Enterprise Security

Penetration Test and Red Team Perspectives

Ahmed Shah | ashah@redcanari.com

NMFTA
National Motor Freight Traffic Association, Inc.

DIGITAL SOLUTIONS CONFERENCE
CYBERSECURITY
NOV 2022

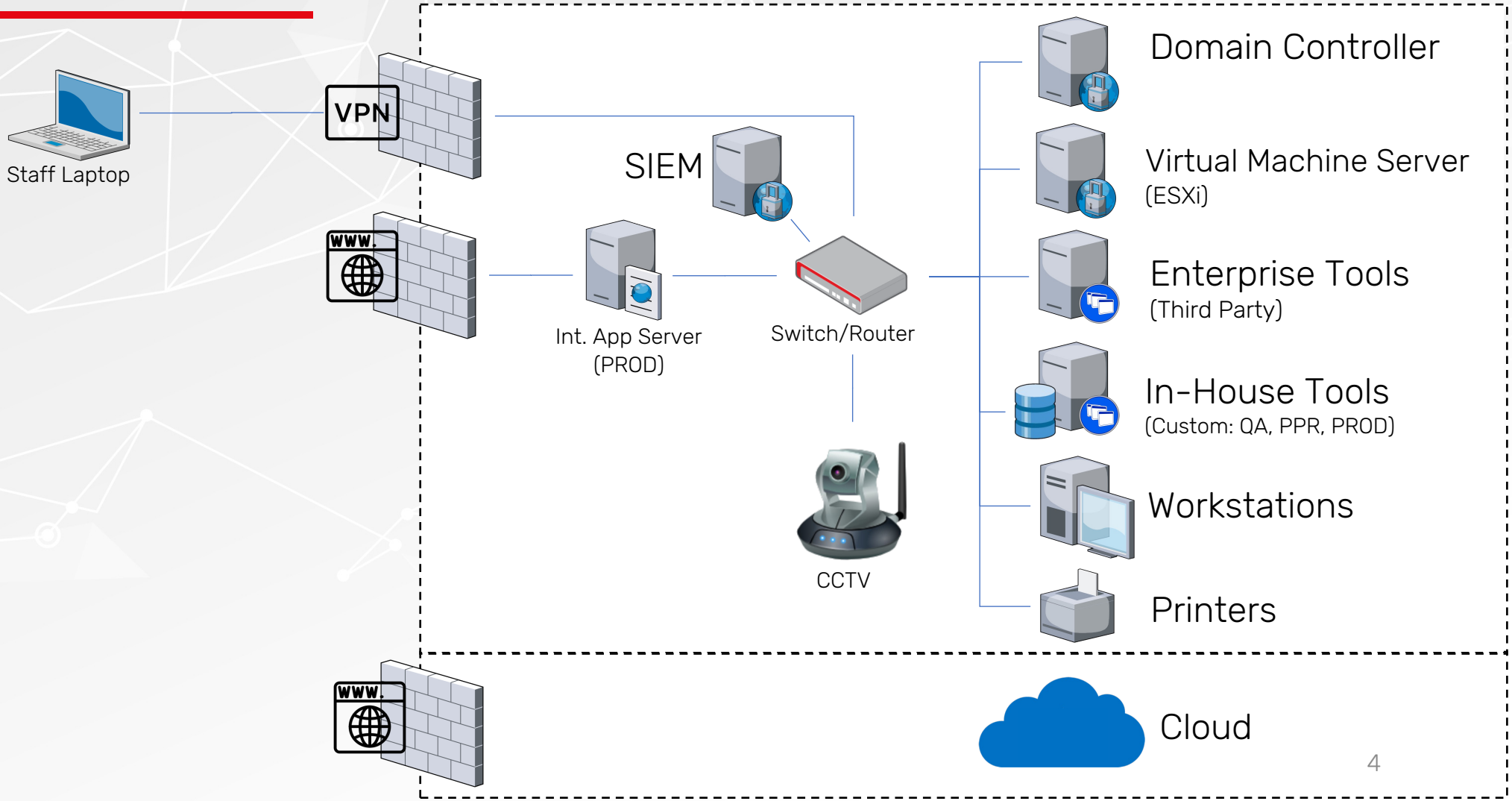
Pen-test vs Red Team

	Penetration Test	Red Teaming
Under Assessment	Application Security	Application Security
		Infrastructure Security
	Infrastructure Security	People, Processes
		Detection Effectiveness (IDS & EDR)
		Logging
Who is Aware of Assessment?	Everyone in organization	Only a few (Blue Team Not Aware)
Volume of Security Events	High	Low (Need to be Under the Radar)

