BRIDGING THE DEV-SEC DIVIDE

Three Tips for Agile Developers

Luisa Emme @emmeblm

BERLIN · HELSINKI · LONDON · MUNICH · STOCKHOLM · STUTTGART · TAMPERE

futurice

> It is no longer a question of whether an organization will be hacked. It is simply a question of when

European Voice of Directors, Cyber-Risk Oversight 2020

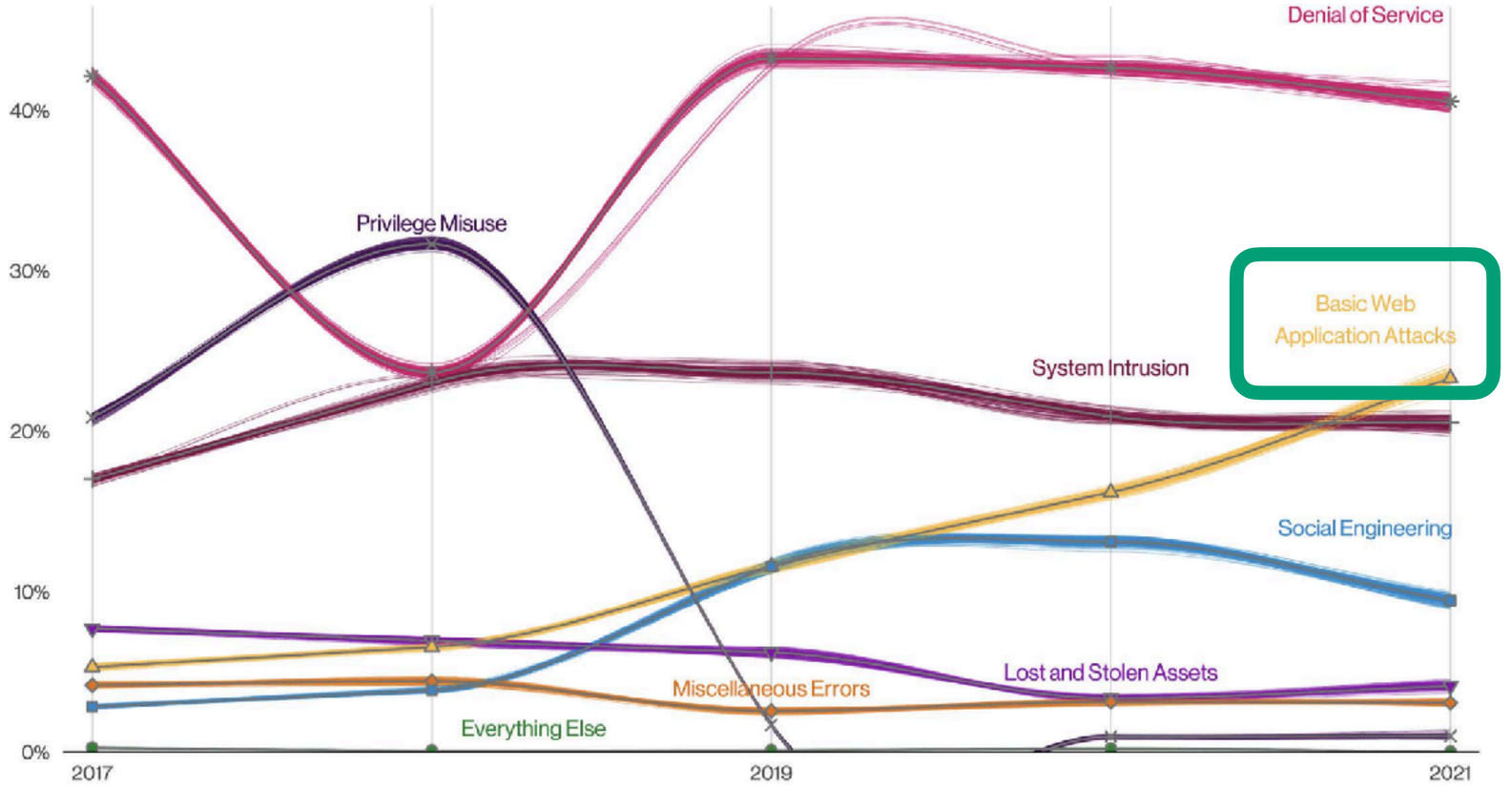
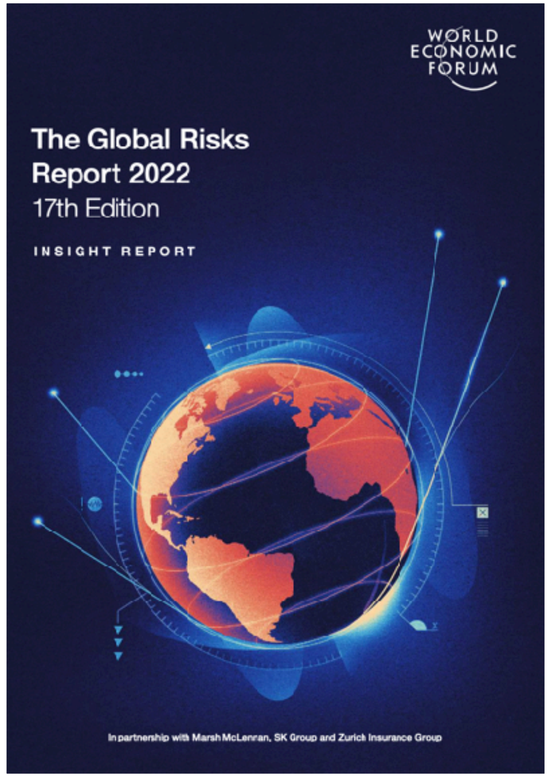


