



# One day of life of a security engineer

---

New York USA  
London UK  
Munich Germany  
Zug Switzerland

I'm...

---



## Vadym Chakrian

*Email:* [vadym.chakrian@gmail.com](mailto:vadym.chakrian@gmail.com)

*TG/VB:* +38 (093) 866 35 89

*Skype:* vadym.chakrian

*Social:*

<https://www.linkedin.com/in/vadymchakrian/>

<https://www.facebook.com/vadymchakrian>

---

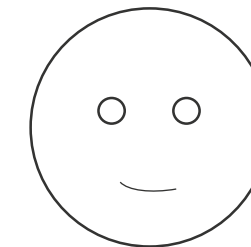
Sincerely,  
Security Architect at DataArt.

# I will tell about...

3

real-life stories

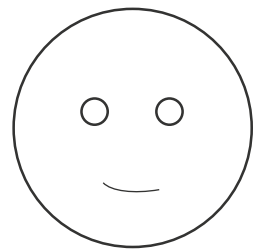
which happened with



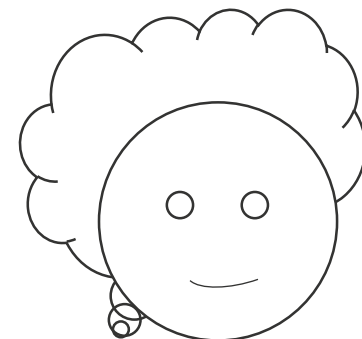
security engineer

# Before we begin meet our team

---



security engineer



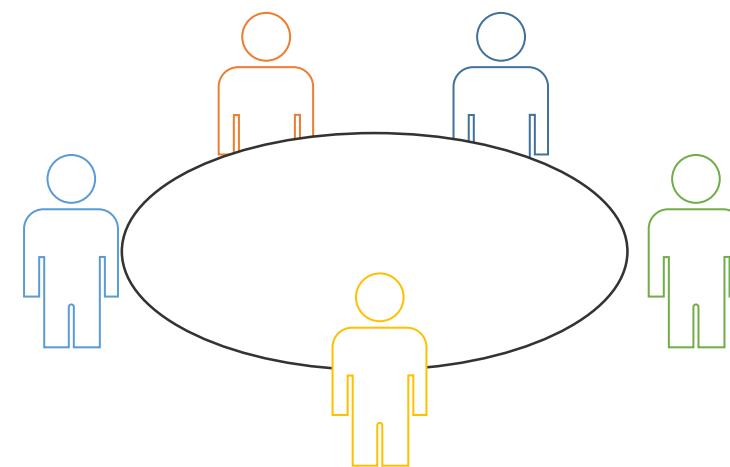
project manager



IT team



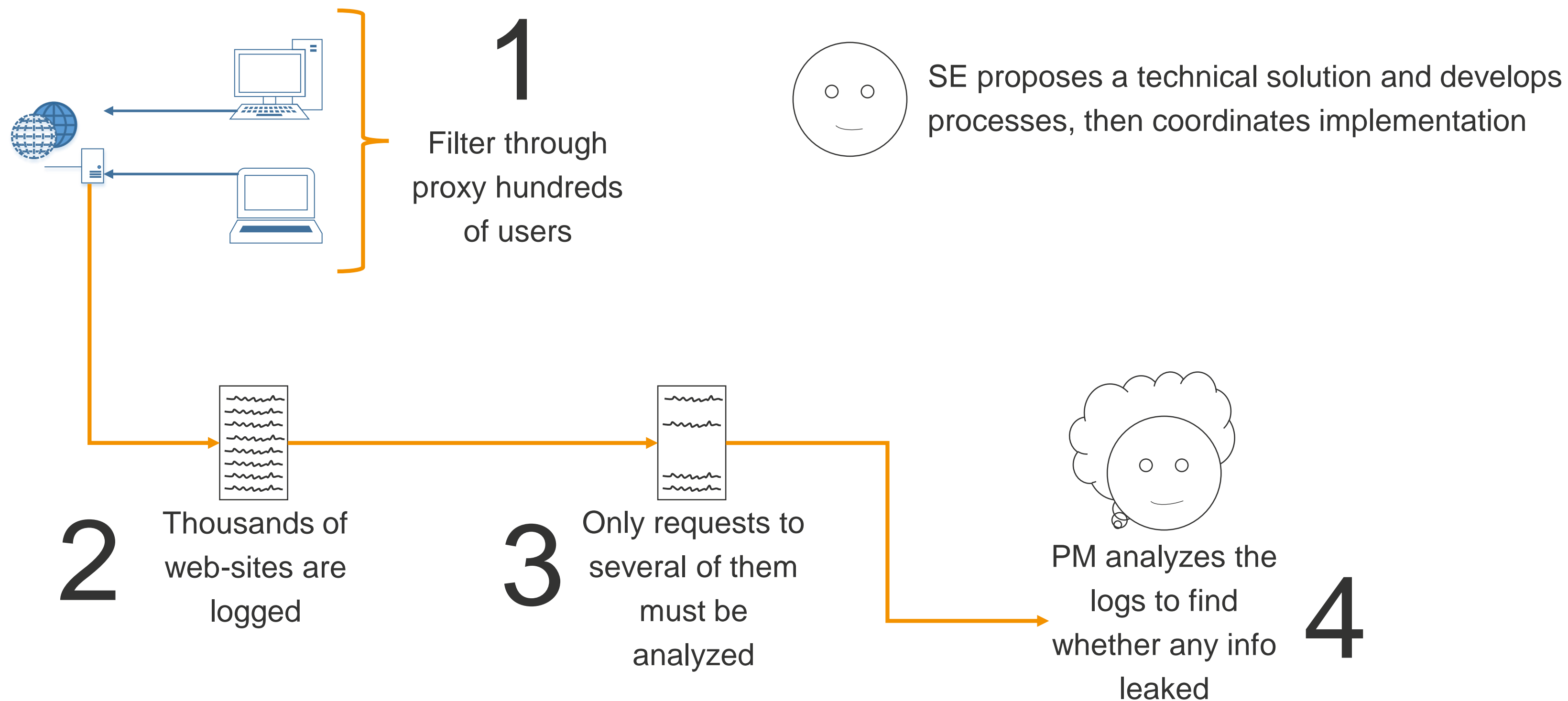
owner of systems



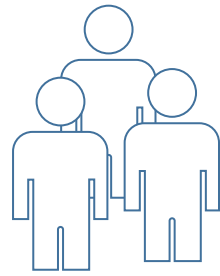
Management

How  analyzed the proxy logs

# The task



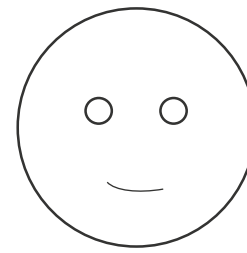
# Solving the task



IT team implements  
proxy and traffic  
forwarding



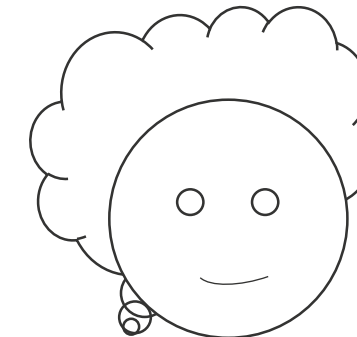
Some services  
become unavailable  
because of SSL  
inspection



