Likelihood				
	“Never”	Unlikely	Possible	Probable	Certain
Catastrophic					
Major					
Moderate					
Minor					
“Insignificant”					

“Clouds in Russia.” by Dmitry Makeev, used under CC BY-SA 4.0
https://commons.wikimedia.org/wiki/File:Clouds_in_Russia._img_421.jpg

@OtherDevOpsGene #techbash
Great Wall of China
“The Great Wall of China” by Jorge Láscar, used under CC BY 2.0/ Cropped from original
https://commons.wikimedia.org/wiki/File:Lascar_The_Great_Wall_of_China_(4475570857).jpg

@OtherDevOpsGene #techbash
THE CLUB

Addressing threats

- Mitigate the threat
- Eliminate the threat
- Transfer the threat
- Accept the risk

Fortress of Città di San Marino

"The fortress of Città di San Marino" by Max_Ryazanov, used under CC BY-SA 3.0/ Cropped from original https://commons.wikimedia.org/wiki/File:Fortress_of_Guaita_2013-09-19.jpg

Framlingham Castle, England

“Postern Gate at Framlingham Caste” by Foshie, used under CC BY 2.0/ Cropped from original
https://commons.wikimedia.org/wiki/File:Framlingham_Castle_Postern_Gate.jpg

Framlingham Castle, England

"Framlingham Castle, Suffolk, England" by Dave Briggs, used under CC BY-SA 2.0/ Cropped from original
https://commons.wikimedia.org/wiki/File:Framlingham_Castle_-Suffolk-8.jpg

Threat Modeling Manifesto

https://www.threatmodelingmanifesto.org/

The best use of threat modeling is to improve the security and privacy of a system through early and frequent analysis.

Threat modeling does not depend on one's innate ability or unique mindset; everyone can and should do it.

Bishop's Palace, England

"Moat and drawbridge at the Bishop's Palace, Wells" by Jeff Buck, used under CC BY-SA 2.0/ Cropped from original
https://commons.wikimedia.org/wiki/File:Moat_and_drawbridge_at_the_Bishop%27s_Palace,_Wells_-_geograph.org.uk_-_2730887.jpg

@OtherDevOpsGene #techbash
Eilean Donan Castle, Scotland
“Panorama Eilean Donan Castle” by Stefan Krause, Germany, used under License Art Libre/ Cropped from original
https://commons.wikimedia.org/wiki/File:Eilean_Donan_Castle_Panorama.jpg

@OtherDevOpsGene #techbash

ISBN-13 978-1118809990
https://a.co/d/1Z9cp44

"Clouds in Russia." by Dmitry Makeev, used under CC BY-SA 4.0
https://commons.wikimedia.org/wiki/File:Clouds_in_Russia._img_384.jpg

STRIDE

- Spoofing
  - Pretending to be someone or something you are not
- Tampering
  - Changing data
- Repudiation
  - Not being able to prove you wrote it
- Information Disclosure
  - Data leak
- Denial of Service
  - Making a service unusable
- Elevation of Privilege
  - Gaining permissions you are not entitled to

Taureau Fort, France

"Le château du Taureau en baie de Morlaix" by Thesupermat, used under CC BY-SA 3.0/ Cropped and darkened from original
https://commons.wikimedia.org/wiki/File:Plouezoc%27h_-_Ch%C3%A2teau_du_Taureau_-_PA00090226_-_032.jpg

Resources

- STRIDE
  - https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats
- OWASP Threat Dragon
  - https://www.threatdragon.com/
- PASTA
  - https://versprite.com/blog/what-is-pasta-threat-modeling/
- CAIRIS
  - https://cairis.org/
- Threagile
  - https://threagile.io/
- ThreatModeler
  - https://threatmodeler.com/

Bodiam Castle, England

"Bodiam Castle" by JamCor, used under CC BY-SA 4.0/ Cropped from original
https://commons.wikimedia.org/wiki/File:Bodiam_Castle_East_Sussex.jpg

Key takeaways

- Brainstorm attacks and defenses
- What are you protecting?
- Balance your resources and time
- Everyone can and should threat model
- Iterate- “early and frequent analysis”

Neuschwanstein Castle, Germany

“Neuschwanstein Castle from Marienbrücke Bridge - June 2014” by GeoMechain, used under CC BY-SA 4.0/ Cropped from original
https://commons.wikimedia.org/wiki/File:Neuschwanstein_Castle_from_Marienbr%C3%BCcke_Bridge.jpg

Questions?

Gene Gotimer
Principal DevOps Engineer at Praeses, LLC
@OtherDevOpsGene

Himeji Castle, Japan

"Himeji Castle, Japan" by Gorgo
https://commons.wikimedia.org/wiki/File:Himeji_Castle_0804_1.jpg

Practice idea

Threat model an alien invasion
as a tabletop or lunchtime exercise

"Grainy B&W image of supposed UFO over Passaic in New Jersey" by George Stock, public domain/ Cropped from original
https://commons.wikimedia.org/wiki/File:Supposed_UFO,_Passaic,_New_Jersey.jpg