Figure 32. Patterns over time in incidents

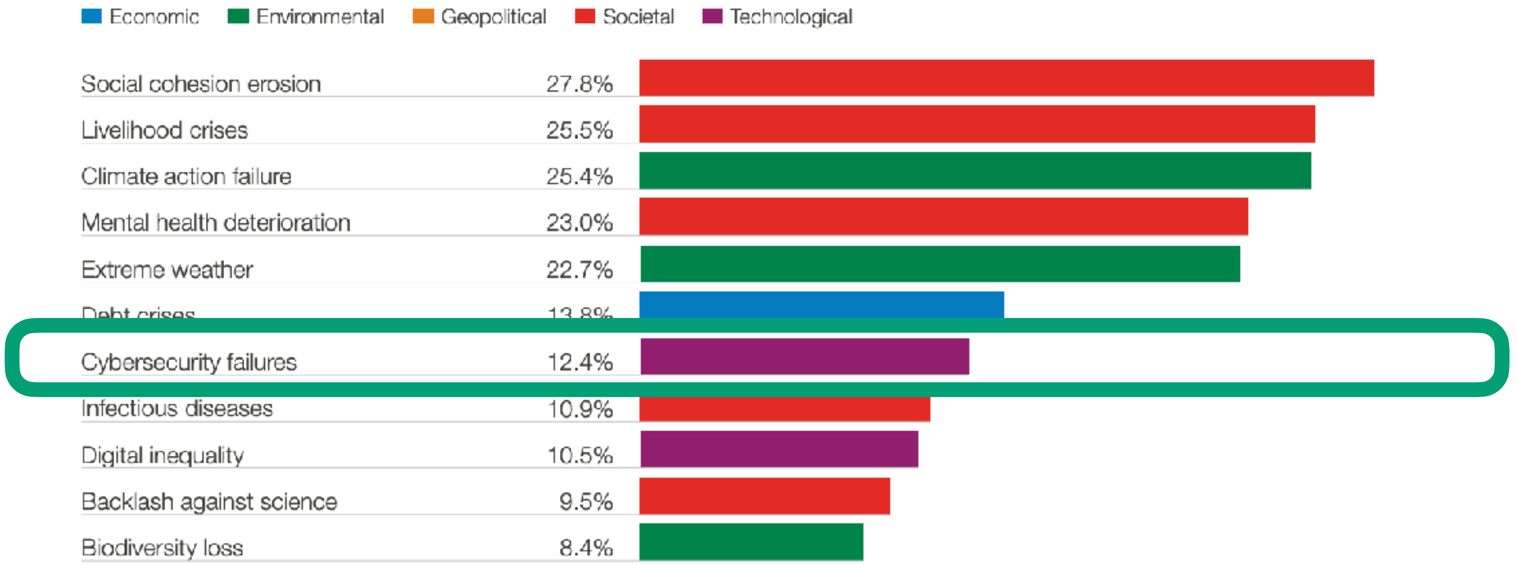


"Growing digital dependency will intensify cyberthreats"

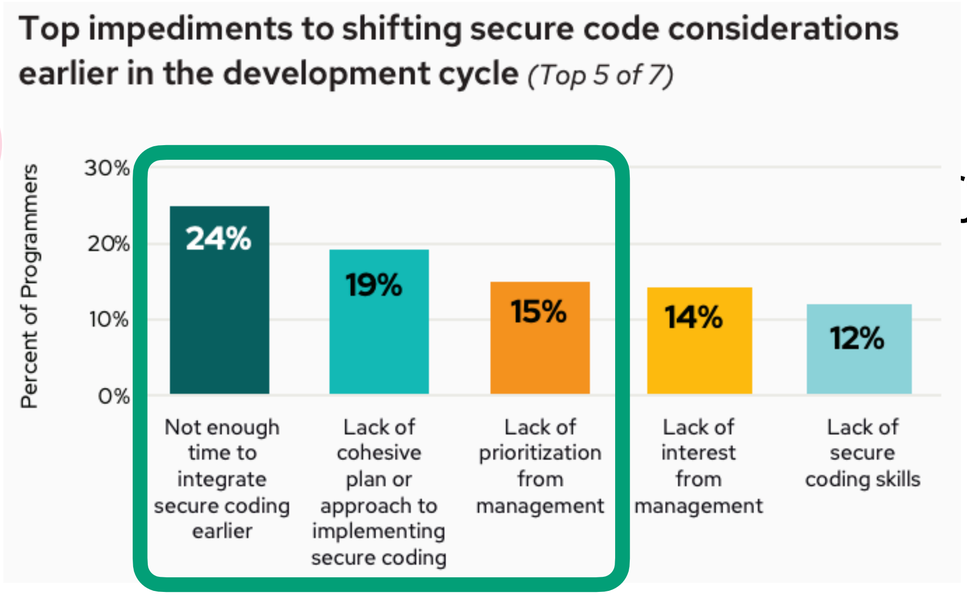
FIGURE I

COVID-19 Hindsight

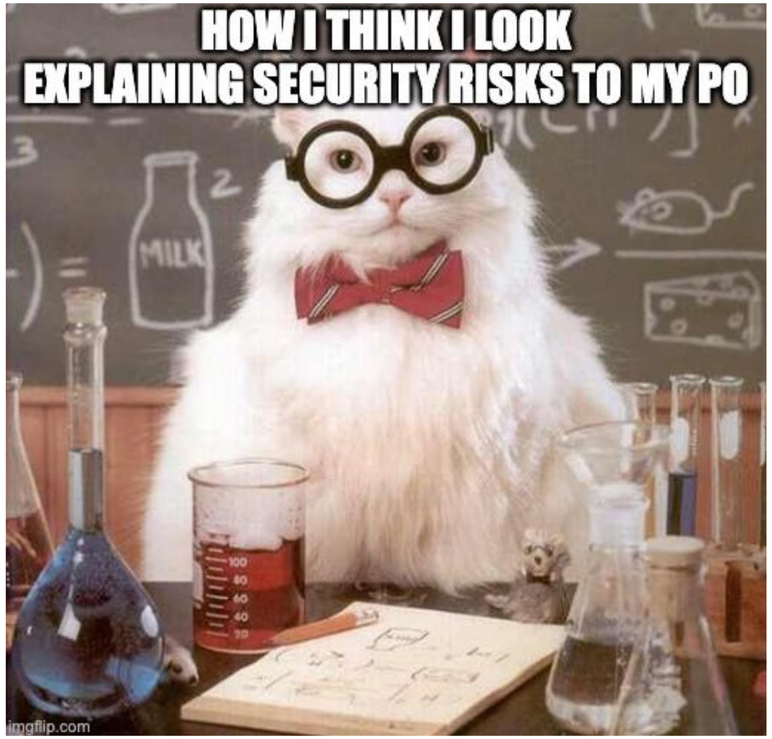
Risks that worsened the most since the start of the COVID-19 crisis