SE develops a script  
to filter logs and  
coordinates IT team



A lot of URLs in  
resulting logs are  
service-oriented and  
are useless

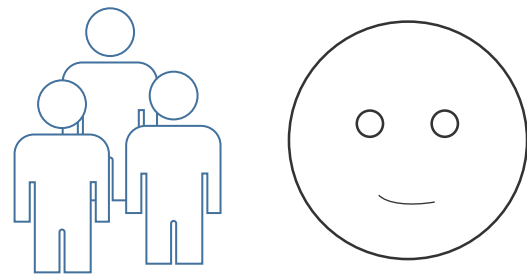


PM checks  
through the  
URLs

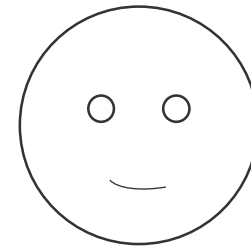


PM is upset because  
she needs to review  
dozens of links  
manually

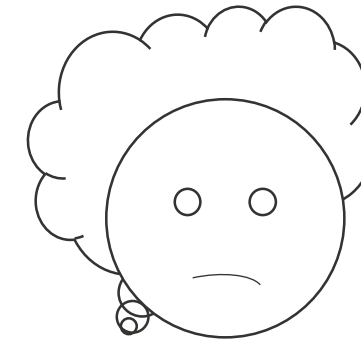
# Solving a problem



Provide exceptions for  
broken resources



Script was modified  
to exclude service-  
oriented URLs



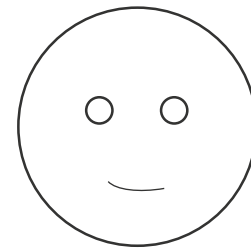
But she is still upset



# Interesting solution

1

URLs are processed through eyewitness to get an HTML report



HTML report is hosted at a web-server and PM is provided an access to it

2

# eyewitness HTML report view



## Table of Contents

- [Uncategorized \(Page 1\)](#)
- [404 Not Found \(Page 4\)](#)

Uncategorized	88
404 Not Found	39
Errors	0
Total	127

Report Generated on 01/09/2019 at 08:36:58  
[Next Page](#)

[Page 1](#) [Page 2](#) [Page 3](#) [Page 4](#) [Page 5](#) [Page 6](#)

## Uncategorized

Web Request Info	Web Screenshot
<a href="https://docs.google.com/spreadsheets/d/198dZkLZud4U535U-dwUzn4ltsxg0RejbosjEb_PlvWI/">https://docs.google.com/spreadsheets/d/198dZkLZud4U535U-dwUzn4ltsxg0RejbosjEb_PlvWI/</a> Resolved to: 64.233.165.139	

# eyewitness HTML report view



[https://docs.google.com/forms/u/0/d/17RAwFs\\_hMbFmtmtl1ue943F5BPYAqtdQve8LyL3b6pM/](https://docs.google.com/forms/u/0/d/17RAwFs_hMbFmtmtl1ue943F5BPYAqtdQve8LyL3b6pM/)  
Resolved to: 64.233.165.113

**Page Title:** Untitled form  
**x-xss-protection:** 1; mode=block  
**x-robots-tag:** noindex, nofollow, nosnippet  
**x-content-type-options:** nosniff  
**set-cookie:** NID=154=luKYN-oRSz94hwZuxbPlmnoNZDRUEyJAmJa86uWejtbmnSIydjW481WukAejuHYDnTGmSSGb3BjkBRcUiMxGMSFsSohObuc5170q5ulbwU-AgqxY\_qNk1HS6d56WhdoF\_TLb-qGtvzCEzf2Mw4e1wC-K7FnyqW\_DEJnezafCHBY;Domain=.google.com;Path=/;Expires=Thu, 11-Jul-2019 13:50:27 GMT;HttpOnly, NID=154=XI46gJlXImBXoyf7VP0nrHMwA2JiJXp8w9dSQRegtOxOUFxeYNGDiS0W3gw1nUAtownOqgzwdtrufw2ksiBa215\_oi2-qI4CXIqnDARsUjkH3tNgJoq-PkJdkEW4NpE55zxixb0XUBoO5wUBtu3e0xGZXPVH0tHTDAZ1D7NkgM8;Domain=.google.com;Path=/;Expires=Thu, 11-Jul-2019 13:50:27 GMT;HttpOnly, S=spreadsheet\_forms=xUDlaRcbmVFshgtgRl6c44eBmeK6pBP3;Domain=.docs.google.com; Expires=Wed, 09-Jan-2019 14:50:27 GMT;Path=/forms/u/0/d/17RAwFs\_hMbFmtmtl1ue943F5BPYAqtdQve8LyL3b6pM; Secure; HttpOnly  
**accept-ranges:** none  
**expires:** Mon, 01 Jan 1990 00:00:00 GMT  
**vary:** Accept-Encoding  
**server:** GSE  
**connection:** close  
**pragma:** no-cache  
cache-control: no-cache, no-store, max-age=0

# eyewitness HTML report view

<https://i.gyazo.com/de6753241f757e913e45601ef32c2fd4.png>  
Resolved to: 104.19.142.111

**Page Title:**  
de6753241f757e913e45601ef32c2fd4.png  
(PNG Image, 2849x960 pixels) - Scaled (50%)

**expect-ct:** max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"

**x-gyazo-cfworker:** true

**content-length:** 186663

**via:** 1.1 google

**set-cookie:**  
\_\_cfduid=d78694e106b337d9d8ca9f5c7e8c06a561547041336; expires=Thu, 09-Jan-20 13:42:16 GMT; path=/; domain=.gyazo.com; HttpOnly

**accept-ranges:** bytes

**expires:** Thu, 09 Jan 2020 13:42:16 GMT

**vary:** Accept-Encoding

**server:** cloudflare

**access-control-allow-origin:** https://gyazo.com

**access-control-allow-credentials:** true

**connection:** close

**etag:** "de67"

**x-cache-level:** ZS

**cache-control:** public, max-age=31536000

**date:** Wed, 09 Jan 2019 13:42:16 GMT

**Response Code:** 200

**cf-ray:** 49675383591a8abc-KBP





**alt-svc:** clear

**content-type:** image/png

**cf-cache-status:** HIT

[Source Code](#)

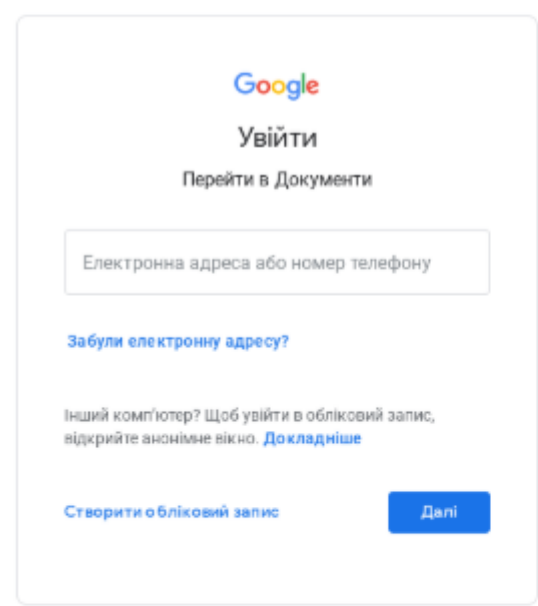
## HOW DID YOU LIKE ...?

