5 Taktiken wie Angreifer Security-Analysen aushebeln

splunk>

Board Meeting

(1) Improve Digital Resilience - Establish and Operate a 24x7 SOC
Vote Results: 12x Yes / 0x No

(...)

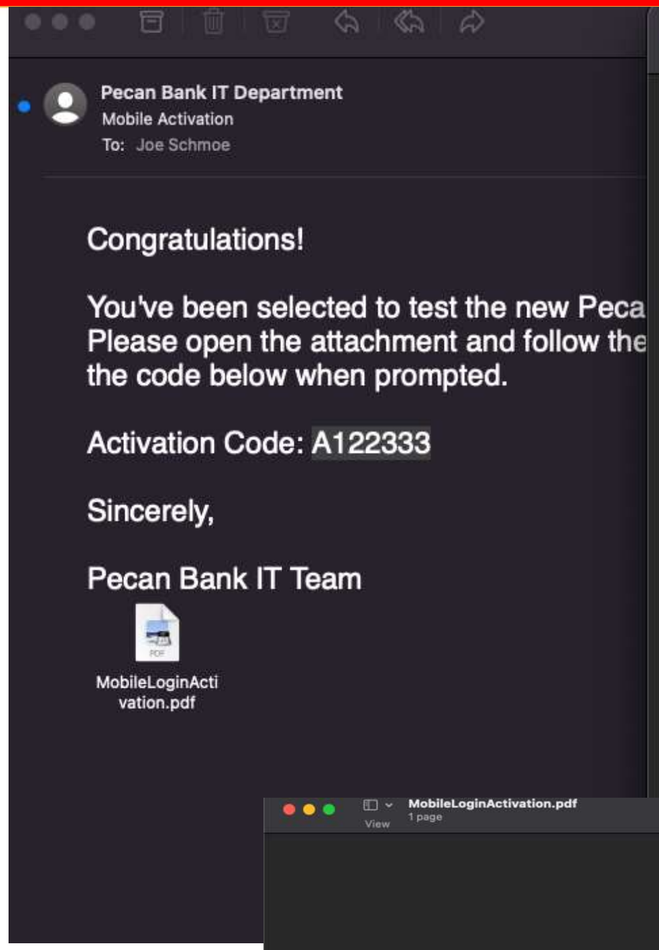
Analyse: Investigate **developed resources** used for initial access attempts
Respond: Adjust security tools to prevent and block **developed resources**

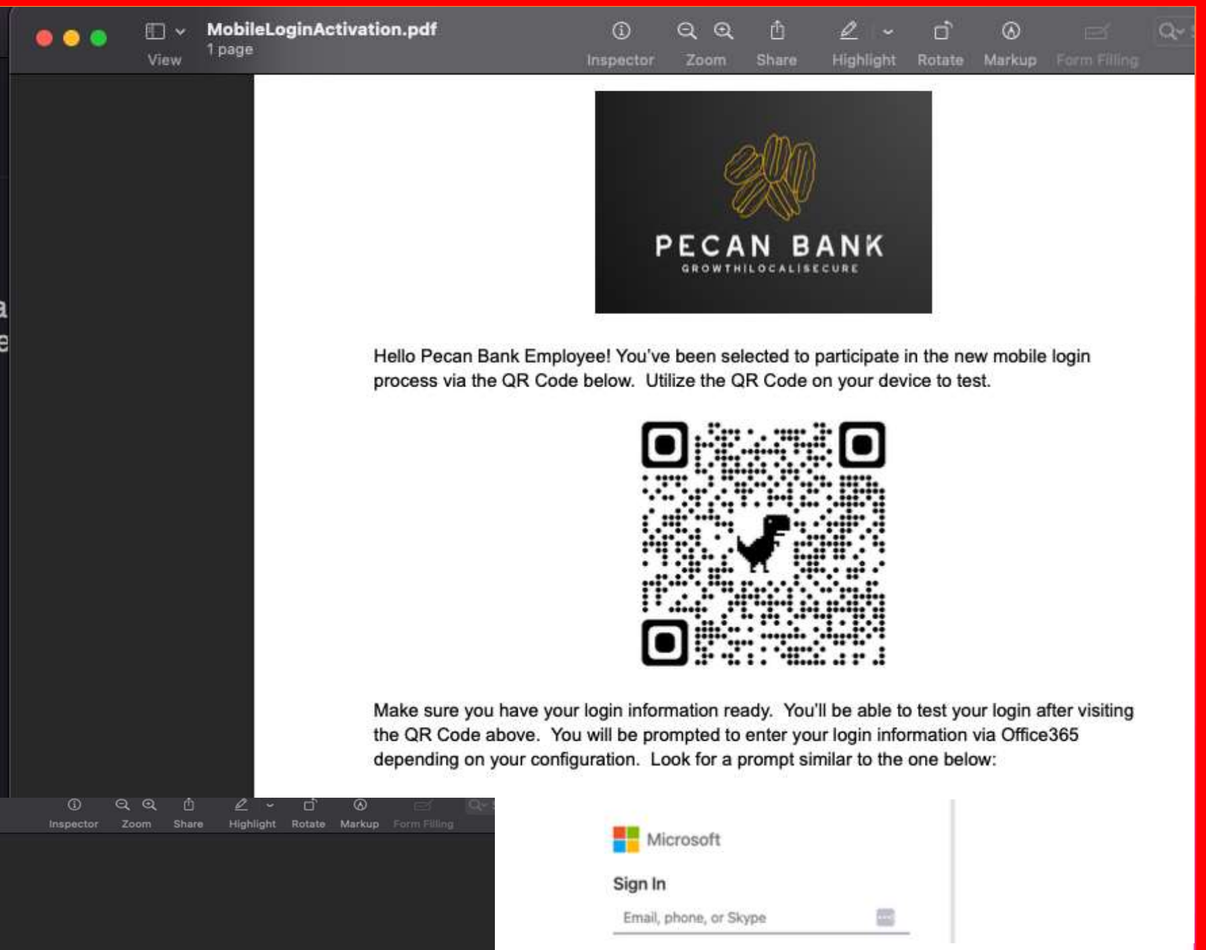
“I will create obstacles to make it difficult for the SOC to analyze and block my developed resources”