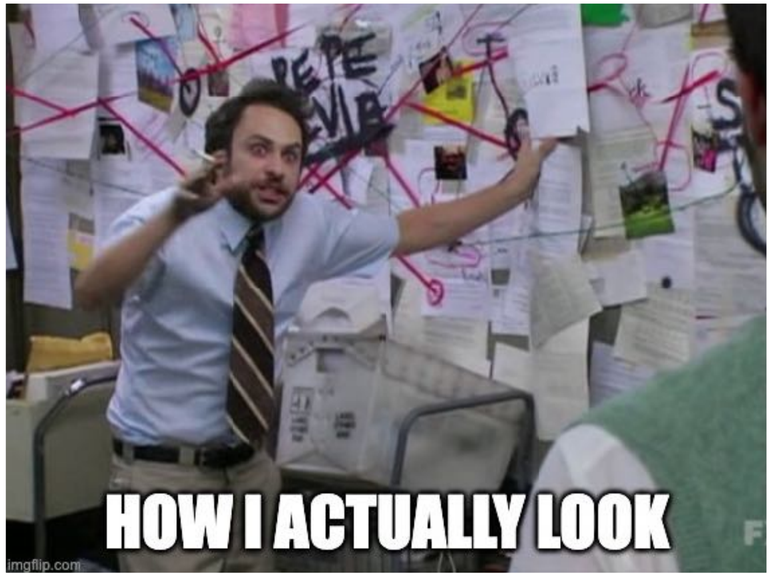


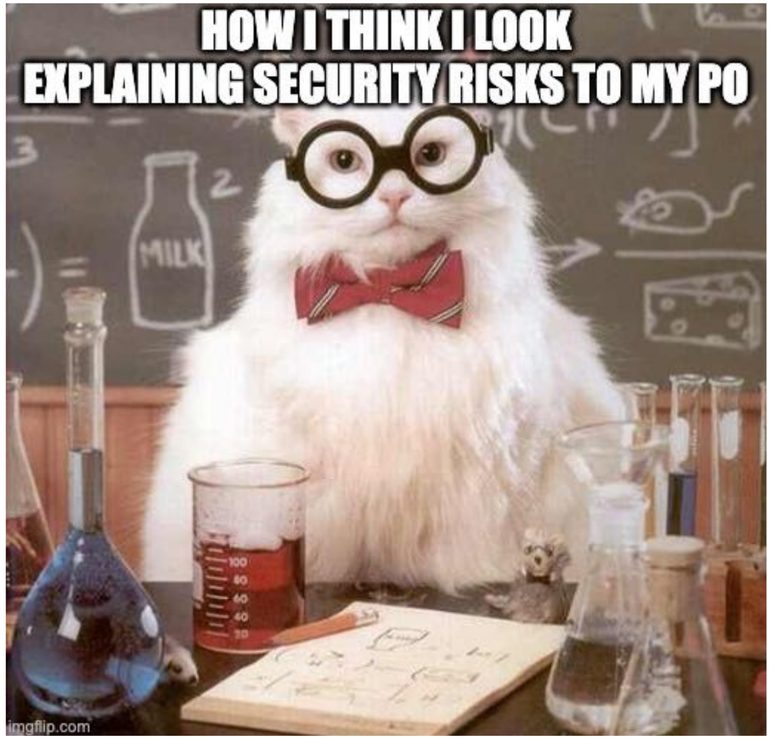
"Cybersecurity is increasingly a priority for leaders"

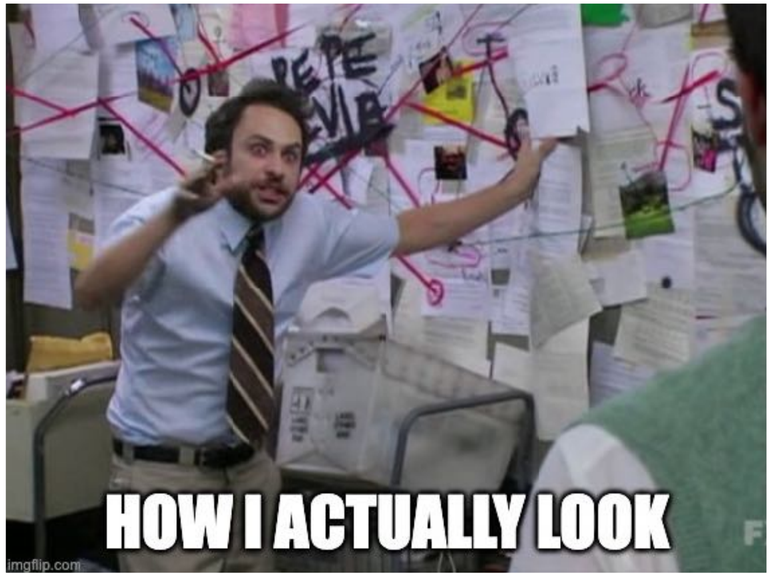


ycles"