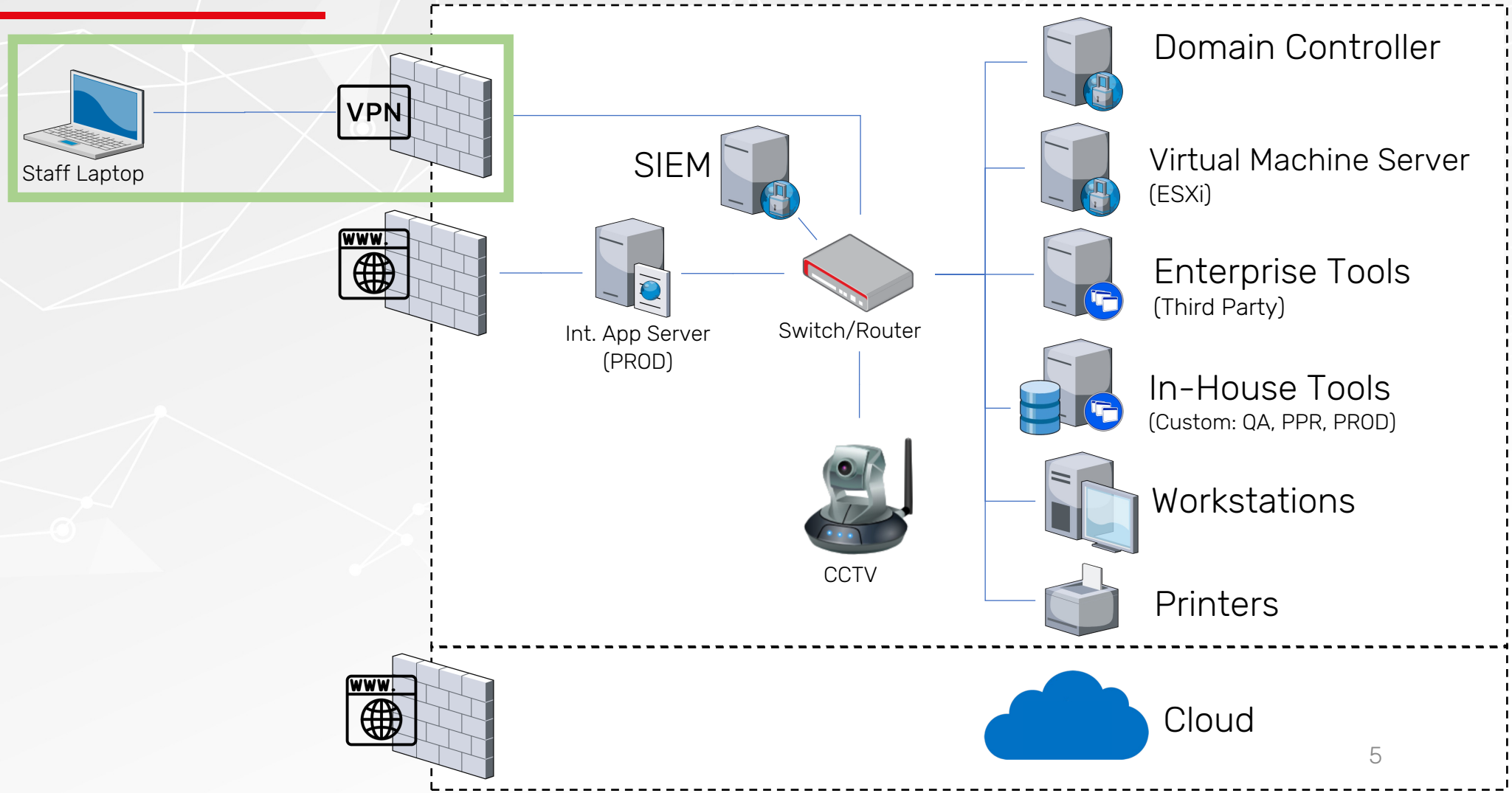
Outline

- Model of Corporate Network
- Open-Source Intelligence
- External Security
- Internal Security
- Organization Conduct