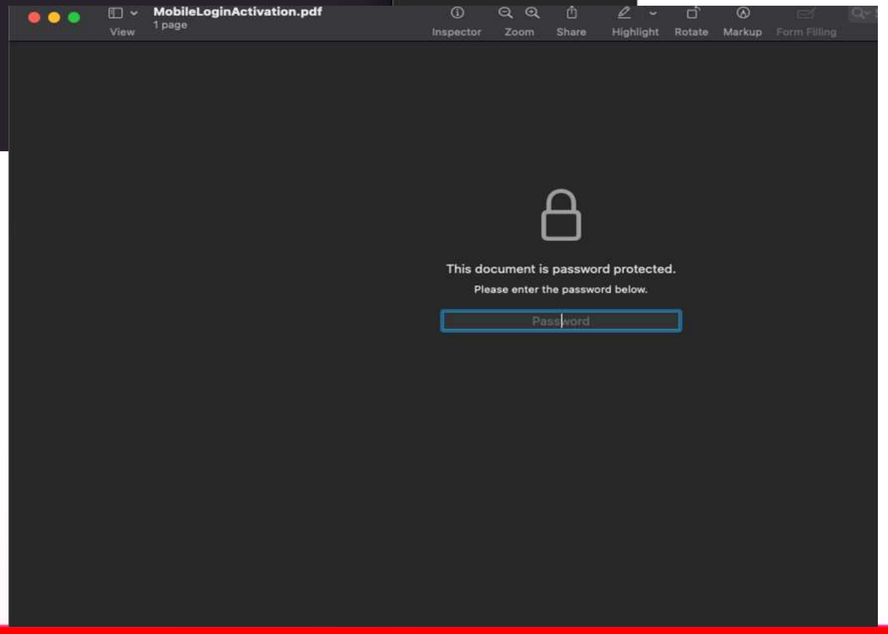
#1 of 5

Attacker Developed Resource:

QR Code Phishing with password protected PDF attachments







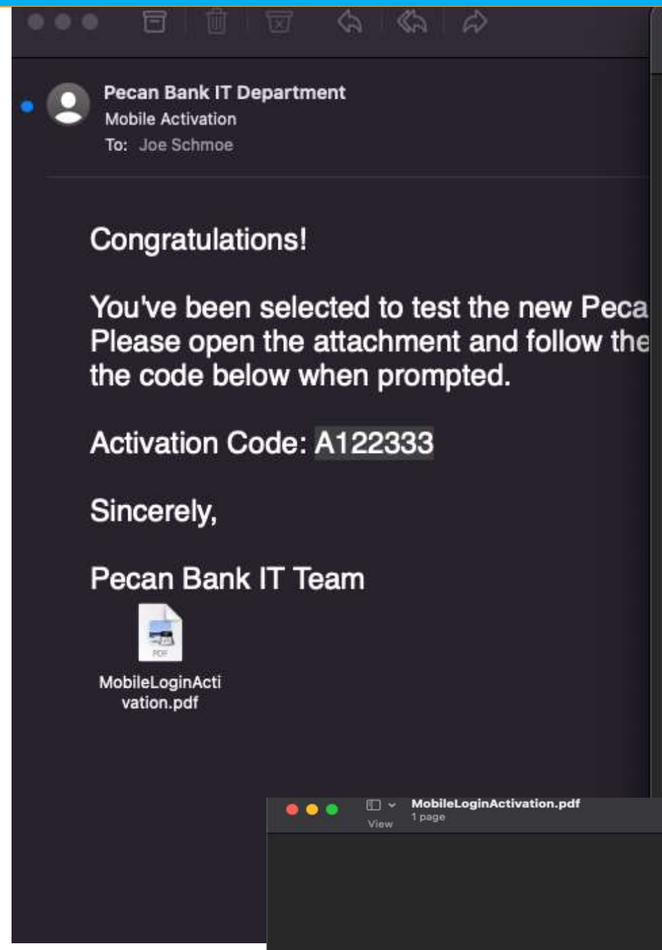
Defender
Analyse & Respond:

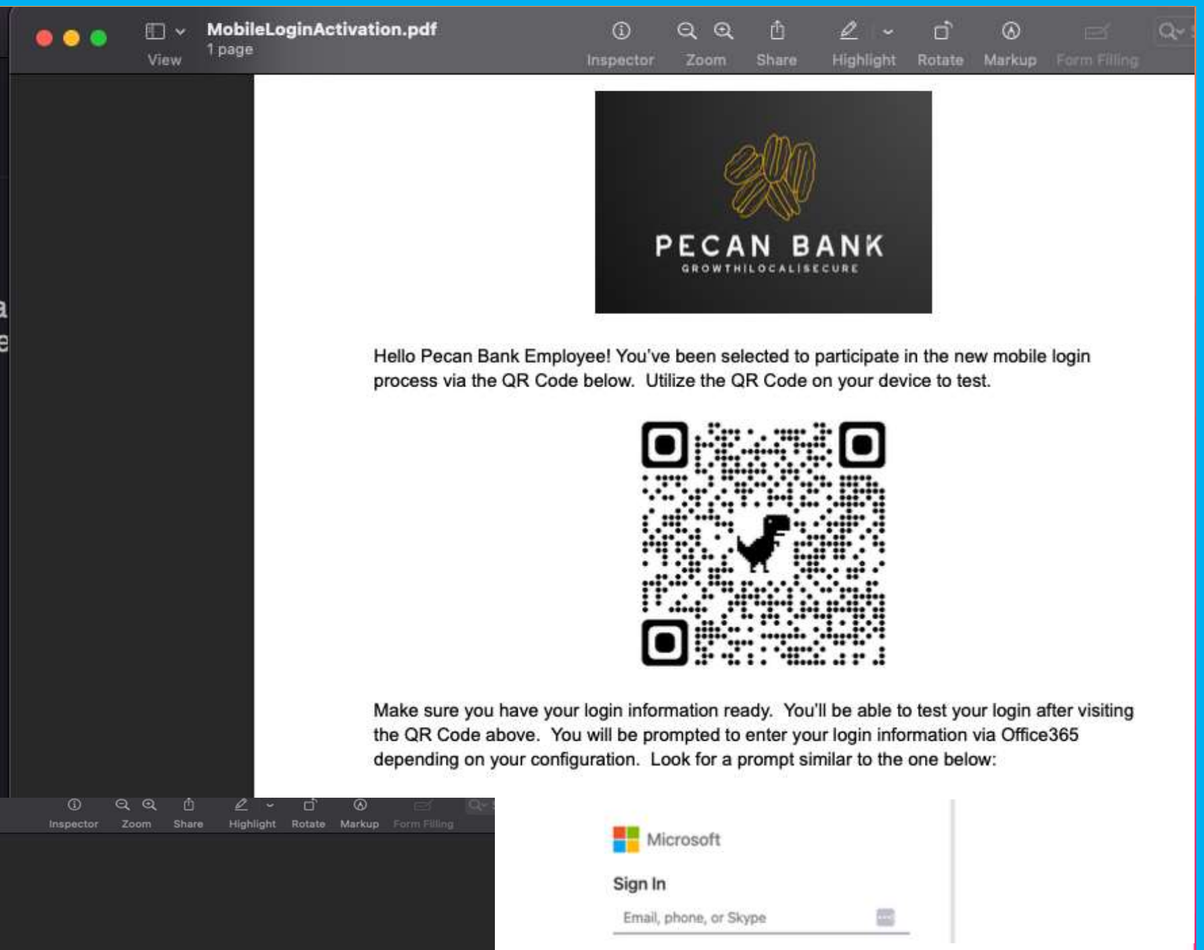
Analyse:

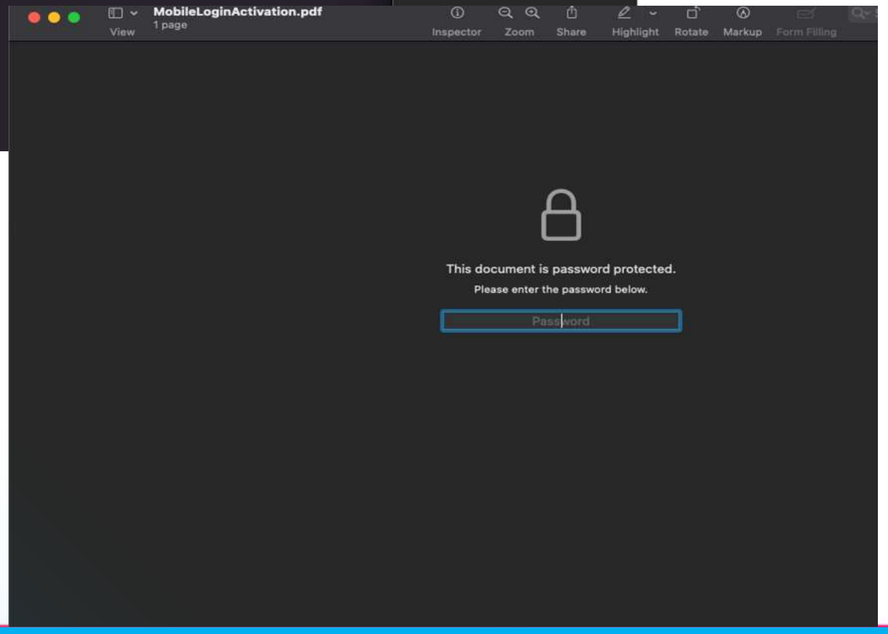
- Open Sandbox Env.
- Open PDF
- Enter Password from E-Mail Body
- Extract URL from QR Code
- ….

Respond:

- Block password protected PDFs?!?
- Block extracted URL
- Block Sender



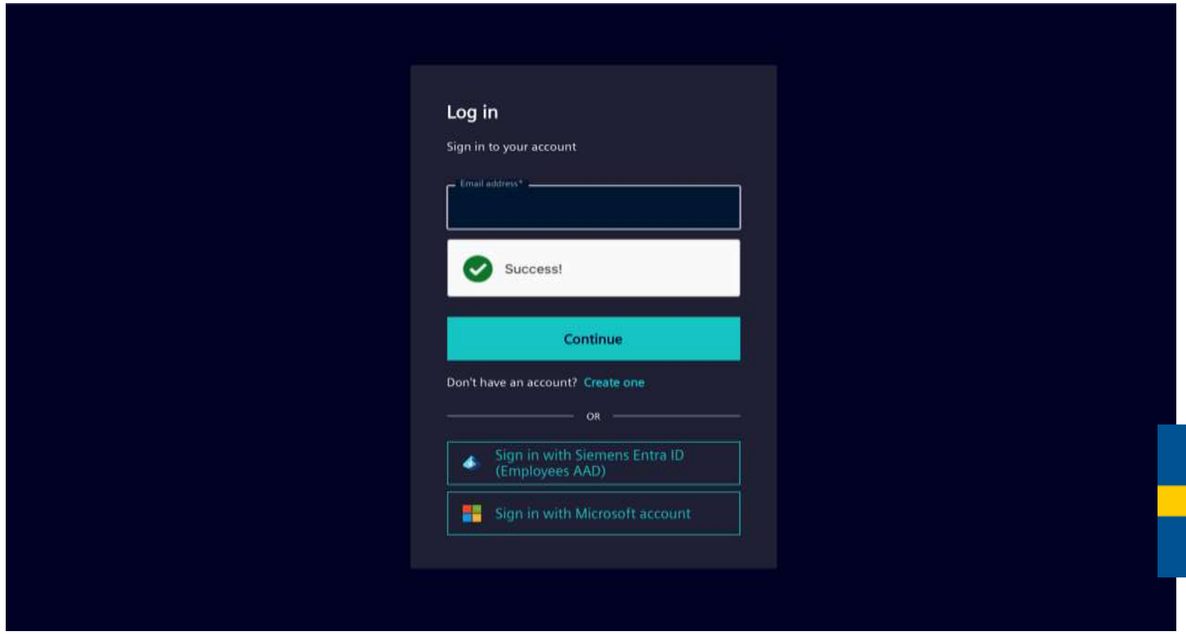


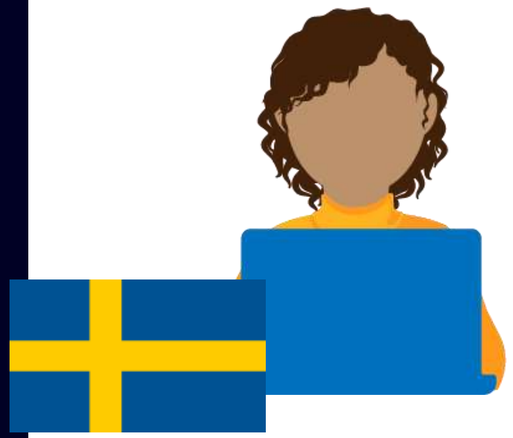


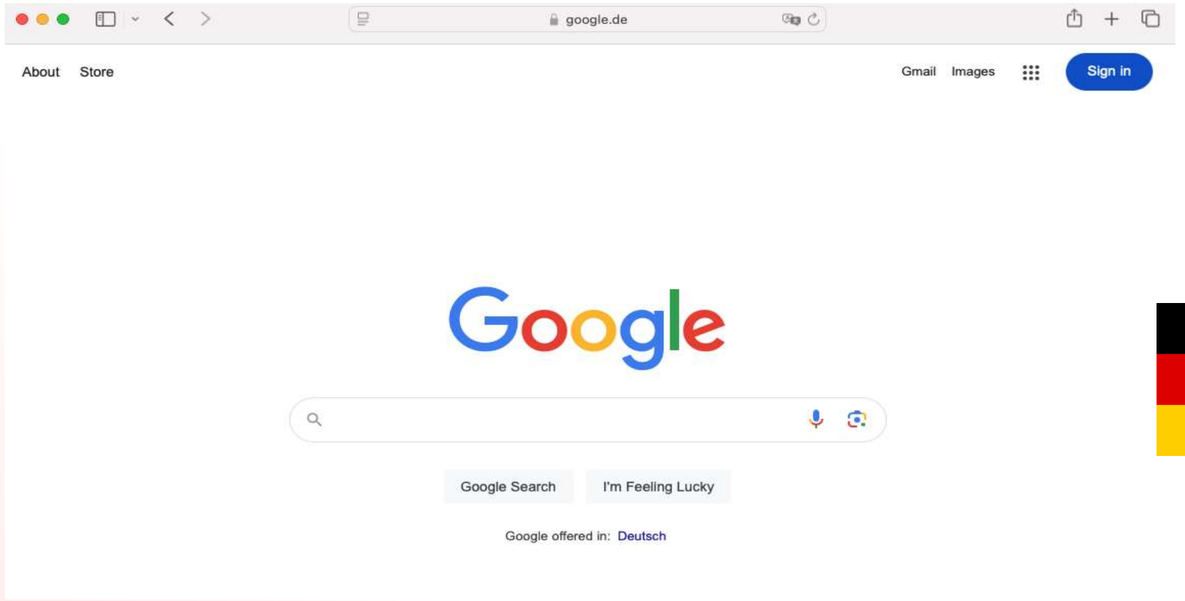
#2 of 5

Attacker Developed Resource:

Geo IP Redirect



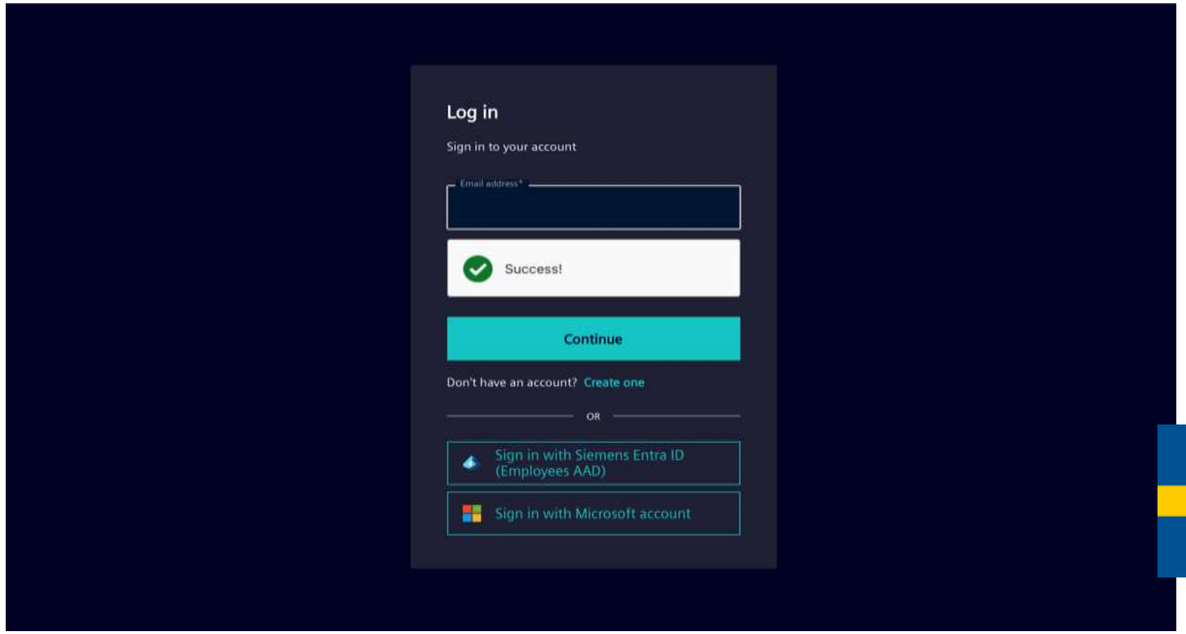


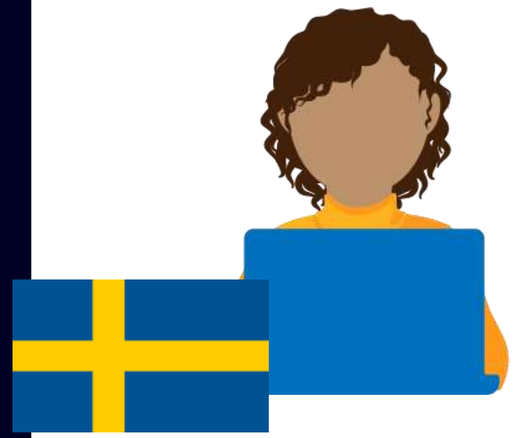


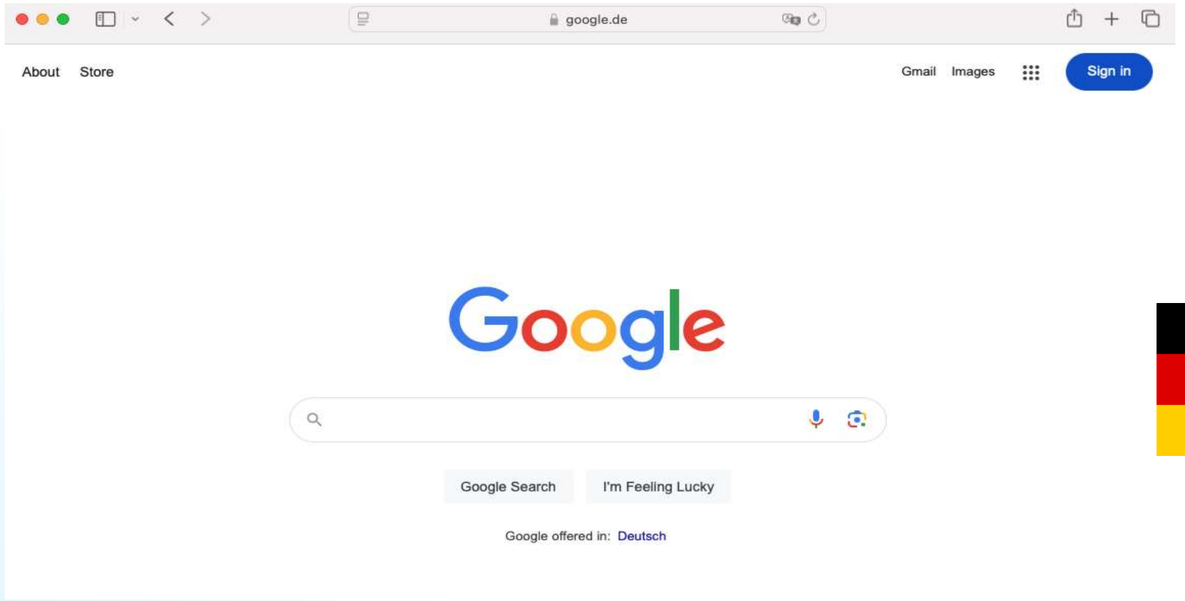
Defender
Analyse and Respond

Analyse:

- Establish capability to investigate phishes from each country your organisation operates







#3 of 5

Attacker Developed Resource:

Smishing Re-Direct
Browser Fingerprinting

Security Analyst

Going to this phishing page on a PC was not possible, however, nor was visiting it via a service like URLscan. I later realized that this was because it was using Cloudflare's service called "Bot Fight Mode". This legit and free service that is designed to prevent bot devices from visiting websites and, in this case, only non-emulated mobile devices. This setting means that any visitor that isn't on a non-emulated mobile device is shown a 404 Not Found HTTP error message instead.