PARTY	PLACE	FOOD	ENTERTAINMENT
			
8.82 out of 10	8.18 out of 10	8.55 out of 10	8.73 out of 10

# eyewitness HTML report view

<https://docs.google.com/document/d/14NY2wR6jc-mBNIFNiGIsinABkJUKUb0Sn9o7r9njgSM/>  
**Resolved to:** 64.233.165.113

**Page Title:** Google  
Ð"Ð¼Ð°Ð½fÐ¼Ð½Ñ,Ð,: Ð²Ñ...Ñ-Ð'  
**strict-transport-security:** max-age=31536000; includeSubDomains  
**x-content-type-options:** nosniff  
**content-security-policy:** script-src 'unsafe-inline' 'unsafe-eval' https: http:;object-src 'none';base-uri 'self';report-uri /cspreport  
**transfer-encoding:** chunked  
**set-cookie:**  
GAPS=1:2tTli61VaBRi4Q9XCEzi5D2bxV3z7w:ImXCV0JMyNrzgC6S;Path=/;Expires=Fri, 08-Jan-2021 13:46:37 GMT;Secure;HttpOnly;Priority=HIGH  
**expires:** Mon, 01 Jan 1990 00:00:00 GMT  
**x-auto-login:**  
realm=com.google&args=service%3Dwise%26continue%3Dhttps%253A%252F%252Fdocs.google.com%252Fdocument%252Fd%252F14NY2wR6jc-mBNIFNiGIsinABkJUKUb0Sn9o7r9njgSM%252Fedit  
**server:** GSE  
**connection:** close  
**x-xss-protection:** 1; mode=block  
**link:**  
<https://www.google.com/intl/uk/drive/>; rel="canonical"  
**pragma:** no-cache



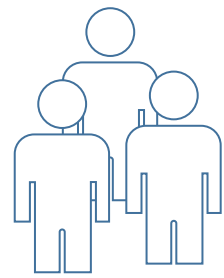
Українська ▾    Довідка    Конфіденційність    Умови

# eyewitness HTML report view

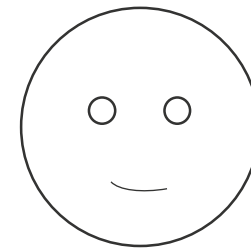
<p><a href="https://docs.google.com/comments/d/AAHRpnXtCUnKsiYWYRUgKDkJ58W-B4aZefyJYdkVgYFllhXh4IkWFP7GUY1LpRFB1IHpHPacD3jKD0o0FcWhksCWhuKieB8Z4Ou7WIFXgnPrGBPCgcHj4I3M/">https://docs.google.com/comments/d/AAHRpnXtCUnKsiYWYRUgKDkJ58W-B4aZefyJYdkVgYFllhXh4IkWFP7GUY1LpRFB1IHpHPacD3jKD0o0FcWhksCWhuKieB8Z4Ou7WIFXgnPrGBPCgcHj4I3M/</a> <b>Resolved to:</b> 64.233.165.101</p> <p><b>Page Title:</b> Error 404 (Not Found)!!1 <b>x-xss-protection:</b> 1; mode=block <b>x-content-type-options:</b> nosniff <b>content-security-policy:</b> script-src 'unsafe-inline' https: http: 'unsafe-eval'; object-src 'none'; base-uri 'self'; report-uri https://csp.withgoogle.com/csp/docs/1 <b>set-cookie:</b> S=comments=8JdsWyPEju-nR2dE1ygI6X7kABpeavBt; Domain=.docs.google.com; Expires=Wed, 09-Jan-2019 14:01:10 GMT; Path=/comments/d/AAHRpnXtCUnKsiYWYRUgKDkJ58W-B4aZefyJYdkVgYFllhXh4IkWFP7GUY1LpRFB1IHpHPacD3jKD0o0FcWhksCWhuKieB8Z4Ou7WIFXgnPrGBPCgcHj4I3M; Secure; HttpOnly <b>accept-ranges:</b> none <b>expires:</b> Mon, 01 Jan 1990 00:00:00 GMT <b>vary:</b> Accept-Encoding <b>server:</b> GSE <b>connection:</b> close <b>pragma:</b> no-cache <b>x-chromium-appcache-fallback-override:</b> disallow-fallback <b>cache-control:</b> no-cache, no-store, max-age=0, must-revalidate</p>	
---	--

# The results

---

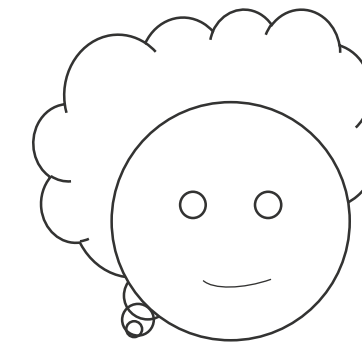


IT team still provides minor fixes but the solution is more or less stable



Logs filtering and HTML reports formation is still on a plate of a SE

Script needs modifying to fully automate the processes



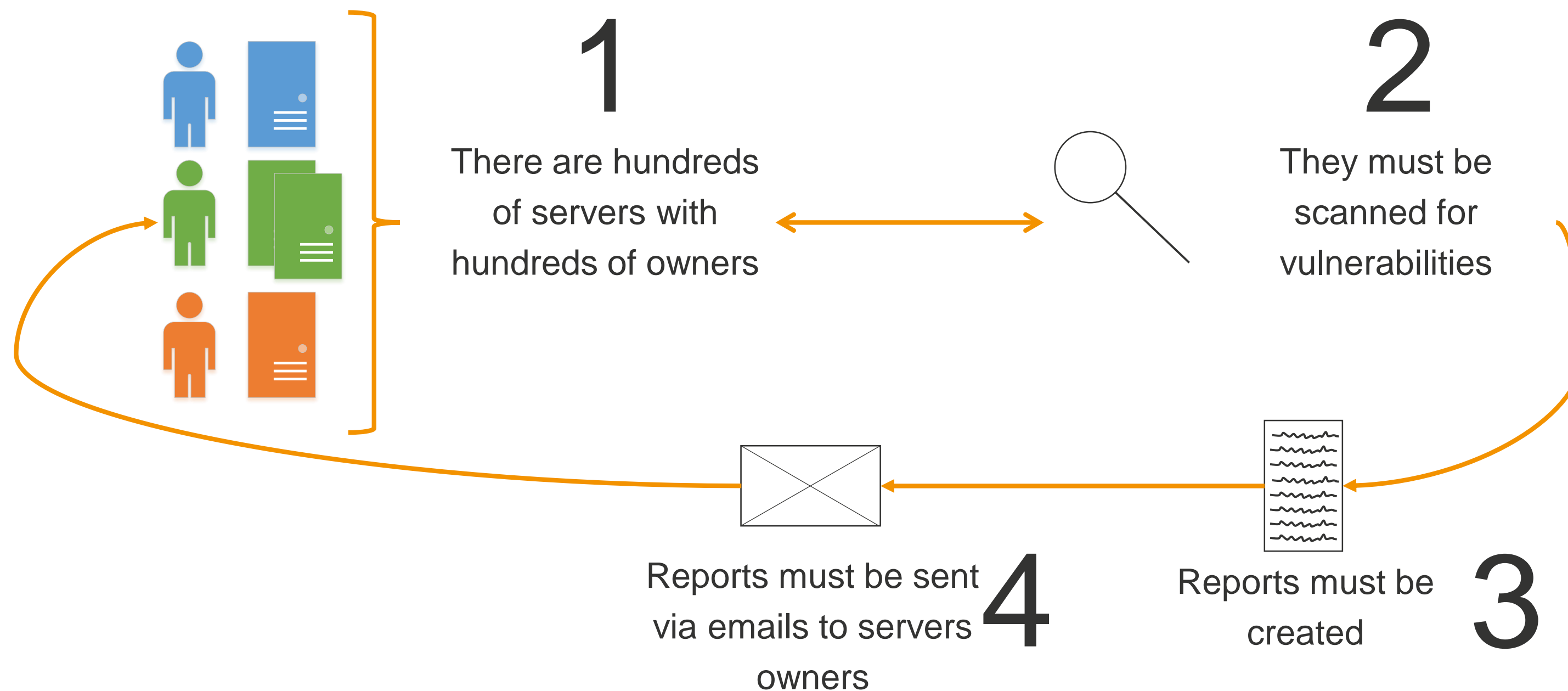
PM still needs reviewing the visited URLs