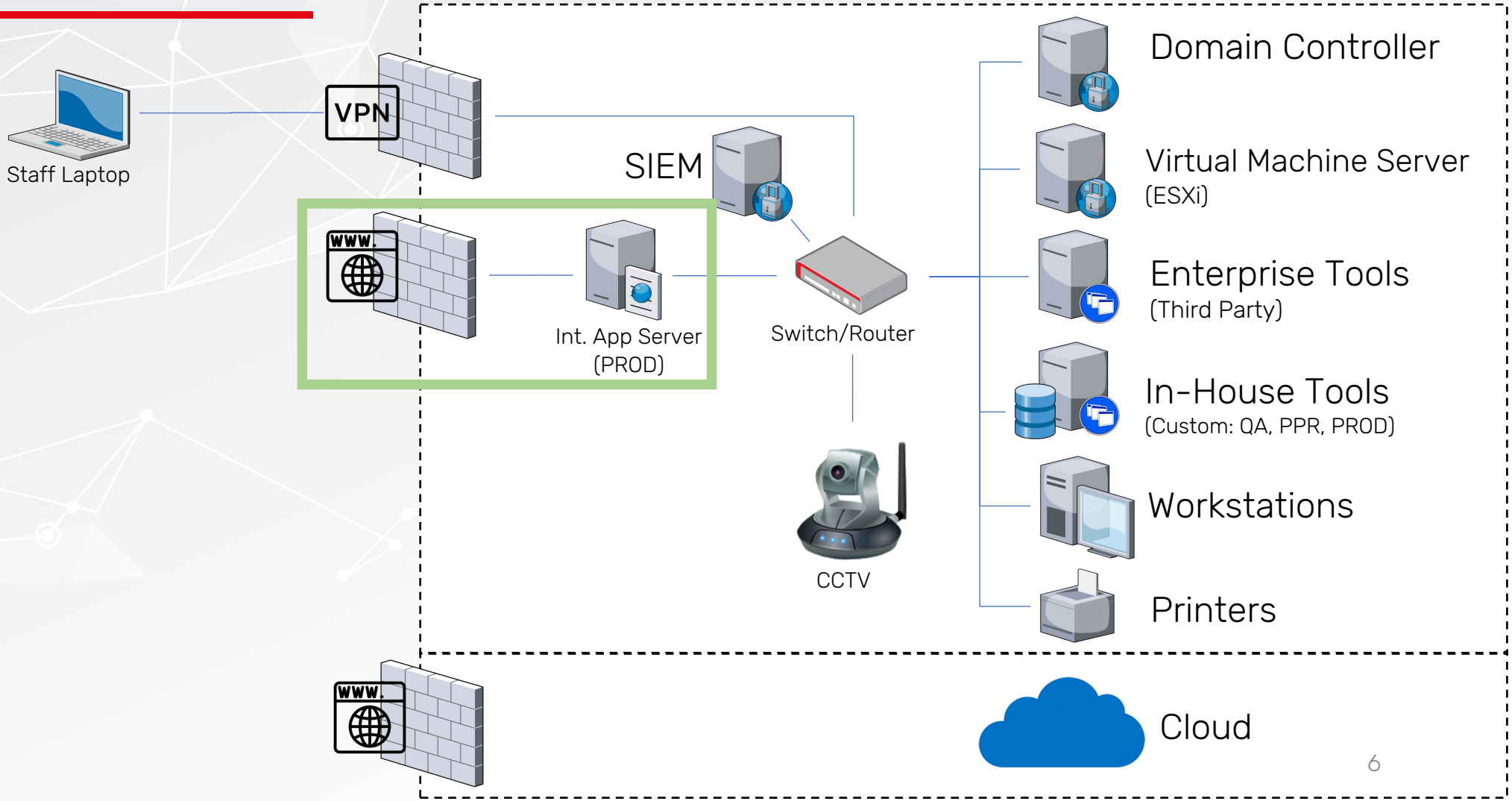
Model of Corporate Network



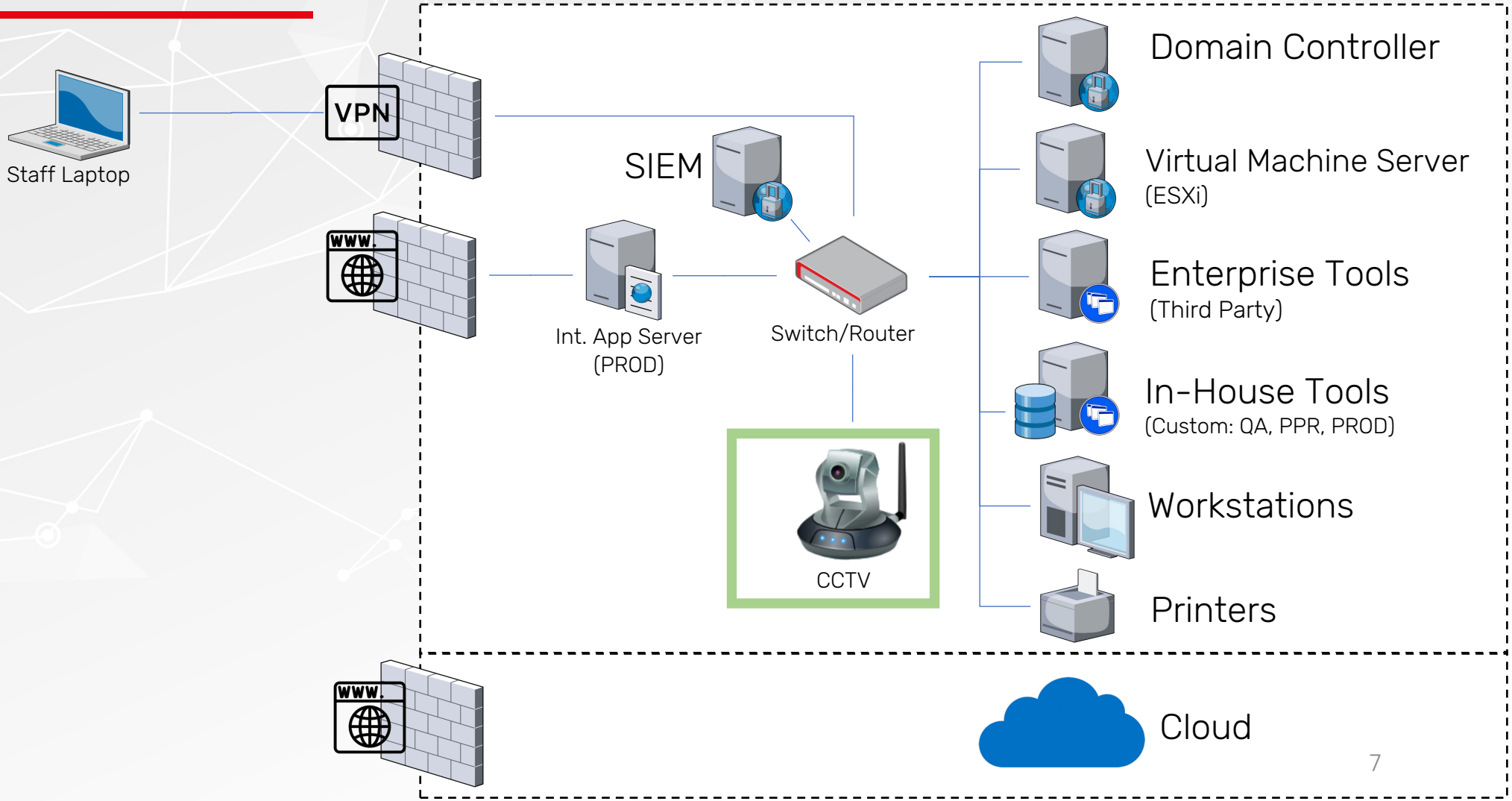
Model of Corporate Network



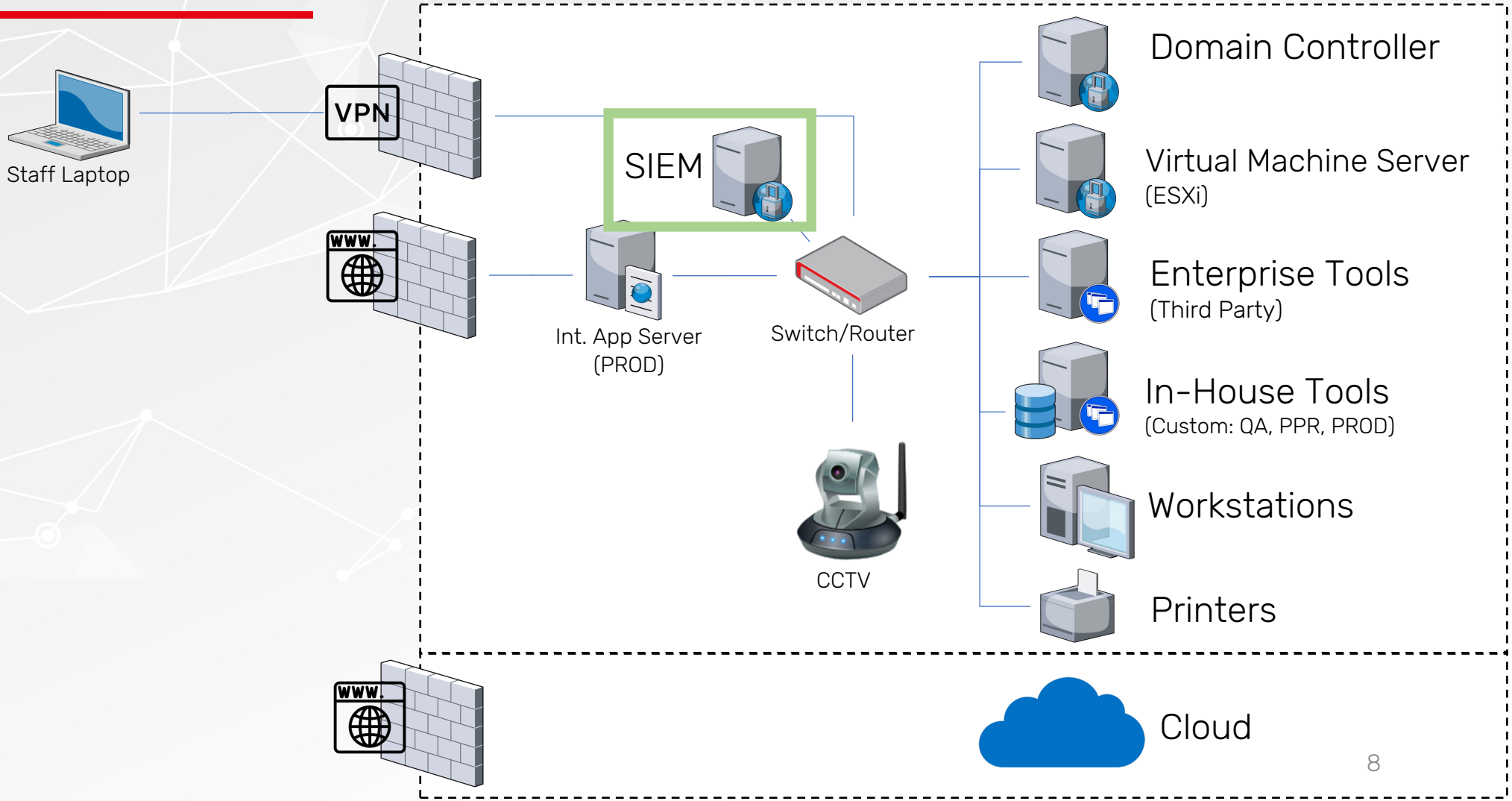
Model of Corporate Network



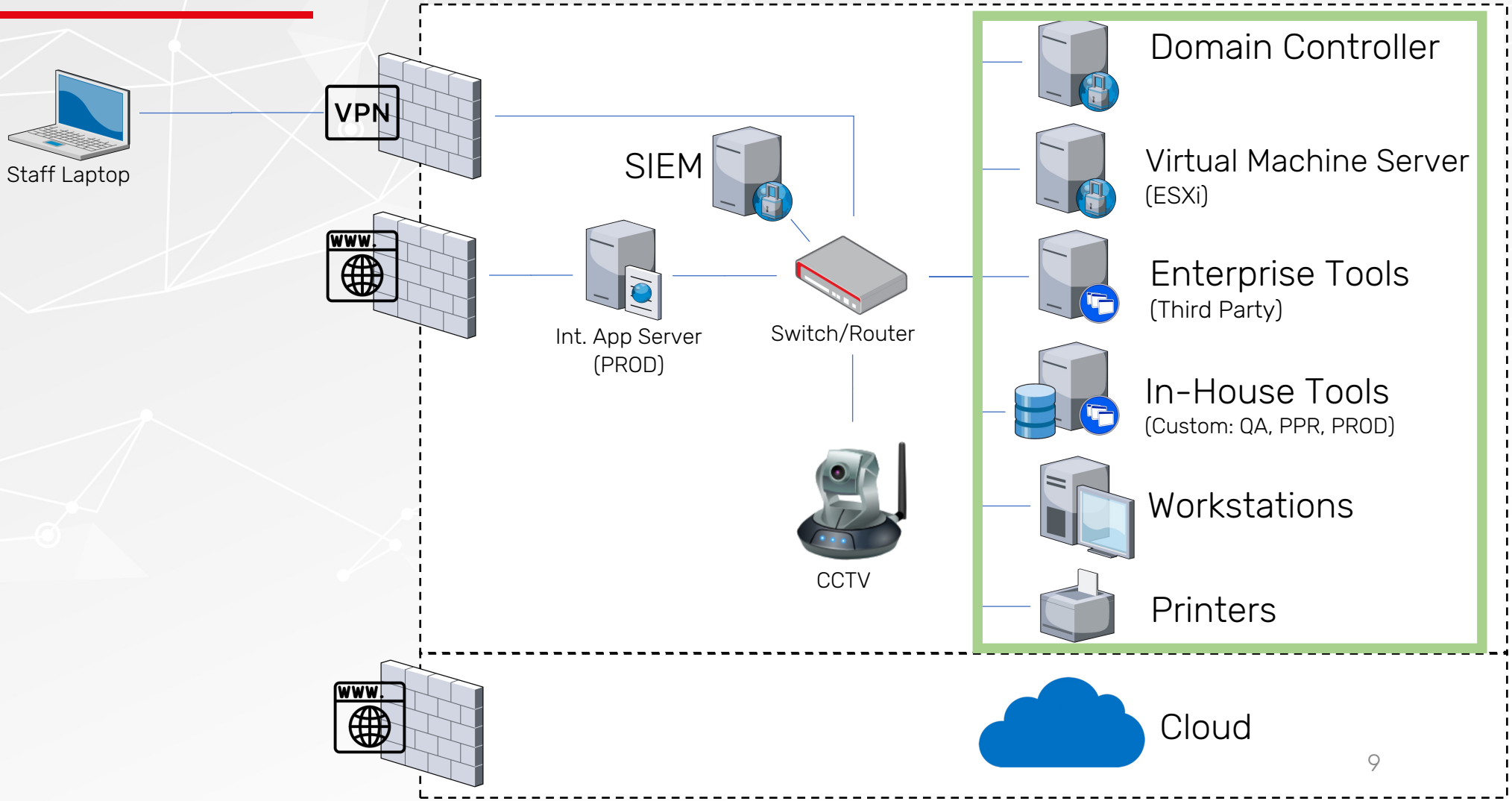
Model of Corporate Network



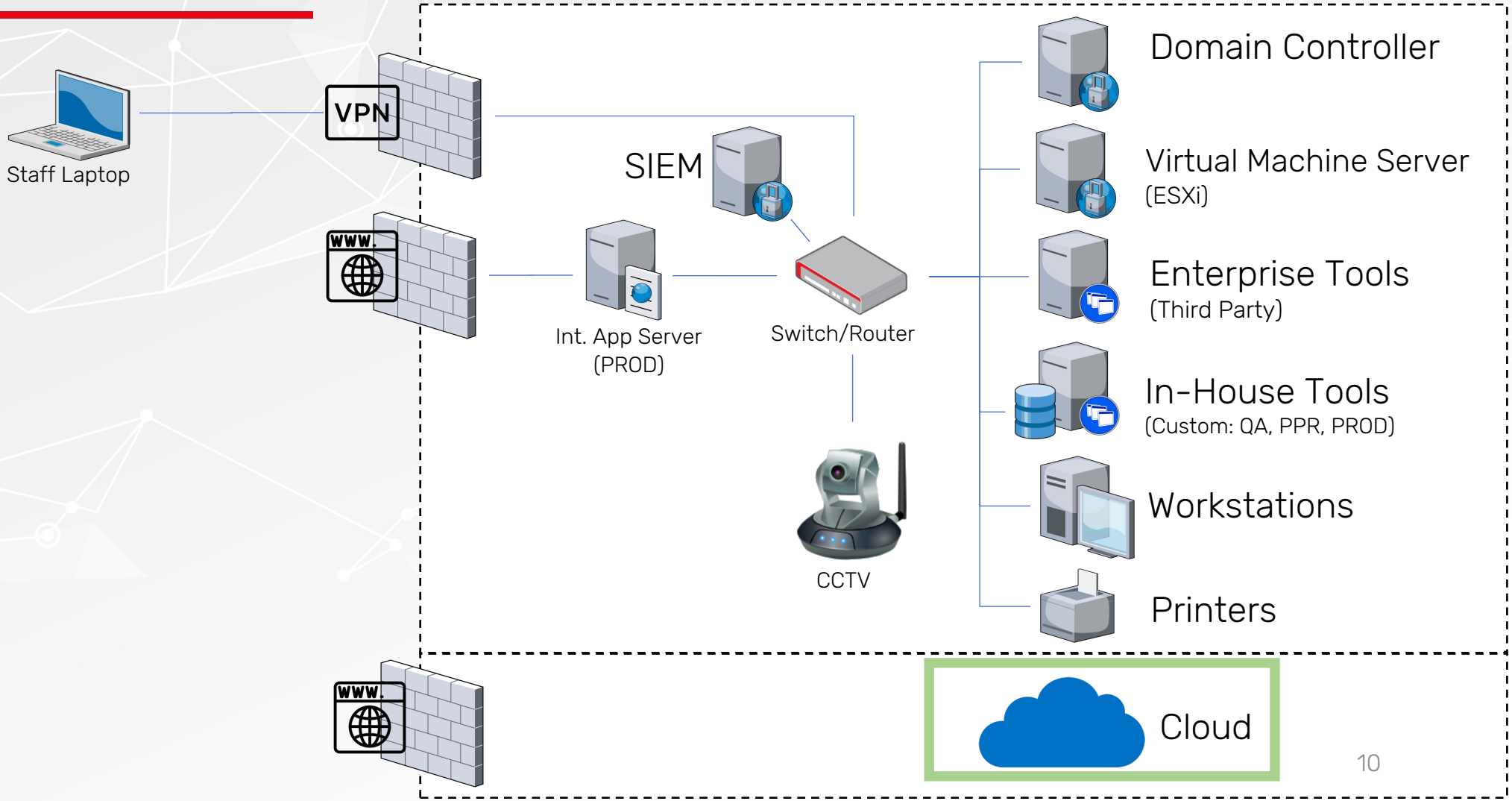
Model of Corporate Network