Defender Analyse and Respond

Analyse :

- Investigate Smishing URLs with mobile devices / good emulators

Security Analyst

Going to this phishing page on a PC was not possible, however, nor was visiting it via a service like URLscan. I later realized that this was because it was using Cloudflare's service called "Bot Fight Mode". This legit and free service that is designed to prevent bot devices from visiting websites and, in this case, only non-emulated mobile devices. This setting means that any visitor that isn't on a non-emulated mobile device is shown a 404 Not Found HTTP error message instead.

#4 of 5

Attacker Developed Resource:

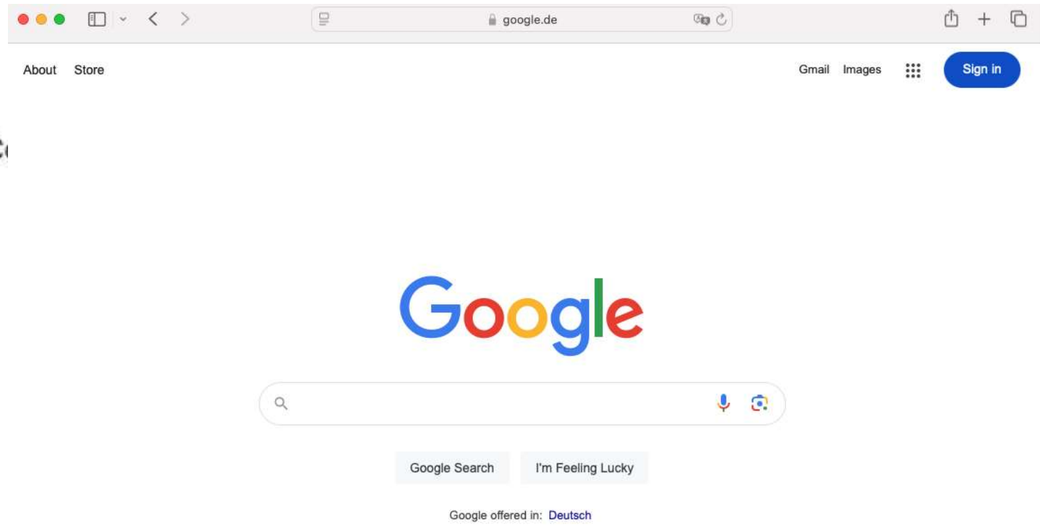
IP Reputation Check

Redirecting known VPN, known Bot, known proxy IPs.

This plugin protects WordPress Sites from unwanted malicious access attempts by leveraging IP reputation data provided by the ThreatPoint IP reputatio ...

Plugin Features

- Detects activity and IP reputation from the following sources:
- Tor exit node traffic
- Proxy (paid)
- Proxy (free)
- VPN (paid)
- VPN (free)
- Known Malicious Behaviour (C
- Brute force detection



Defender Analyse and Respond

Analyse:

Strategically decide which investigation tools you use and share your information with

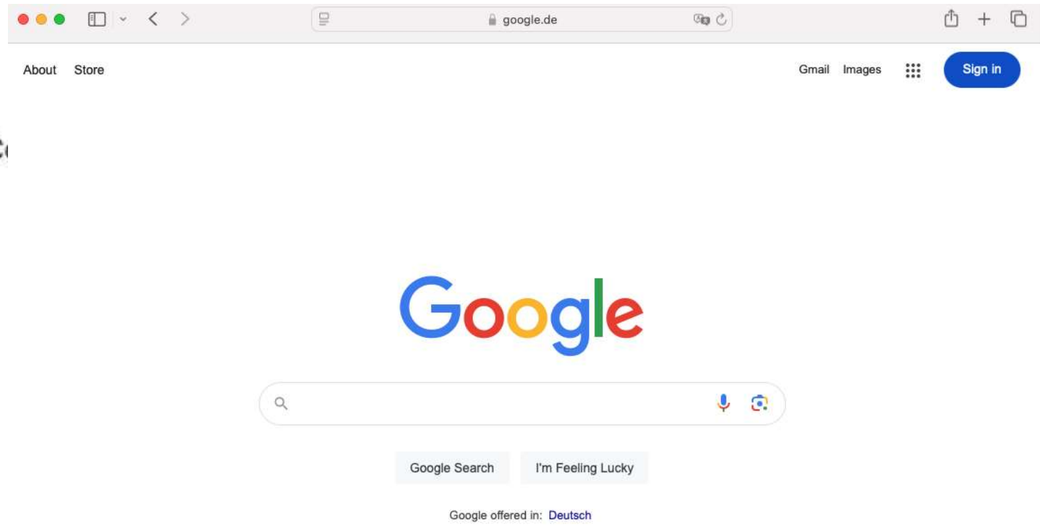
ThreatPoint IP Reputation

By ThreatPoint · ip · reputation · tor

This plugin protects WordPress Sites from unwanted malicious access attempts by leveraging IP reputation data provided by the ThreatPoint IP reputatio ...

Plugin Features

- Detects activity and IP reputation from the following sources:
- Tor exit node traffic
- Proxy (paid)
- Proxy (free)
- VPN (paid)
- VPN (free)
- Known Malicious Behaviour (C
- Brute force detection



#5 of 5

Attacker Developed Resource:

reCAPTCHA in front of phishing page

PRICING

reCAPTCHA Pricing

Discover the solution that best meets your business requirements.

Item	reCAPTCHA Essentials	reCAPTCHA Standard	reCAPTCHA Enterprise
Cost per month	Free up to 10,000 assessments*	Free $8 fc	
Term	None	Mont	
Assessments per month	< 10,000	10,0	

CLOUDFLARE

Solutions Products Pricing Resources Partners Why Cloudflare

Sales: +49 89 2555 2276 Support Contact sales Log in

	Free	Pro	Business	Enterprise
	For personal or hobby projects that aren't business-critical.	For professional websites that aren't business-critical.	For small businesses operating online.	For mission-critical applications that are core to your business.
	$0/month Add-ons billed monthly	$20/month When billed annually or $25/mo billed monthly	$200/month When billed annually or $250/mo billed monthly	Custom Billed annually
	Add a Website	Get Started	Get Started	Talk to an Expert
Fast, Easy-to-use DNS	✓	✓	✓	✓
Unmetered DDoS Protection	✓	✓	✓	✓
CDN	✓	✓	✓	✓
Universal SSL Certificate	✓	✓	✓	✓
Free Managed Ruleset	✓	✓	✓	✓
Web Application Firewall (WAF)	✓	✓	✓	✓
Lossless Image Optimization	✗	✓	✓	✓

[redacted].ru

Checking if the site connection is secure

Verify you are human

[redacted].ru needs to review the security of your connection before proceeding.