But she is much happier having HTML reports

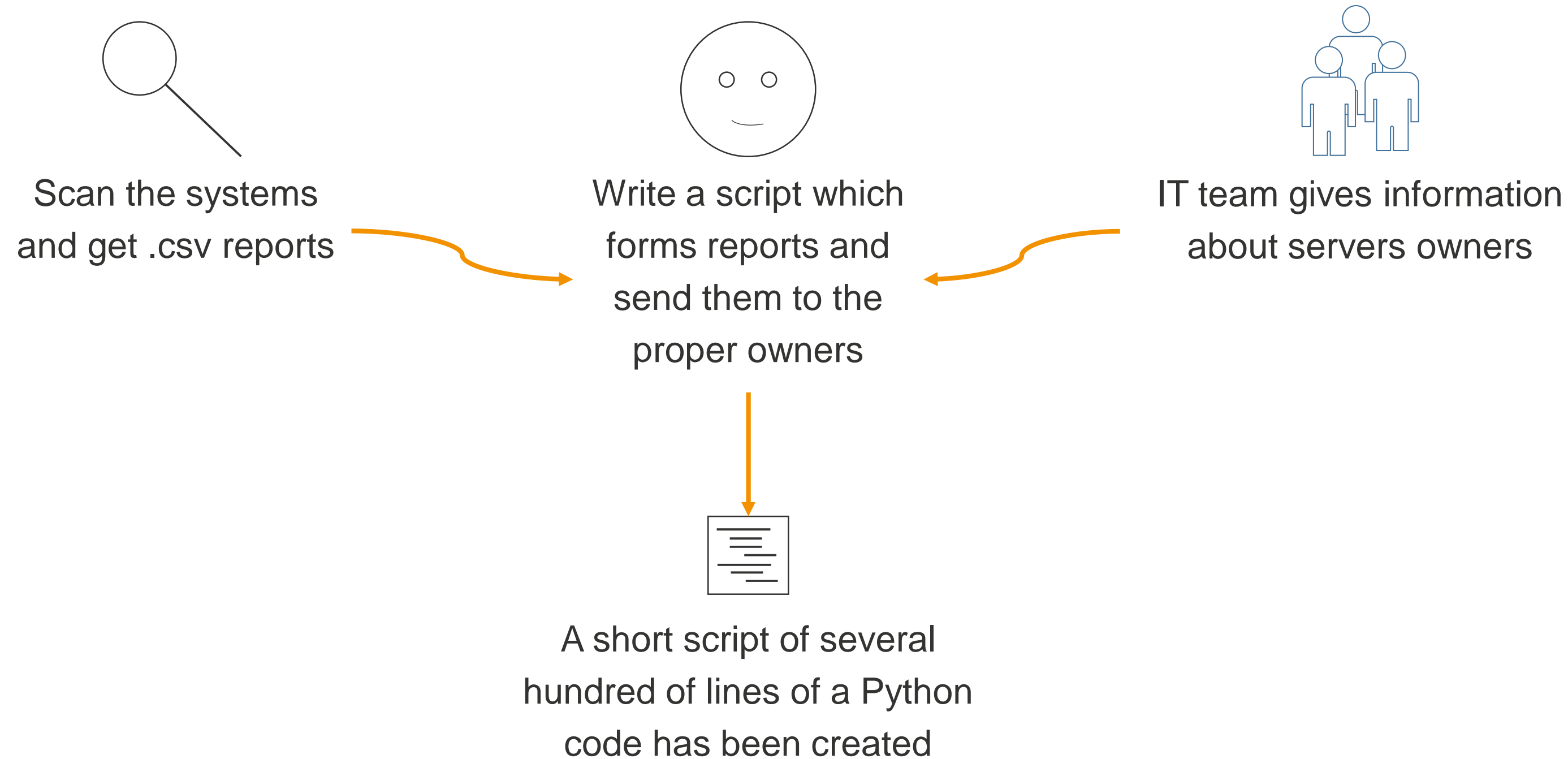
How  reported vulnerabilities



# The task



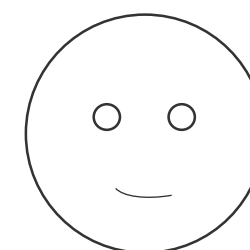
# Solution



# First problem



Problem: system owners didn't have a chance to fix all vulnerabilities, it was needed to send only the critical ones

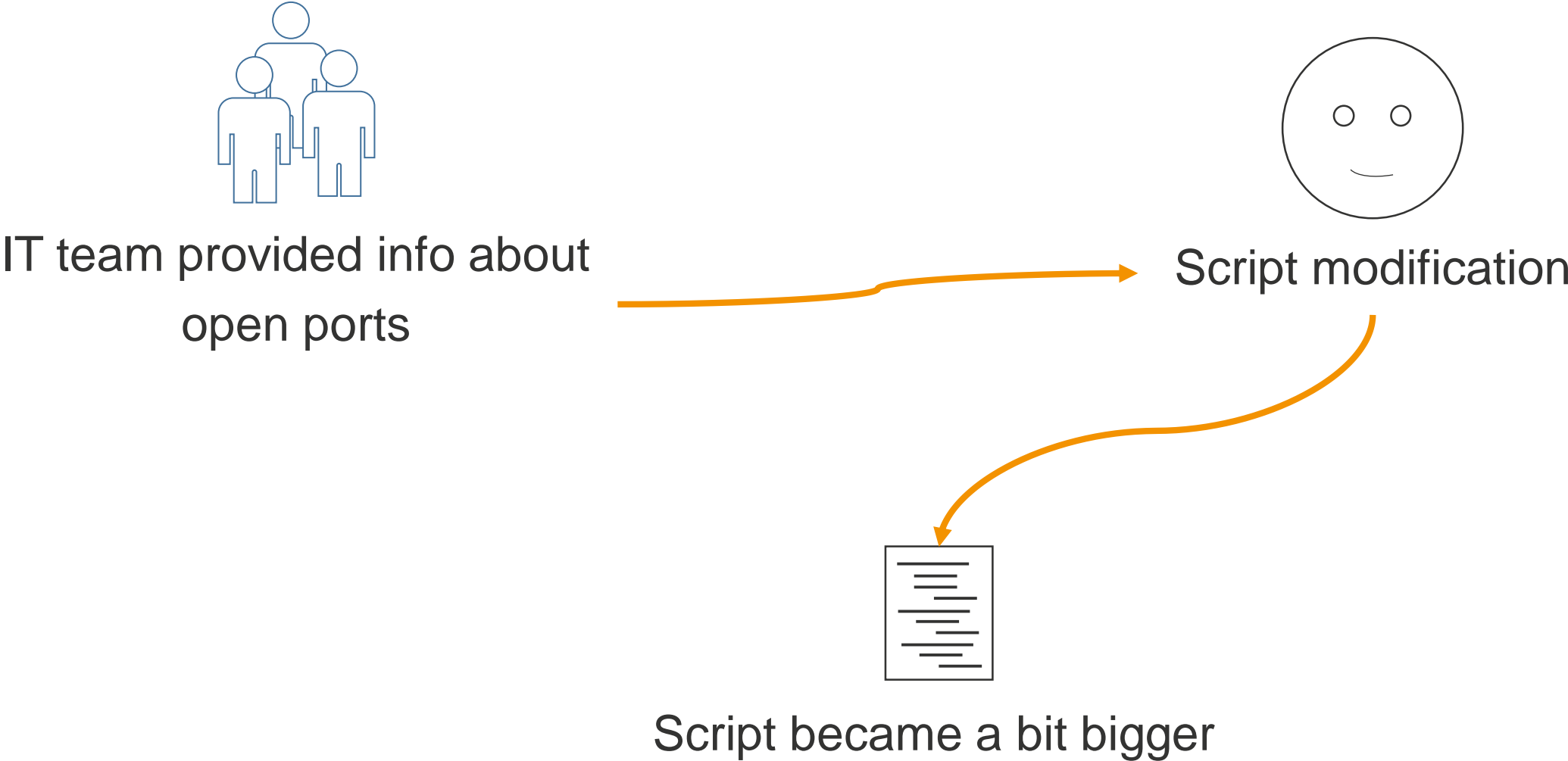


Solution: notify only about vulnerabilities on ports open to the Internet and High/Critical ones