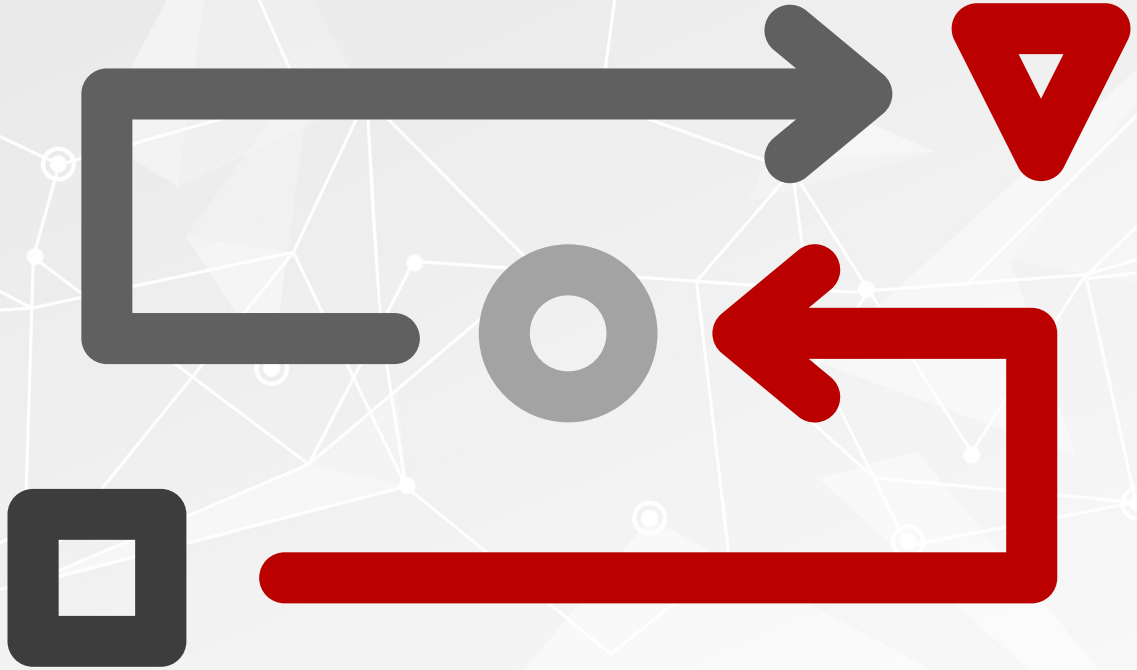


Model of Corporate Network



Model of Corporate Network





Open-Source Intelligence

OSINT

Goal: Find sensitive info. about the organization and it's systems.

- Private customer information
- Administrative user guides
- subdomains
- Unintended exposed ports/services
- Technologies Used
- UserIDs
- Leaked source code
- API keys / passwords

OSINT - Shodan

SHODAN | Explore | Downloads | Pricing | port:21 "220-QTCP" country:"US,CA" as400 | Account

TOTAL RESULTS

57

TOP COUNTRIES

United States	56
Canada	1

TOP CITIES

New York City	7
Atlanta	3
Chicago	2

View Report | Download Results | Historical Trend | View on Map

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

2021-11-11T01:49:35.357265

Savvy Networks
USA
United States, White Plains

```
220-QTCP at AS400.
220 Connection will close if idle more than 5 minutes.
530 Log on attempt by user ANONYMOUS rejected.
214-Server-FTP commands follow:
214-Unsupported commands marked with an *.
214-ABOR, ACCT*, ADDM, ADDV, ALLO*, APPE, AUTH, CDUP, CRTL, CRTP, CRTS,
214-CWD, DELE, DLTF, DLTL, ...
```