HOW I THINK I LOOK
EXPLAINING SECURITY RISKS TO MY PO
MILK
imgflip.com


HOW I ACTUALLY LOOK
imgflip.com

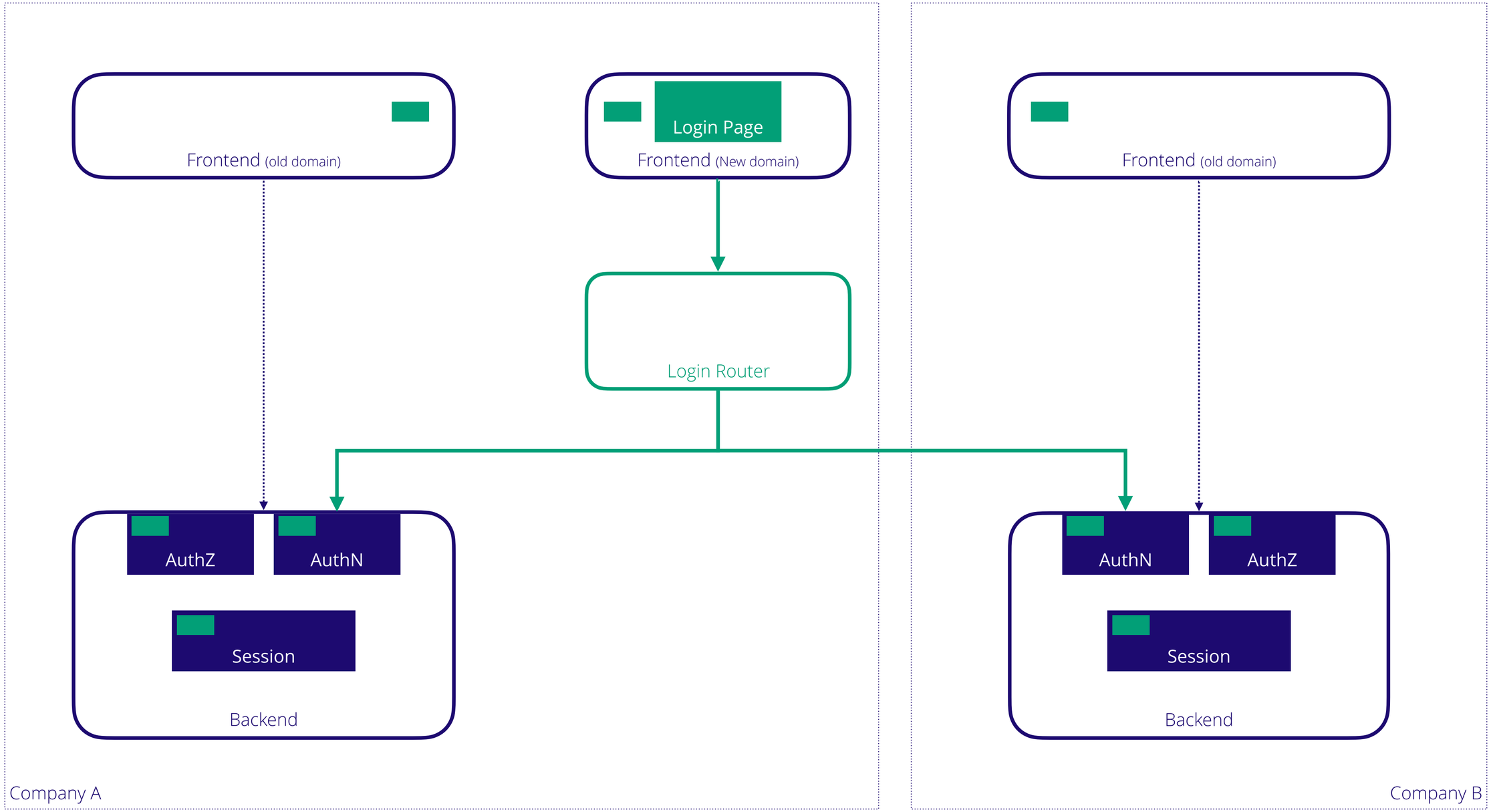

HOW I THINK I LOOK
EXPLAINING SECURITY RISKS TO MY PO
MILK
imgflip.com

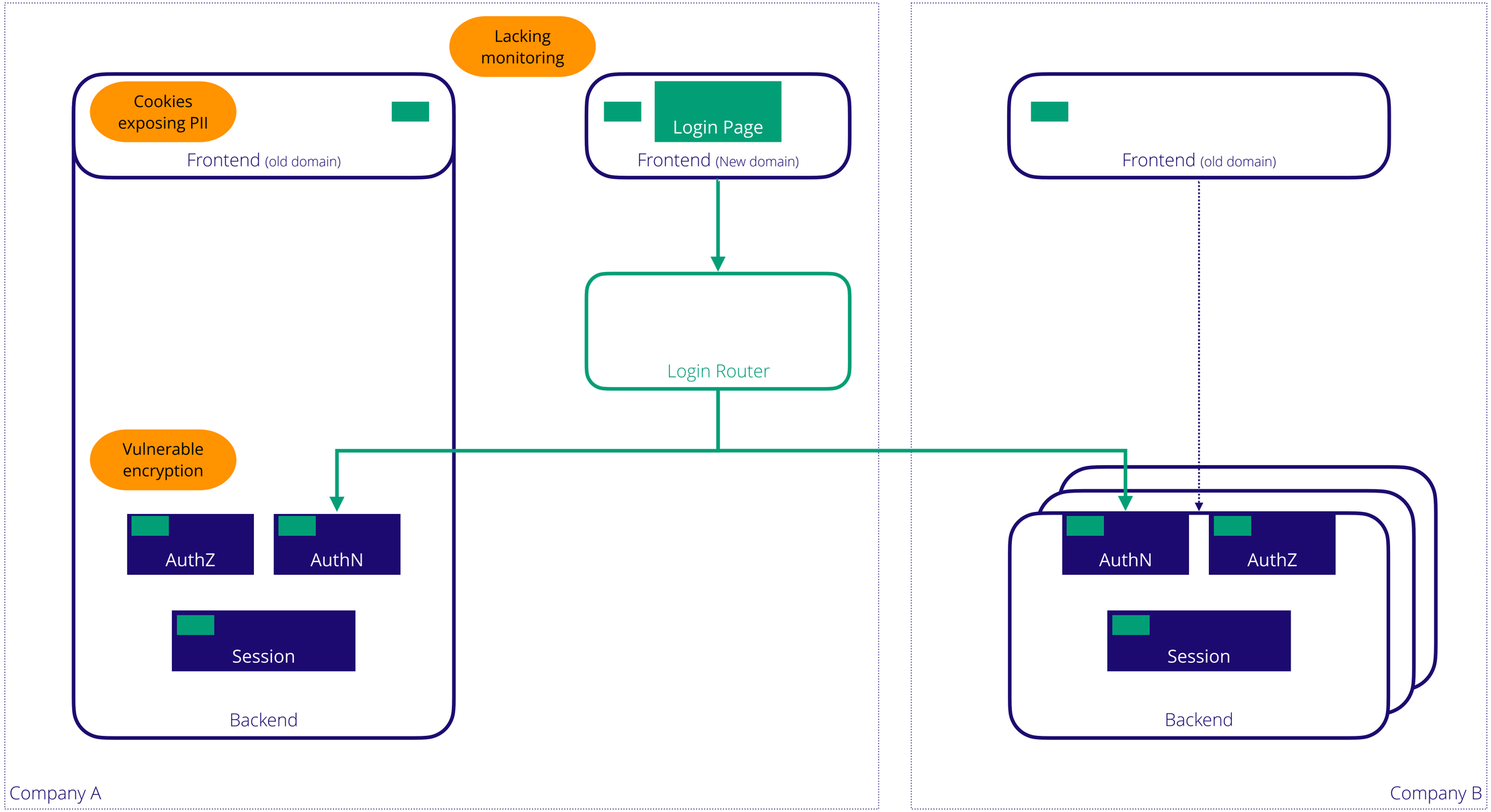

HOW I ACTUALLY LOOK
imgflip.com

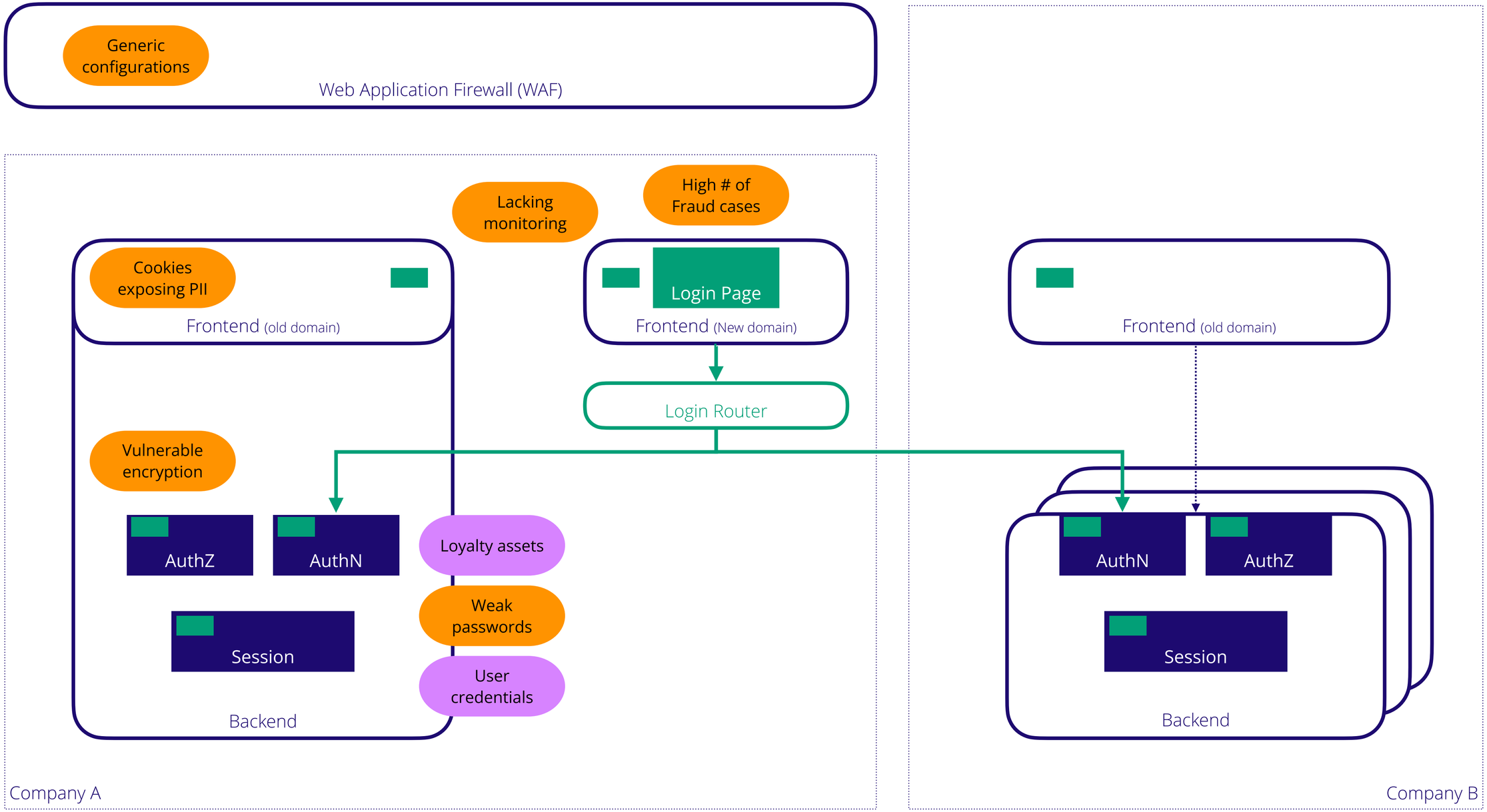
WHY ARE YOU TALKING ABOUT
CYBERSECURITY?
imgflip.com