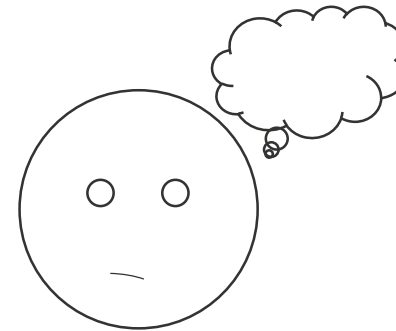
Script needs modification

# Solution



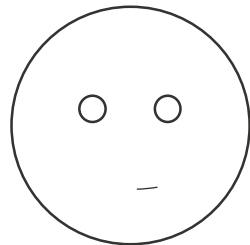
# How/What would you?..

---

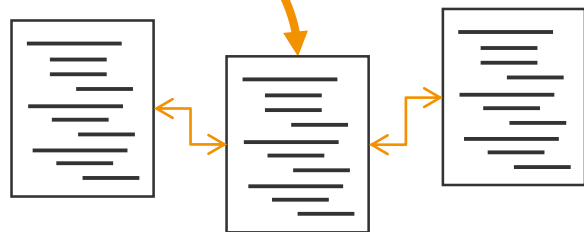


1. How would you find vulnerabilities that were not remediated for a long time?
2. How would you rank and prioritize them?
3. What would you do with the systems which have non-remediated vulnerabilities?
4. What would you do if owners did not have enough capacity or knowledge to fix the vulnerabilities?
5. What would you do if you felt push-back from a project team?

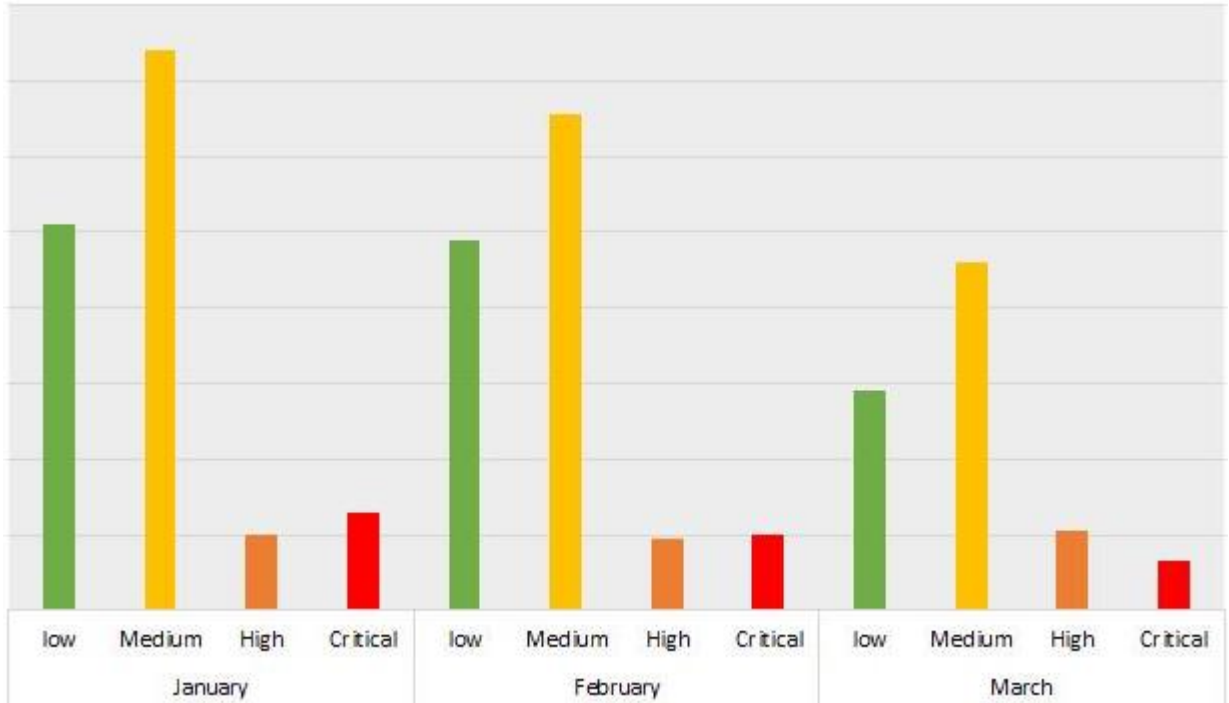
# Solving the technical problems



Totally rewriting a script

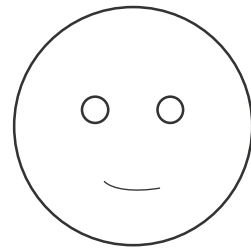


Get a small complex system of interconnected libraries with thousands of code lines

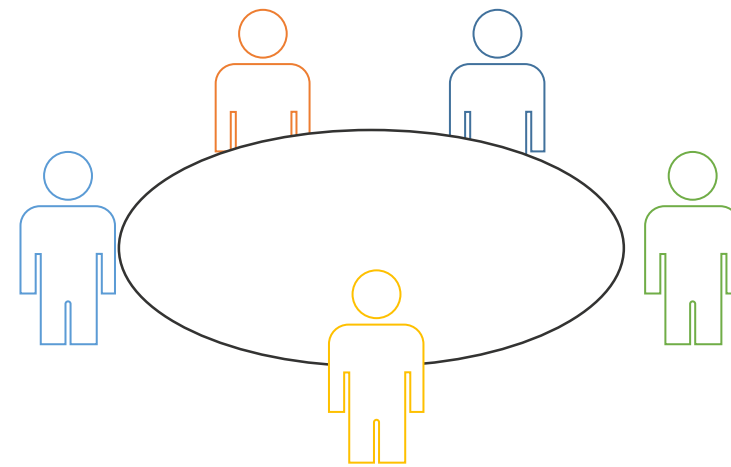


But now it: shows graphs, searches for non-remediated systems, prioritizes vulnerabilities, saves your remediation process comments, and a lot more...

# Solving the non-technical problems



Get an oversight and support from management

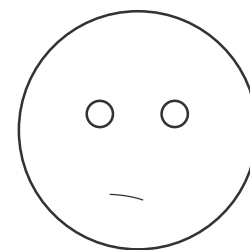


Only the management of the company can help to define priorities. Nothing works without the management oversight. Solutions will be different depending on the company and its business.