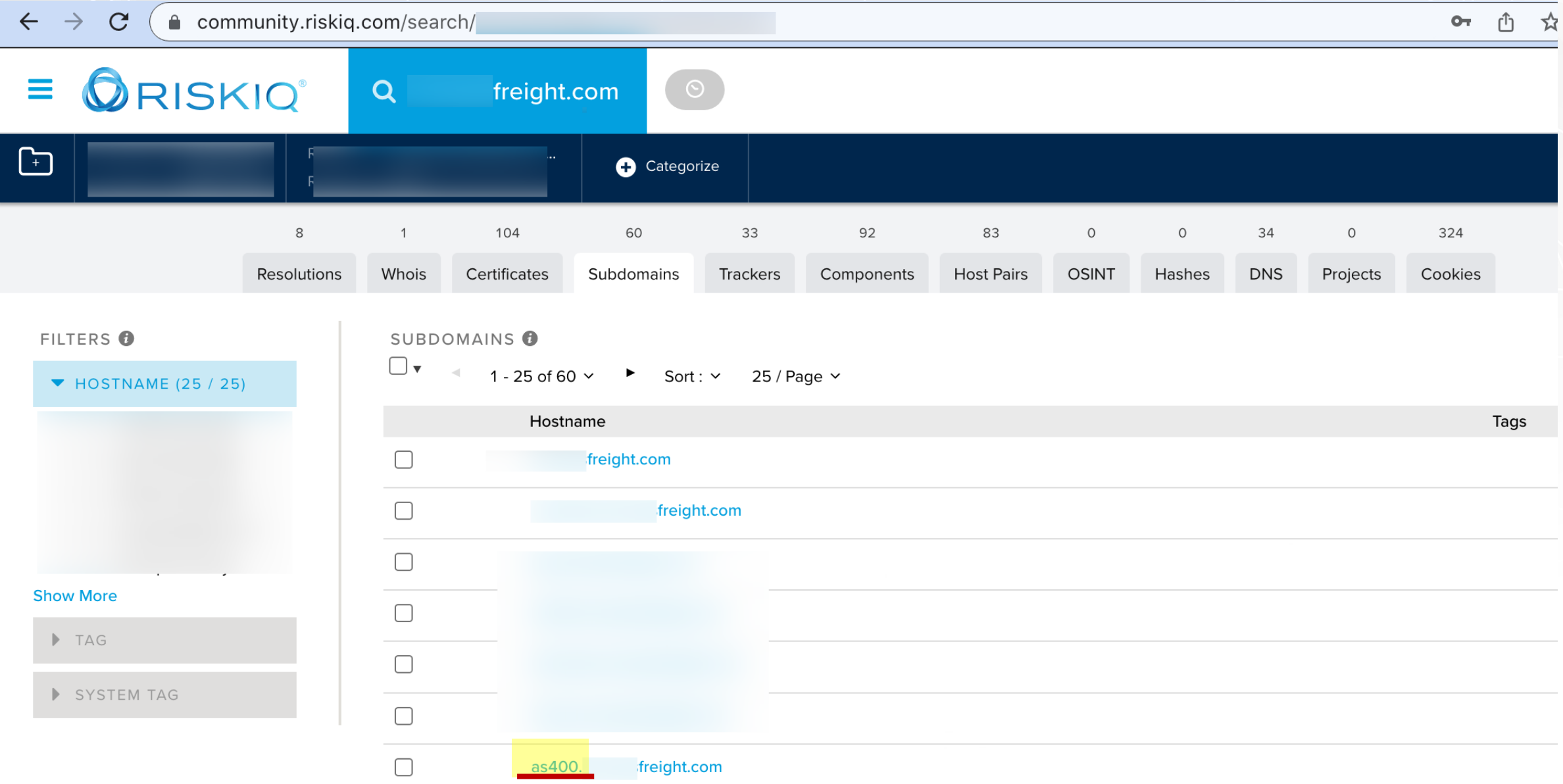
220-QTCP at AS400. [redacted] FREIGHT.COM.