THIS IS FINE.

Discover the real and active threats in your products


Frontend (old domain)
Login Page
Frontend (New domain)
Frontend (old domain)
Login Router
AuthZ
AuthN
Session
Backend
AuthN
AuthZ
Session
Backend
Company A
Company B

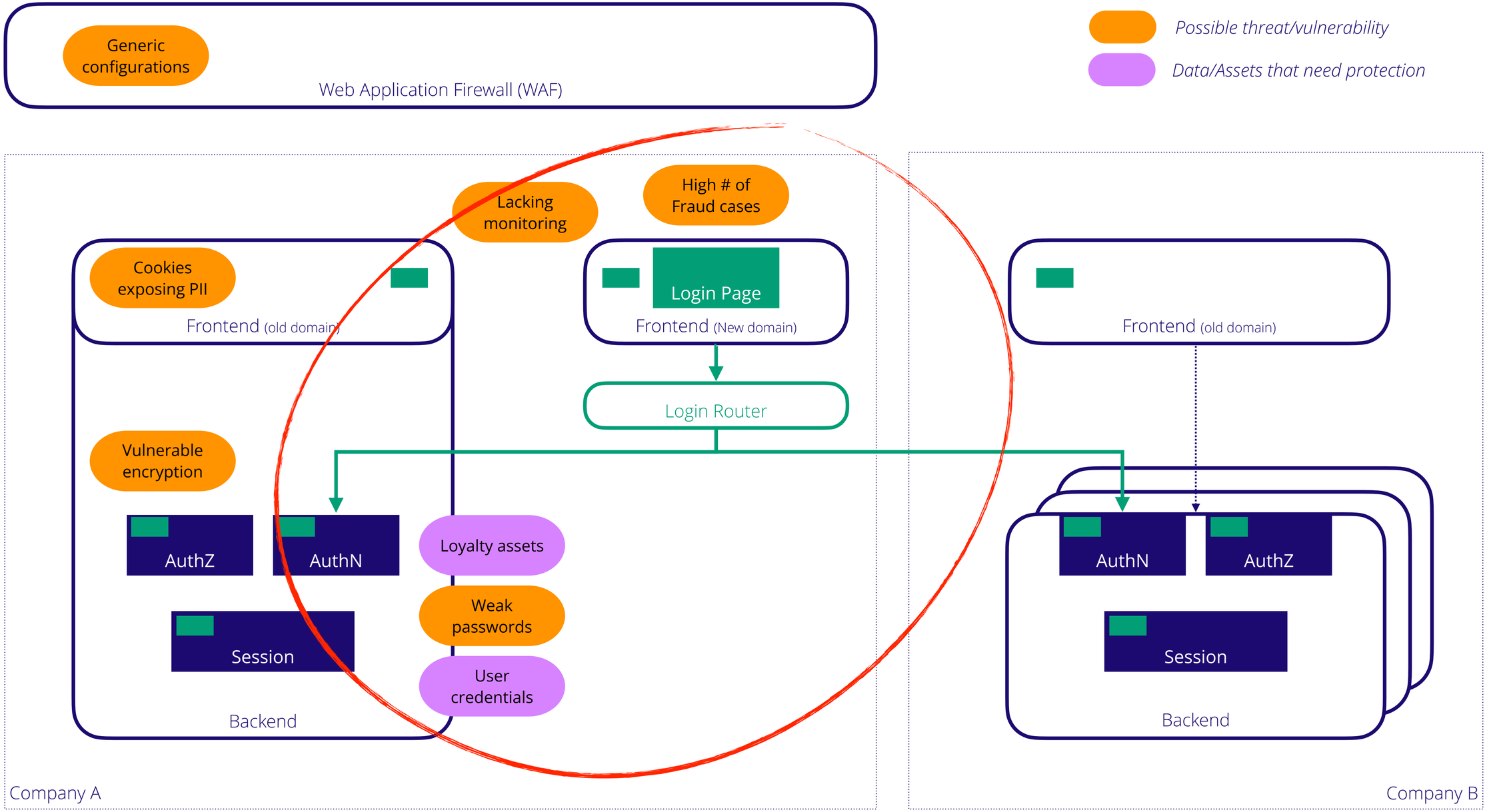

Lacking monitoring
Cookies exposing PII
Frontend (old domain)
Login Page
Frontend (New domain)
Login Router
Vulnerable encryption
AuthZ
AuthN
Session
Backend
Company A
Frontend (old domain)
AuthN
AuthZ
Session
Backend
Company B