How  managed incidents





# Bad thing happened



1






## Hits by host (last 7d)



Host 	Count 
kiv-ids	66






## Source IP (last 7d)



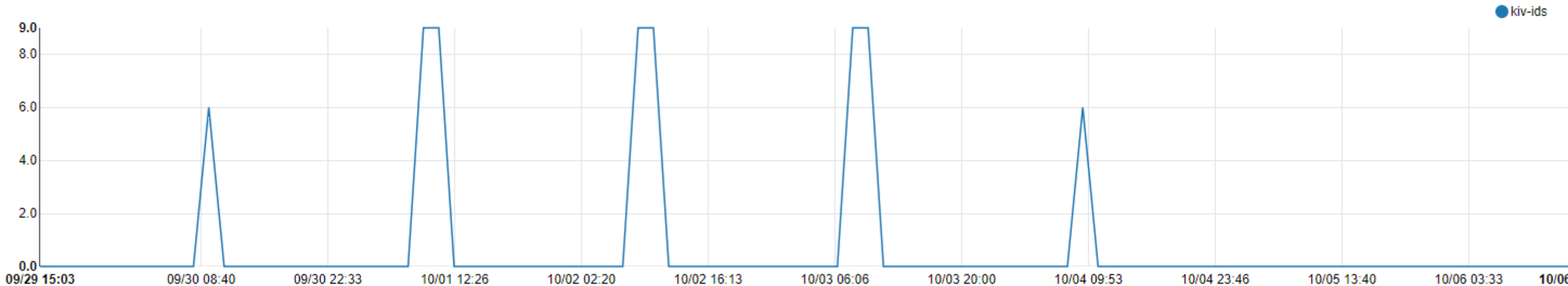
Host 	Count 	Actions 
192.168.169.4	66	 

## Destination IP (last 7d)



Host 	Count 	Actions 
65.52.144.78	66	 

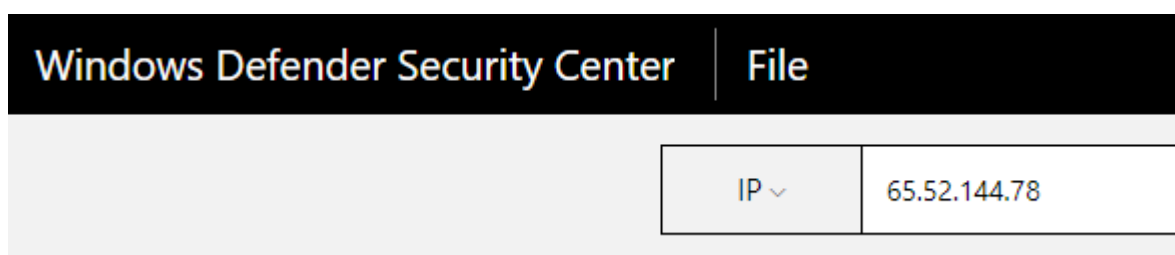
## Activity (last 7d)




# Hopefully EDR is in place

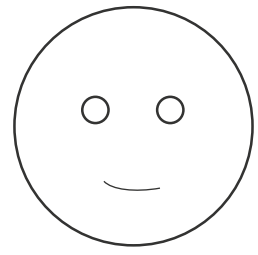


2



3

Machine		Description
10.04.2017		
10:02:32		a9b9fazaxzuaf.exe tried to communicate with 65.52.144.78
C:\Program Files\Common Files\xgstnlvi\ a9b9fazaxzuaf.exe		795c6cf6503a5ea1bb6e2805ecba8ff0c1fad945



# can block the threat in 2 clicks



4

File

File worldwide

File

Actions

Stop and Quarantine File

Block file

Action center

ea1bb6e2805ecba8ff0c1fad945

Submit a request to apply an action to this file

Issuer: unsigned

Malware detection

VirusTotal detection ratio:

52/66

VirusTotal

Windows Defender AV:

EUS:Win32/CustomEnterpriseBlock!cl

# Actually blocking it

5

Block this file?

×

This action will prevent this file from running on machines in your organization.

File details

Sha1: 795c6cf6503a5ea1bb6e2805ecba8ff0c1fad945			
Prevalance worldwide:	15.6k	File names:	2 ⓘ
Prevalence in organization:	1	File instances:	0

Reason: \*

This is a part of a Linkury PUP

ⓐ

⌚ This action applies only to files seen in the last 30 days on machines with Windows 10 Creators Update and newer.

Yes, block file

No

6

Action center

×

Stop and Quarantine file

^

Submission time	Success	Failed	Pending
-----------------	---------	--------	---------

Block file

^

Submission time	Status	
10.06.2017   15:19:19	Blocked	✕ Remove from block list

⌚ 10.06.2017 | 15:19:19 File blocked  
vchakryan@dataart.com: This is a part of a Linkury PUP







ⓘ For submitted actions to take effect, machines must be connected to the network.

Close

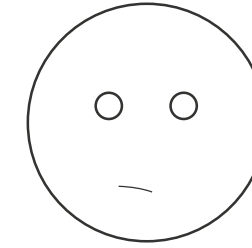
# It worked



7

Date	Event	Details
10.04.2017		
11:13:52	 Windows Defender AV detected an active 'CustomEnterpriseBlock' malware	
11:13:52	 <a href="#">e5cbd5ewaxwhw.exe</a> was blocked by enterprise response policy  C:\Program Files\Common Files\2muiu4a1\e5cbd5ewaxwhw.exe  <a href="#">Read more on Microsoft Encyclopedia</a>	  <a href="#">795c6cf6503a5ea1bb6e2805ecba8ff0c1fad945</a>

# CoinMiner detected by IDS



1

"signature": "ETPRO TROJAN CoinMiner Known Malicious Stratum Authline (2017-08-31 1)",



"dest\_ip": "149.28.199.108",

"packet": "ThP7ANPteCSvnkC/CABFAAAoK/JAAIAG66/AqMX8IRzHbGN6Absldio1KqOg8FARBAFIMAAAAAAAAAAAAA",

# Use EDR to detect soft



2

13:06:44	 [REDACTED]	brt.exe successfully established connection with 149.28.199.108:443 (a.deepsecu.com)	
	c:\program files (x86)\brtsvc\brt.exe	9016e3d0f3391dc64ddb9d4ea588d0d6afe912c7	

# Scripting detection 3



Run query



New



Save



```
1 MiscEvents
2 | where EventTime >= ago(1d) and (FileName == "BRTSvc.exe" or FileName == "brt.exe" or FileName == "brtsvc.exe")
3 | project SHA1, FileName, FolderPath, FileOriginIP, FileOriginUrl, EventTime, MachineId, ReportId
```