Why am I seeing this page?

I am human

hCaptcha

Privacy - Terms

Ik ben geen robot

reCAPTCHA

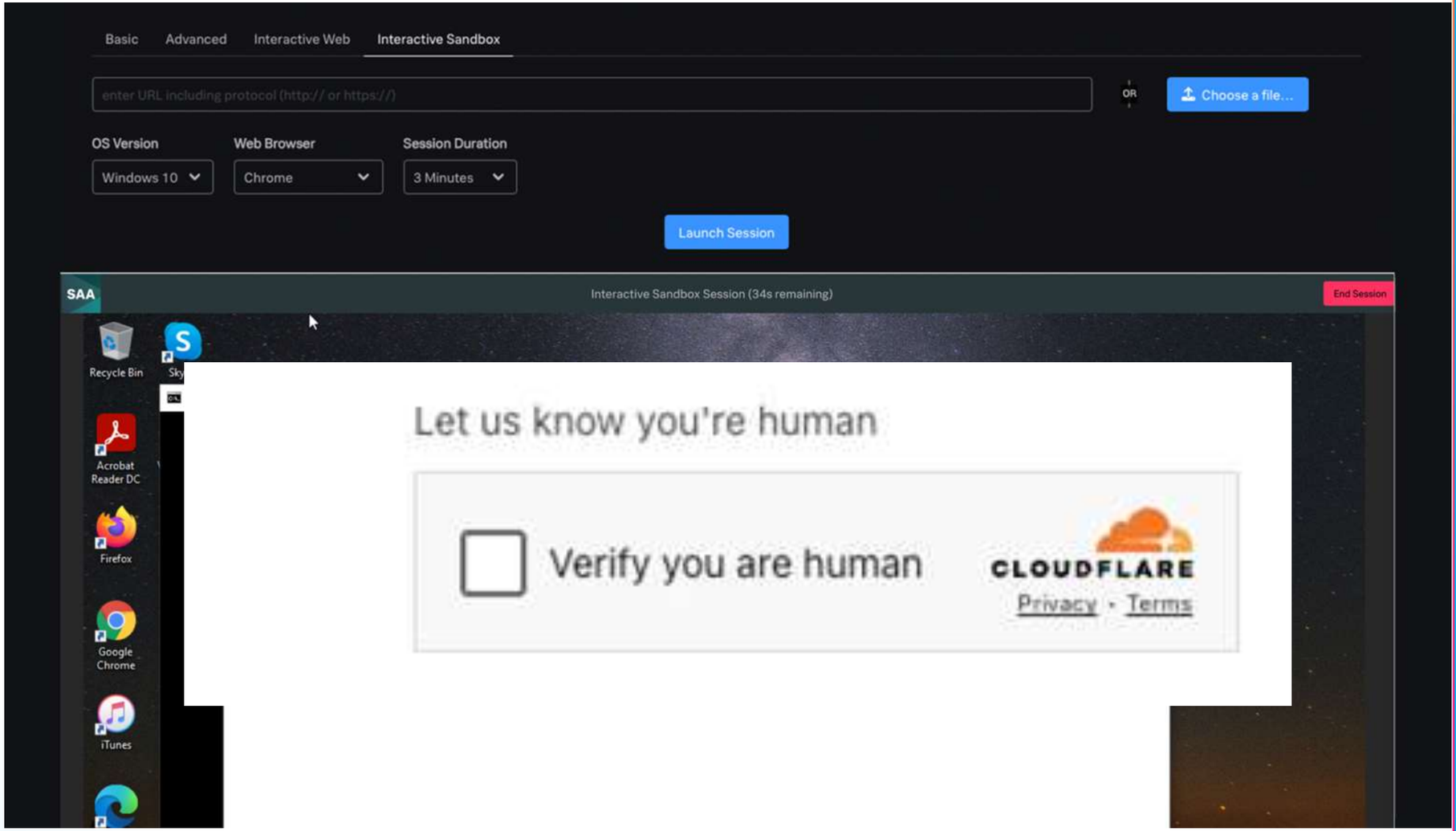
Privacy - Voorwaarden

Defender Analyse and Respond

Analyse :

- Ensure your analysis tools (IPs) are whitelisted (Security providers want to avoid those)

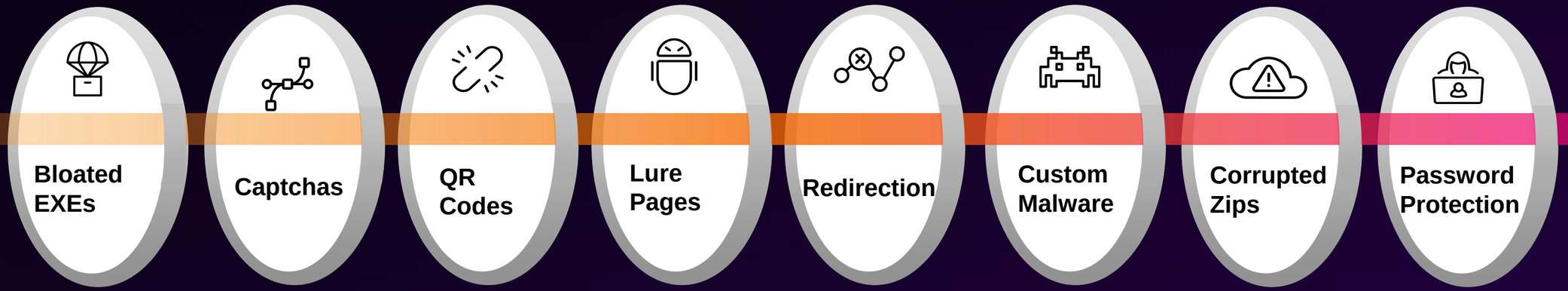
- Ensure you can switch from automated analysis to interactive sandboxes to manually “unblock”



Why Do Some Threats Get Through?