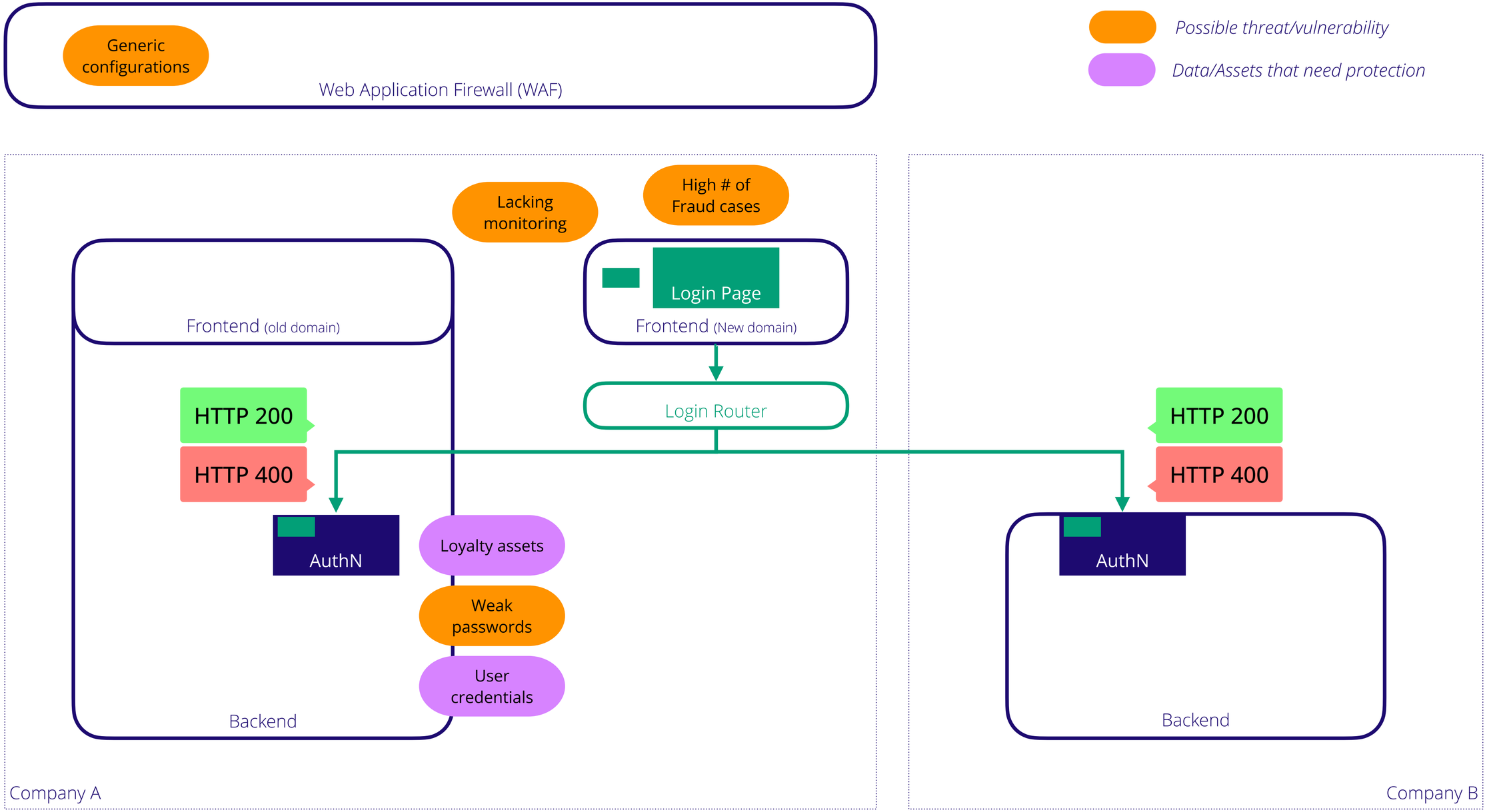

Generic configurations
Web Application Firewall (WAF)
Lacking monitoring
High # of Fraud cases
Cookies exposing PII
Frontend (old domain)
Login Page
Frontend (New domain)
Login Router
Vulnerable encryption
AuthZ
AuthN
Loyalty assets
Weak passwords
User credentials
Session
Backend
Company A
Frontend (old domain)
AuthN
AuthZ
Session
Backend
Company B