Run query



New



Save



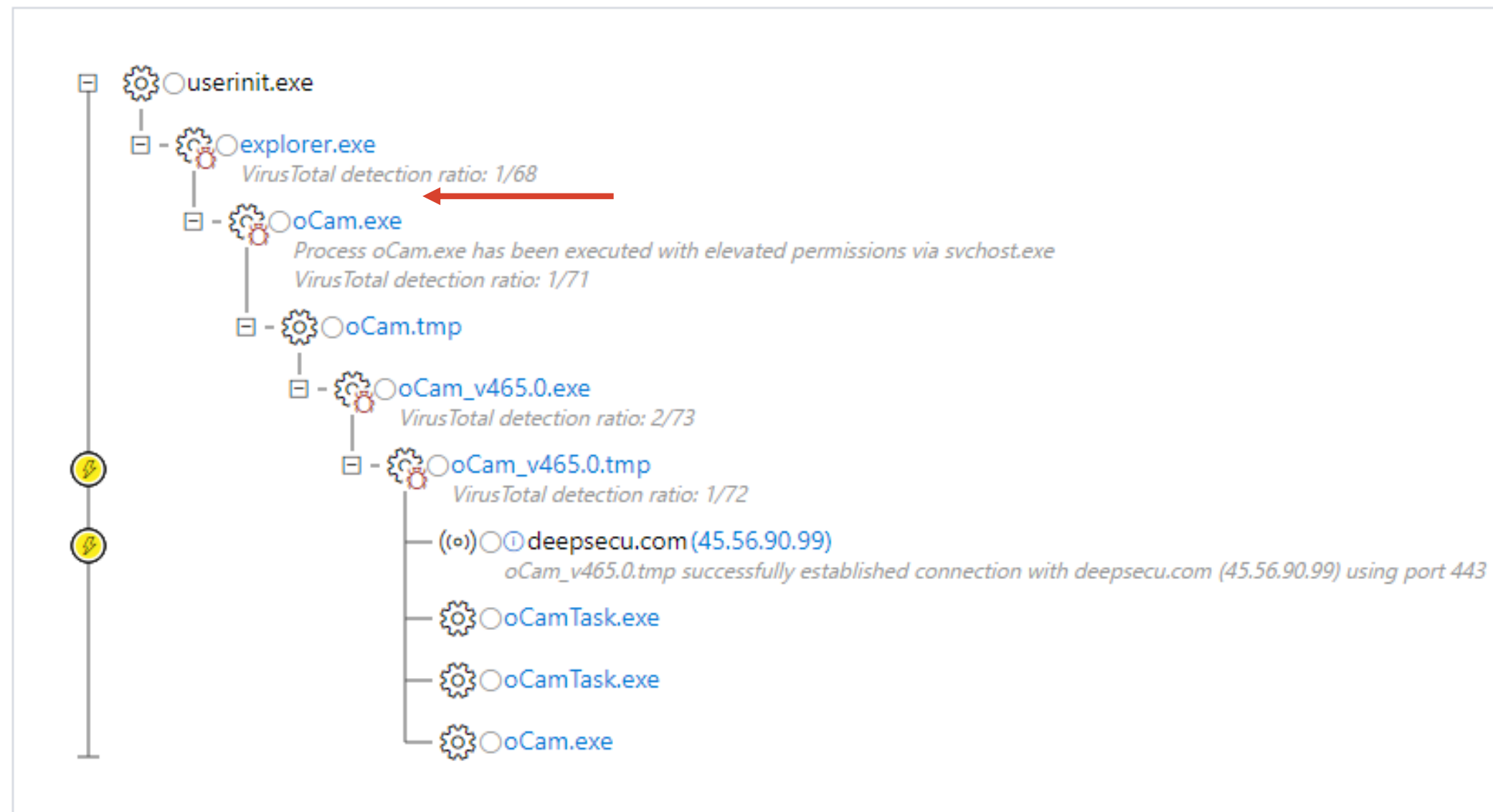
```
1 NetworkCommunicationEvents
2 | where EventTime <= ago(1d) and RemoteUrl contains "deepsecu."
3 | project EventTime, MachineId, ReportId
```