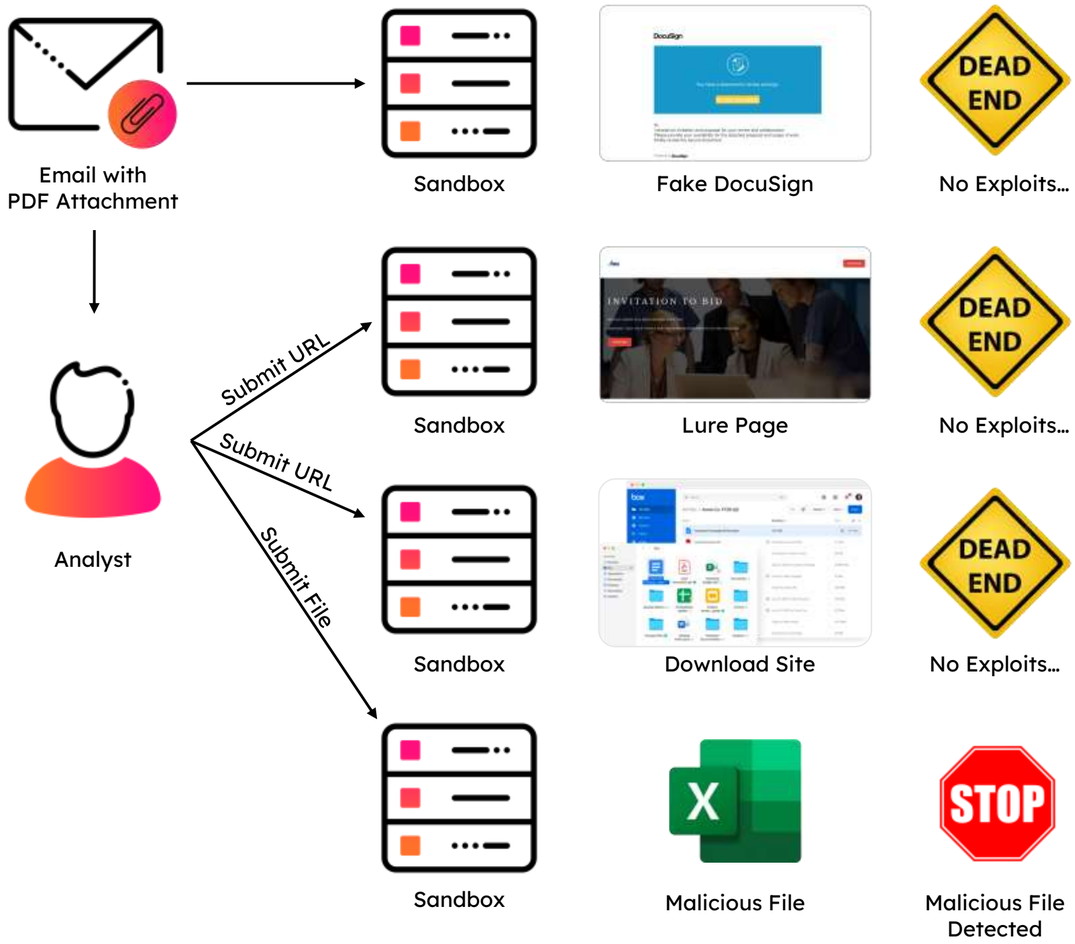
Splunk Attack Analyzer

Jumps Through All the Hoops So Analysts Don’t Have To



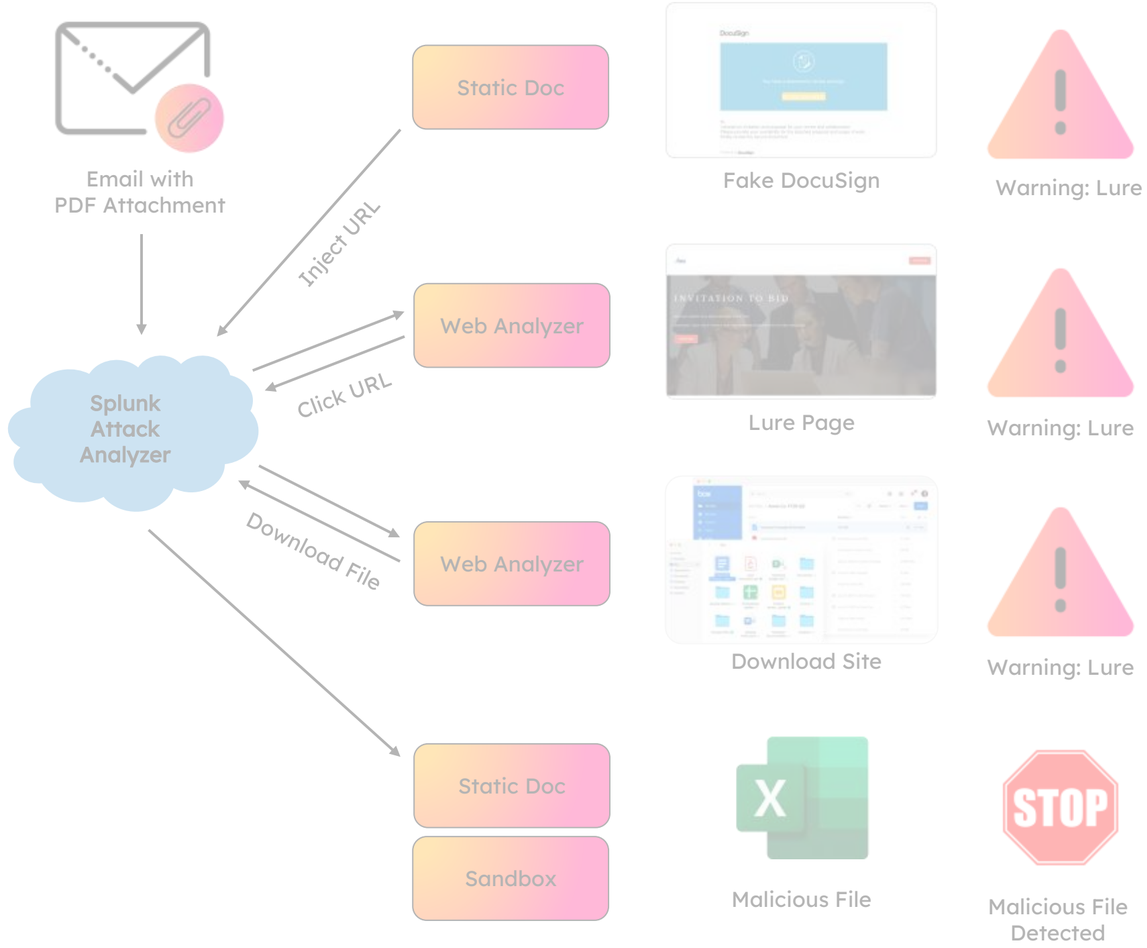
Traditional Sandbox

Multiple Manual Analyst Interventions



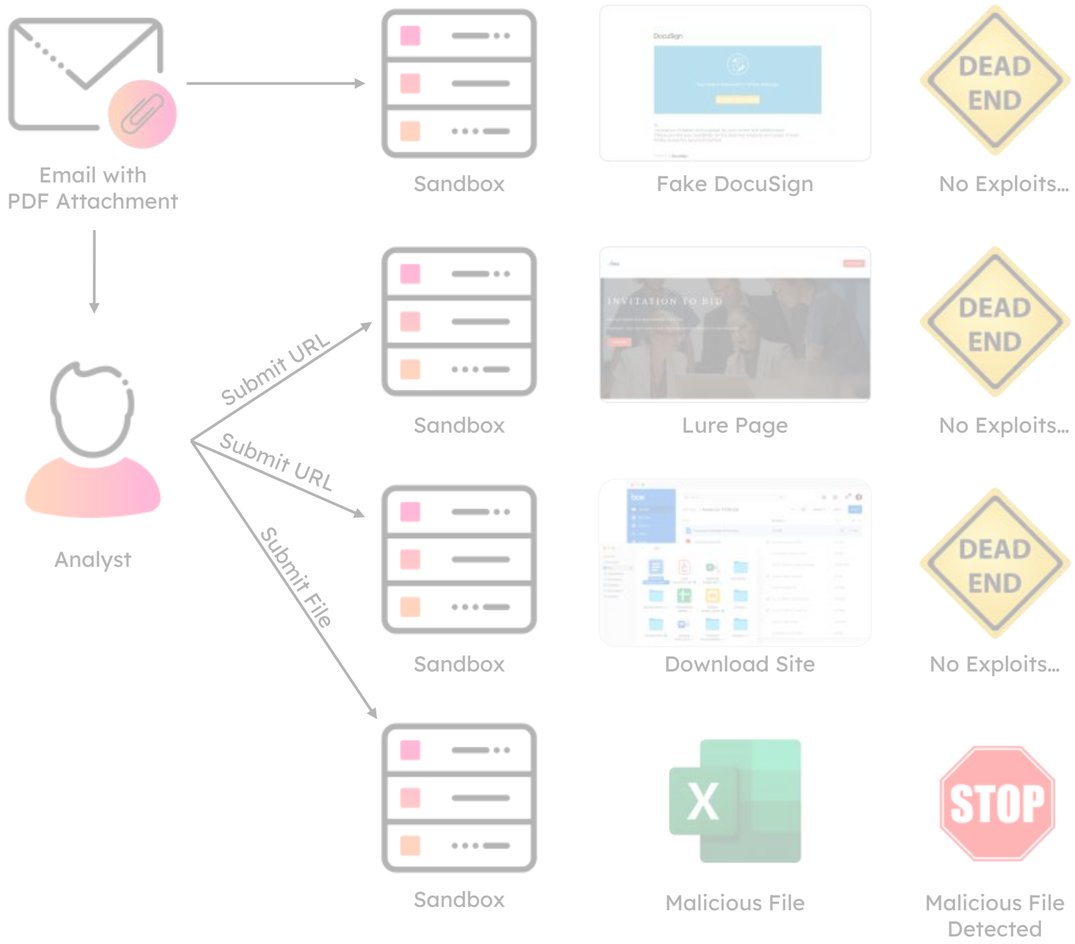
Splunk Attack Analyzer

Fully Automated Threat Analysis



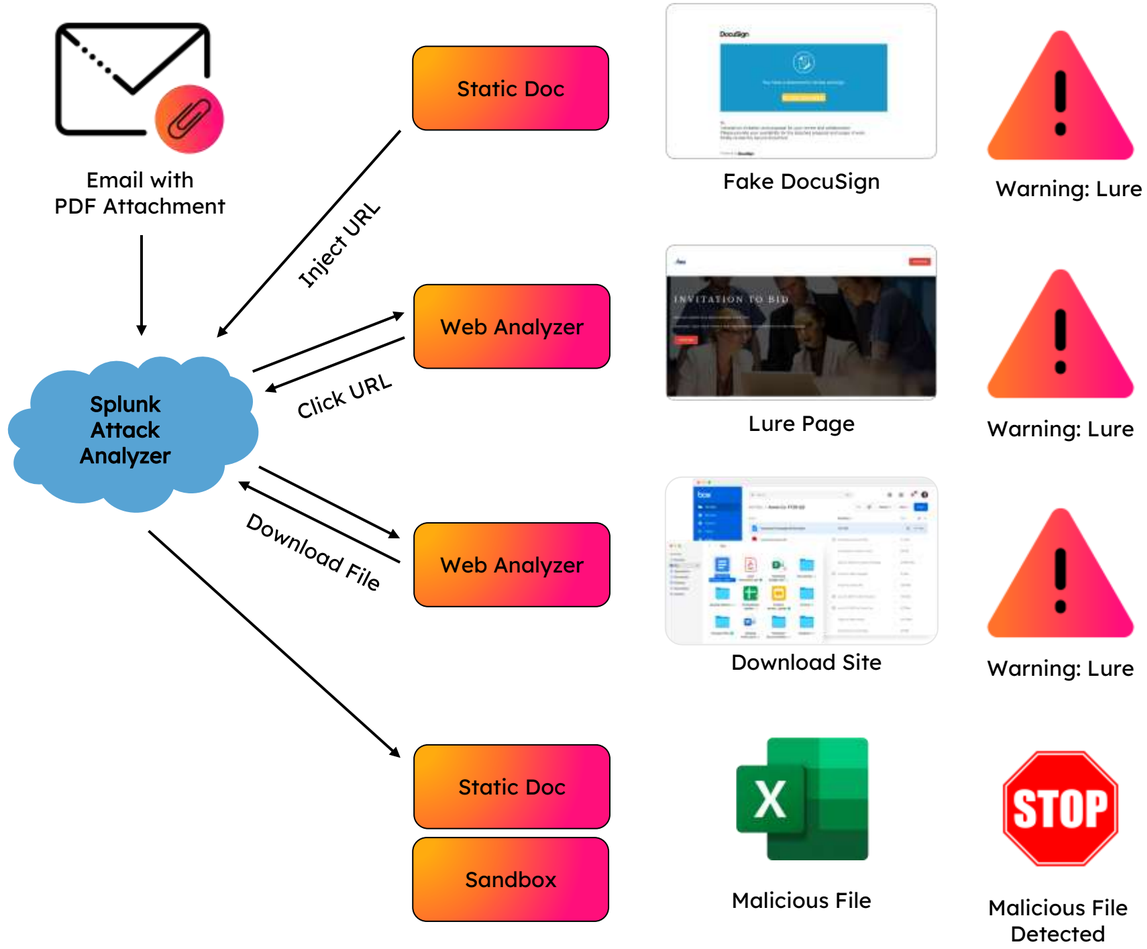
Traditional Sandbox

Multiple Manual Analyst Interventions



Splunk Attack Analyzer

Fully Automated Threat Analysis



Popular examples for triage and analysis

Splunk Attack Analyzer

Email Analysis	Employee Reported Emails	Retroactive Email Threat Detections	Customer Reported Brand Fraud	
EDR/AV	Potential False Negatives	Low Confidence Alerts (False Positive Review)	Secondary IoCs/IoAs for Quarantined Threats	Public Submission Forms
Proxy/Web	Potential False Negatives	Unblock Requests for SWG/Proxy Block Requests	Categorization Requests for New URLs	Web Referrer Logs Scanning
Threat Hunting & Ad-hoc Investigations	Ad-hoc URL Submissions	Ad-hoc File Submissions	Live Detonation of Websites	Live Detonation of Files