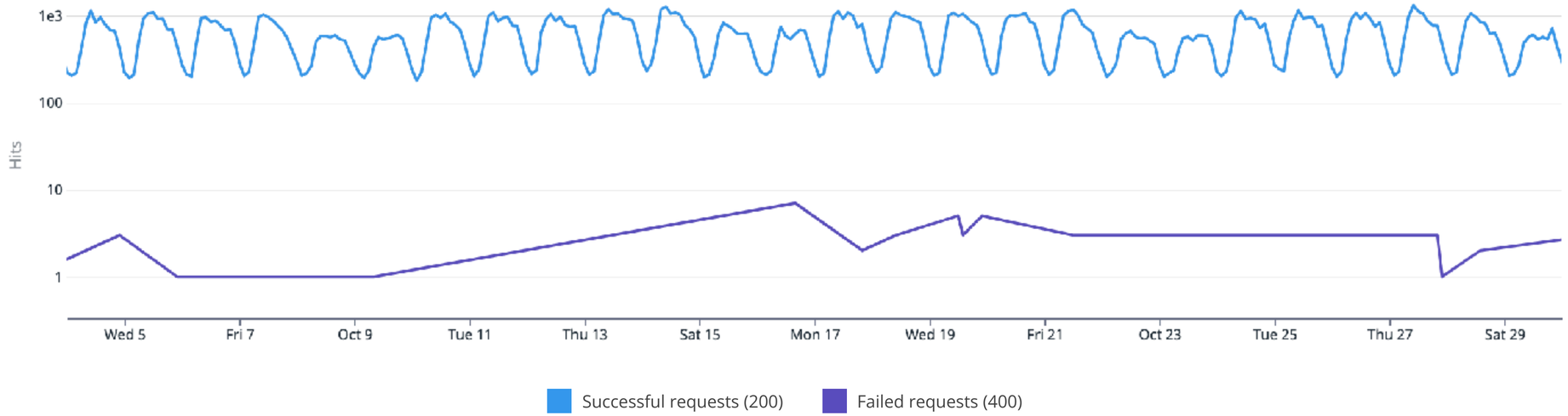
FIRST TIP

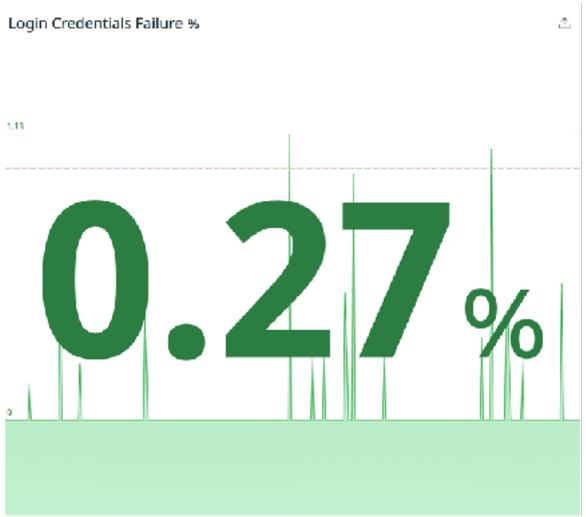
Threat Modeling is your go-to tool

Martin Fowler’s Blog: A Guide to Threat Modeling for Developers by Jim Gumbley

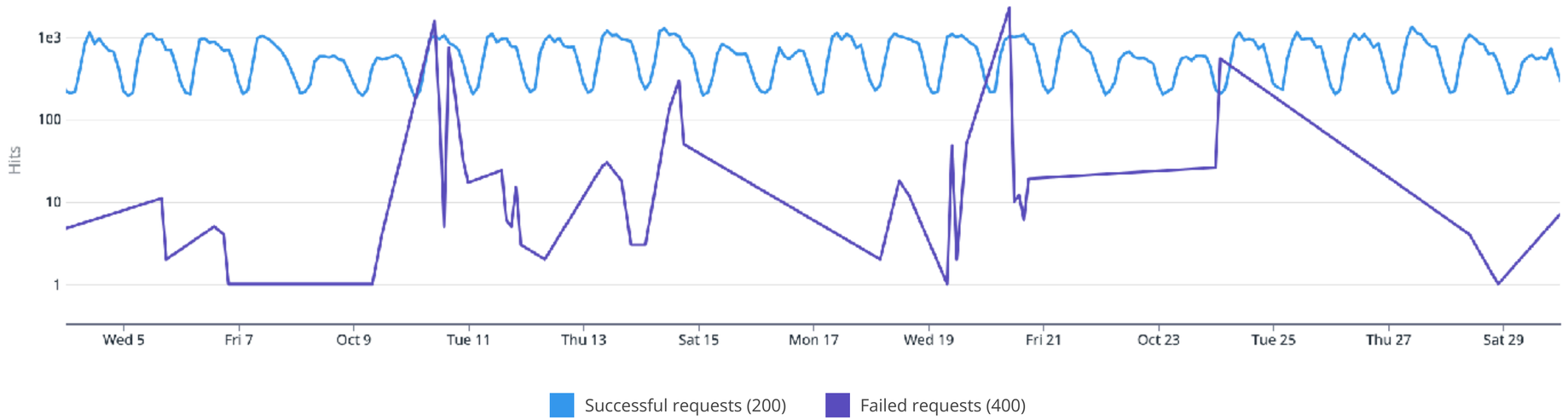

Generic configurations
Web Application Firewall (WAF)
Possible threat/vulnerability
Data/Assets that need protection
Lacking monitoring
High # of Fraud cases
Cookies exposing PII
Frontend (old domain)
Login Page
Frontend (New domain)
Login Router
Vulnerable encryption
AuthZ
AuthN
Loyalty assets
Weak passwords
User credentials
Session
Backend
Company A
Frontend (old domain)
AuthN
AuthZ
Session
Backend
Company B

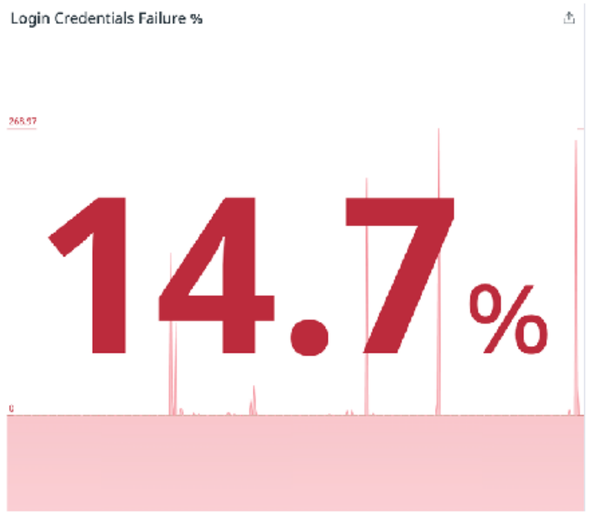

Generic configurations
Web Application Firewall (WAF)
Possible threat/vulnerability
Data/Assets that need protection
Lacking monitoring
High # of Fraud cases
Login Page
Frontend (New domain)
Frontend (old domain)
Login Router
HTTP 200
HTTP 400
AuthN
Loyalty assets
Weak passwords
User credentials
Backend
HTTP 200
HTTP 400
AuthN
Backend
Company A
Company B





*Reference graphs





*Reference graphs

SECOND TIP

Detecting malicious activity is a key part of building security

STRIDE Framework (learn.microsoft.com)