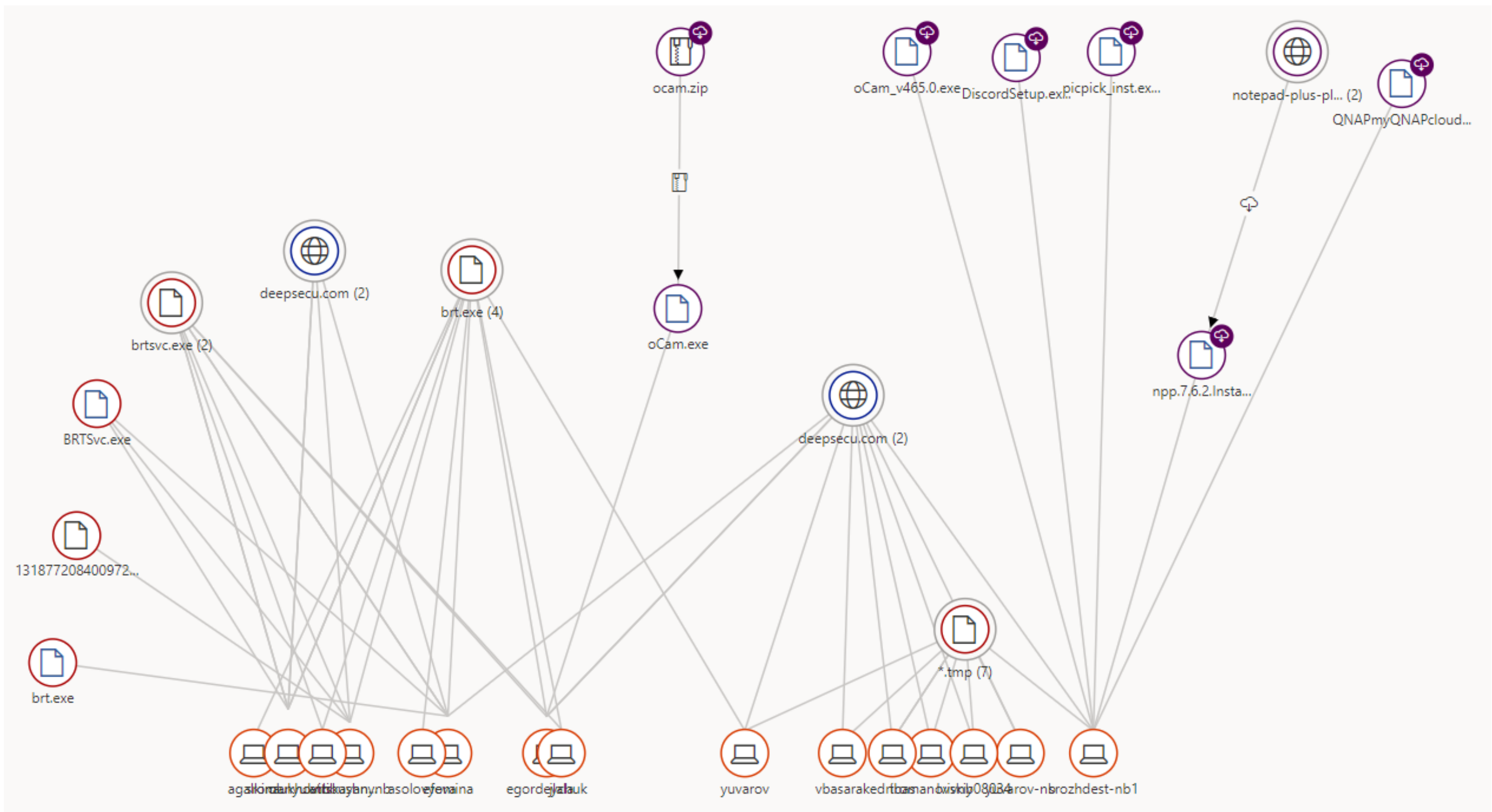
# Hidden threat

4

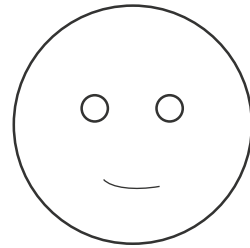
Alert process tree



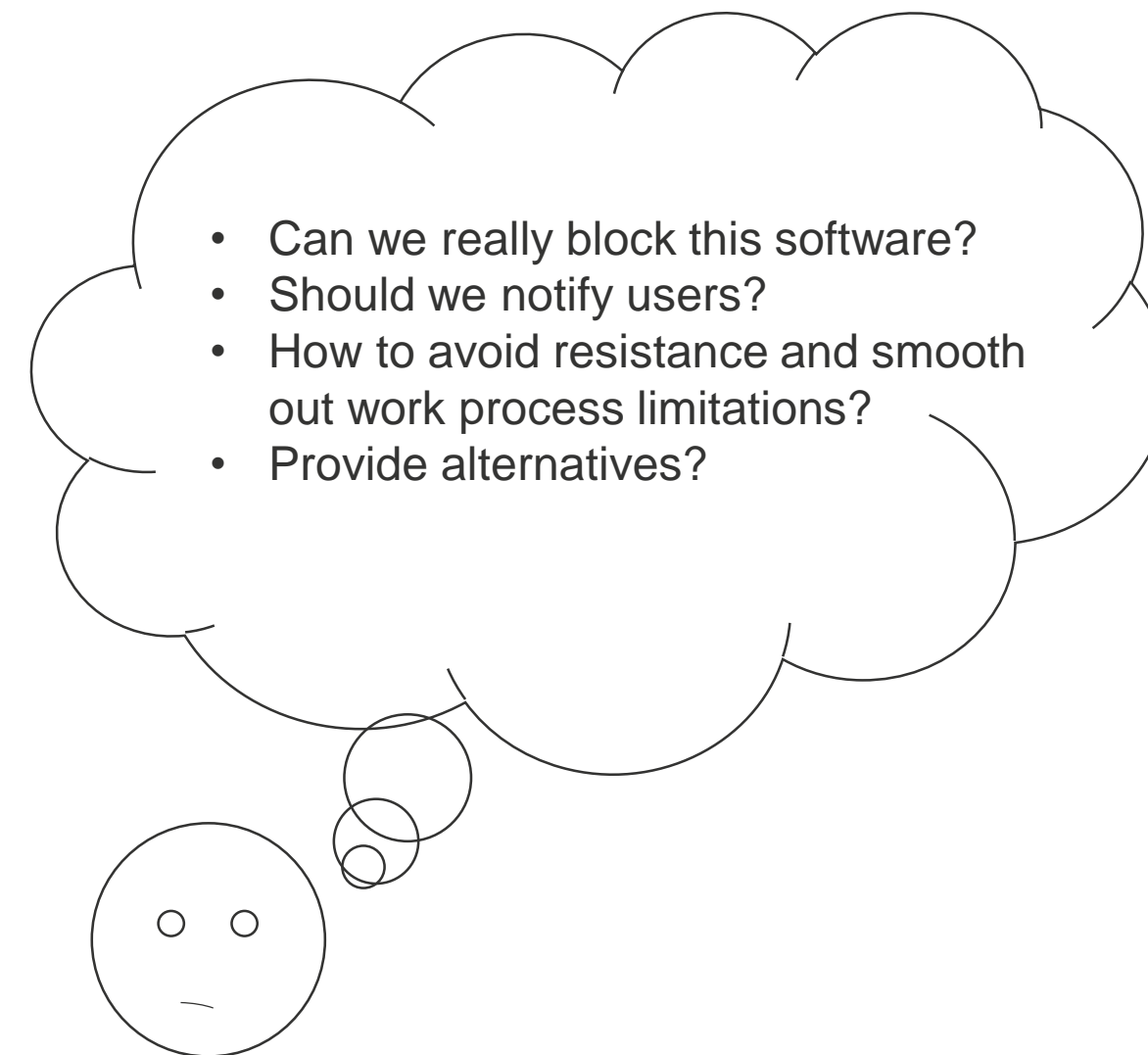
# Here how the graph looks like



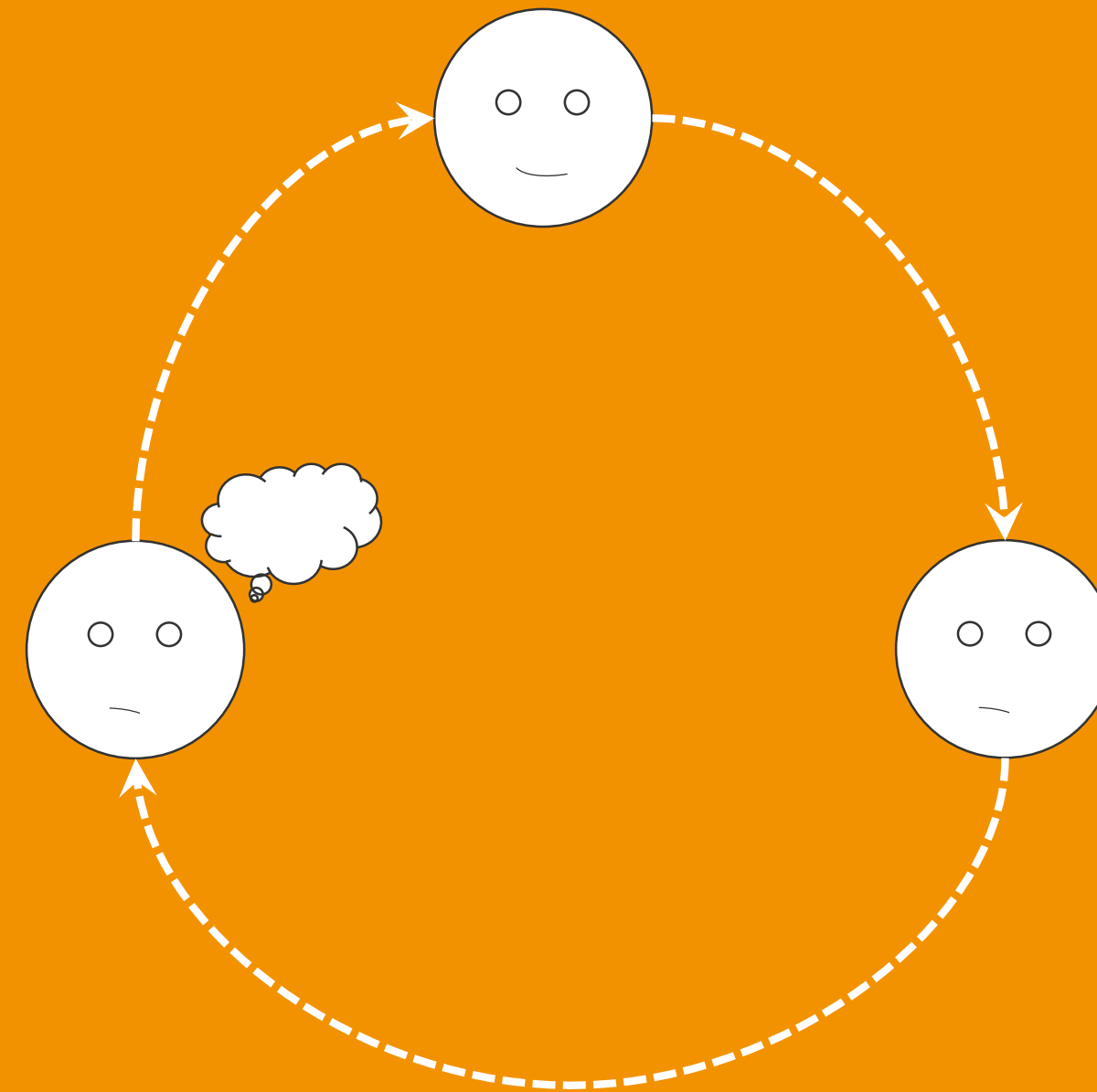
# Blocking a threat



- ✓ Block domains on firewalls
- ✓ Block files at EDR console
- ✓ Detect and alert constantly



# Work Lifecycle



Thank you!