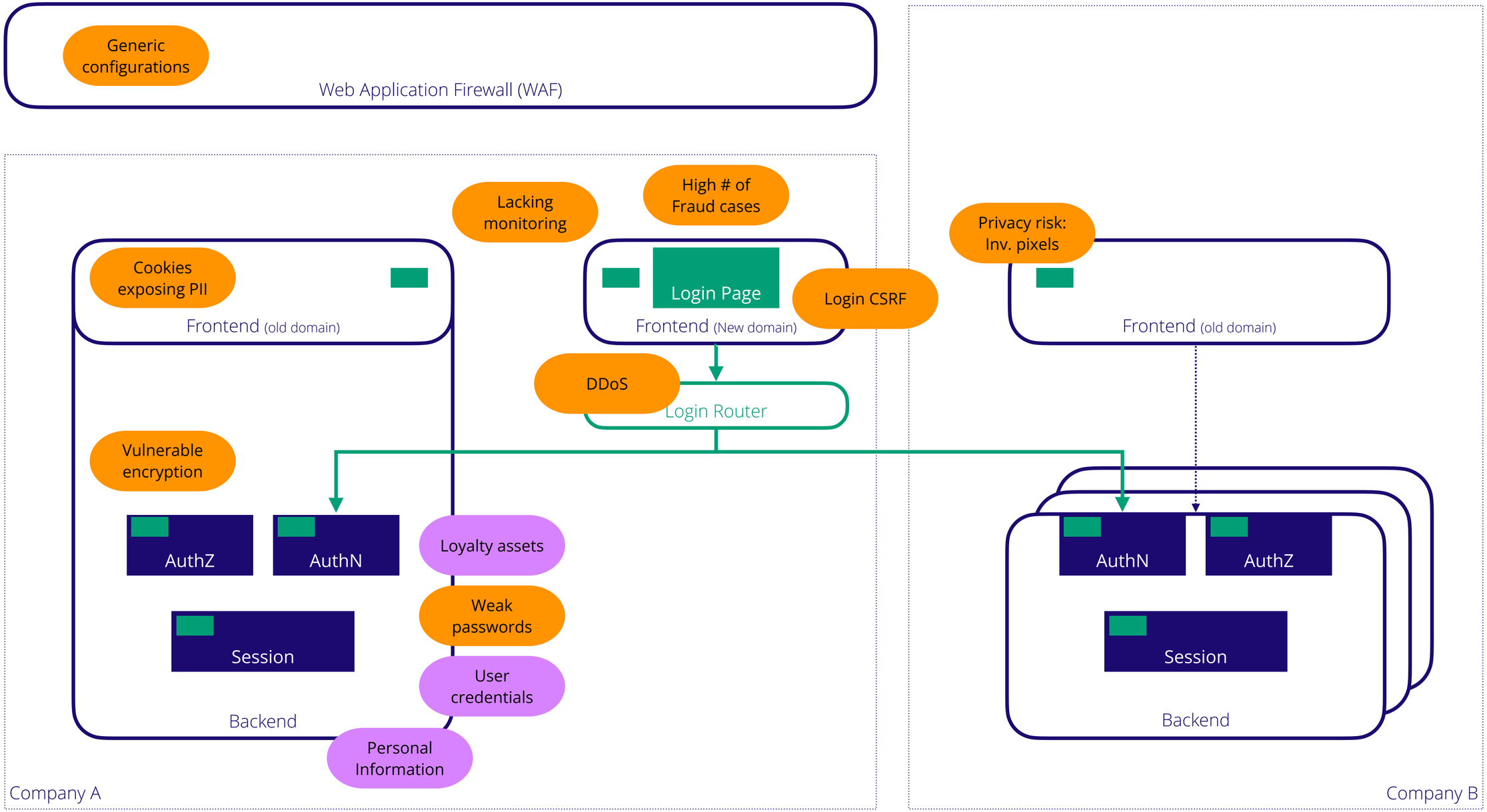
imgflip.com

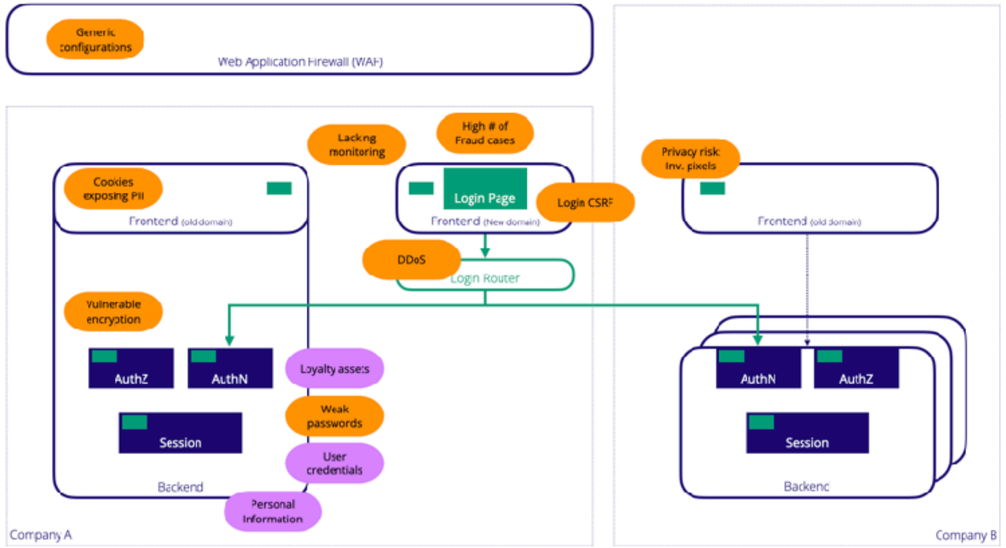
SAY WHAT?
imgflip.com

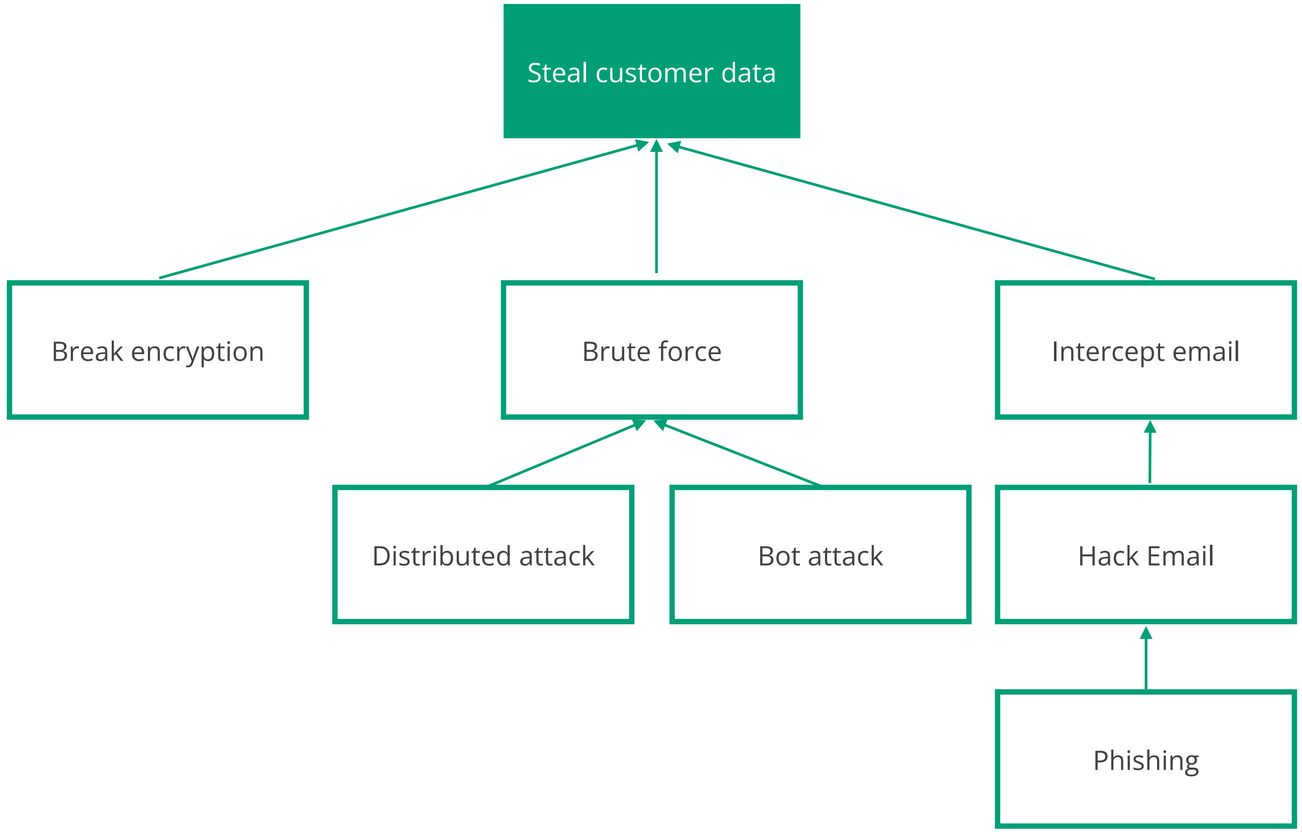
imgflip.com

imgflip.com

imgflip.com


Generic configurations
Web Application Firewall (WAF)
Lacking monitoring
High # of Fraud cases
Privacy risk: Inv. pixels
Cookies exposing PII
Frontend (old domain)
Login Page
Frontend (New domain)
Login CSRF
Frontend (old domain)
DDoS
Login Router
Vulnerable encryption
AuthZ
AuthN
Loyalty assets
Weak passwords
User credentials
Personal Information
Session
Backend
AuthN
AuthZ
Session
Backend
Company A
Company B





Definition of
"Ready for Development"

Security ACs

THIRD TIP

Share your knowledge

Discover the real and active threats in your products

THANKS
DANKE
GRACIAS

Luisa Emme
@emmeblm
www.futurice.com

futurice

Co-creating a resilient future

Sign up to our DevBreakfast Newsletter
for a monthly dose of the latest in tech!

SCAN ME