2021-11-10T21:34:13.563147

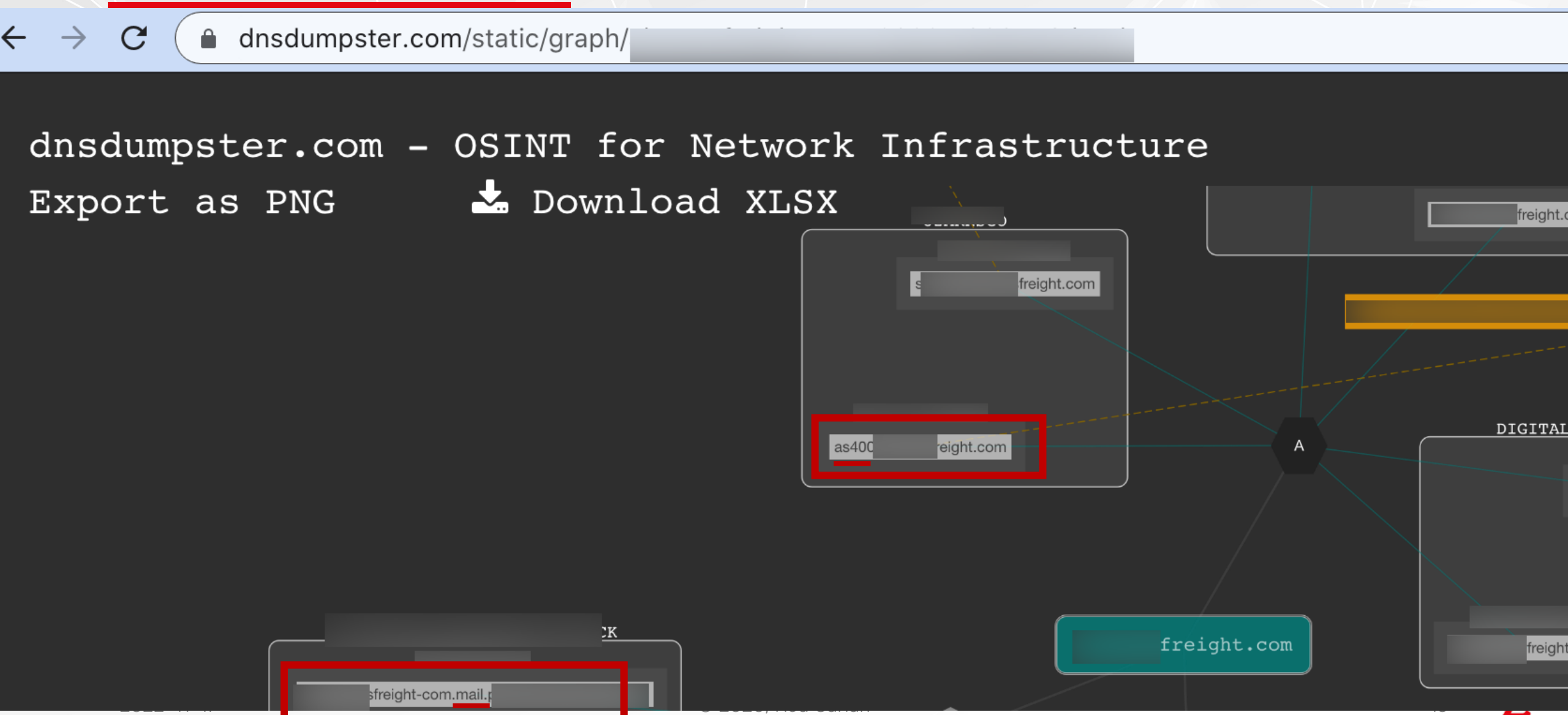
OzarksGo, LLC
United States, Fayetteville

```
220-QTCP at AS400.      FREIGHT.COM.
220 Connection will close if idle more than 5 minutes.
530 Log on attempt by user ANONYMOUS rejected.
214-Server-FTP commands follow:
214-Unsupported commands marked with an *.
214-ABOR, ACCT*, ADDM, ADDV, ALLO*, APPE, AUTH, CDUP, CRTL, CRTP, CRTS,
214-CWD,...
```

OSINT – RiskIQ

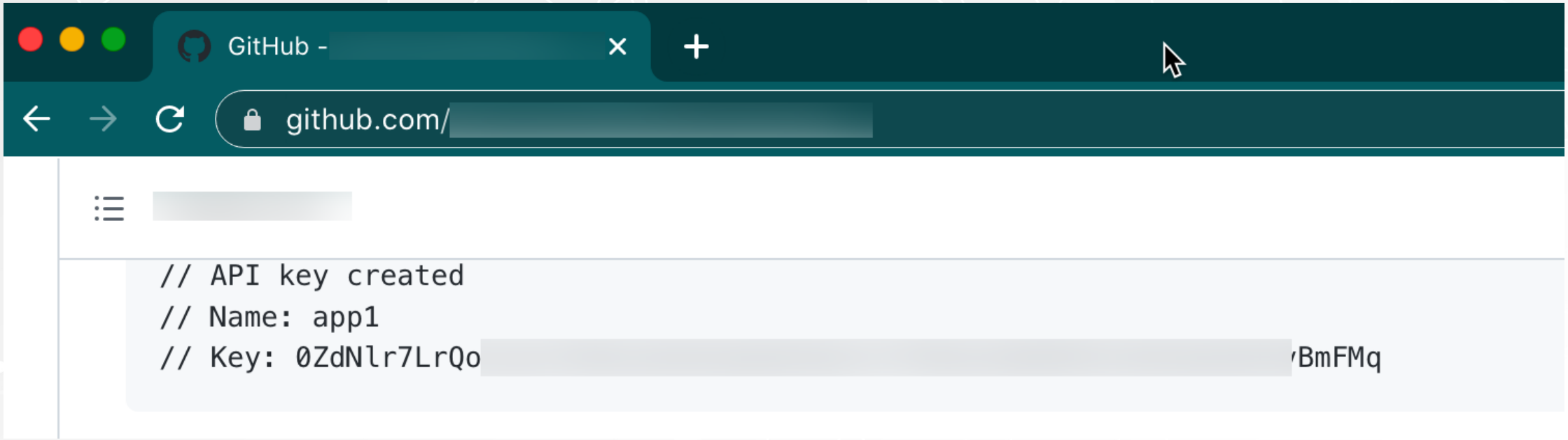


OSINT – DNSdumpster



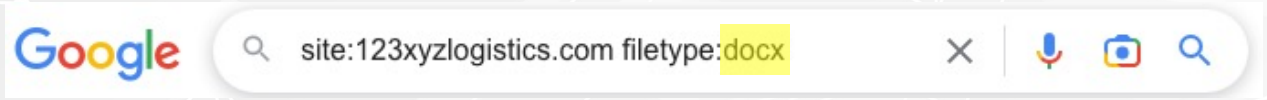
OSINT – Github & Stackoverflow

- Are employees or contractors accidently leaking code in Stackoverflow or Github?



OSINT – Other Places to Look

- Google / DuckDuckGo “Dorking”
  - `filetype: pptx, docx, xlsx, ext..`
  - `site:<companywebsite>`



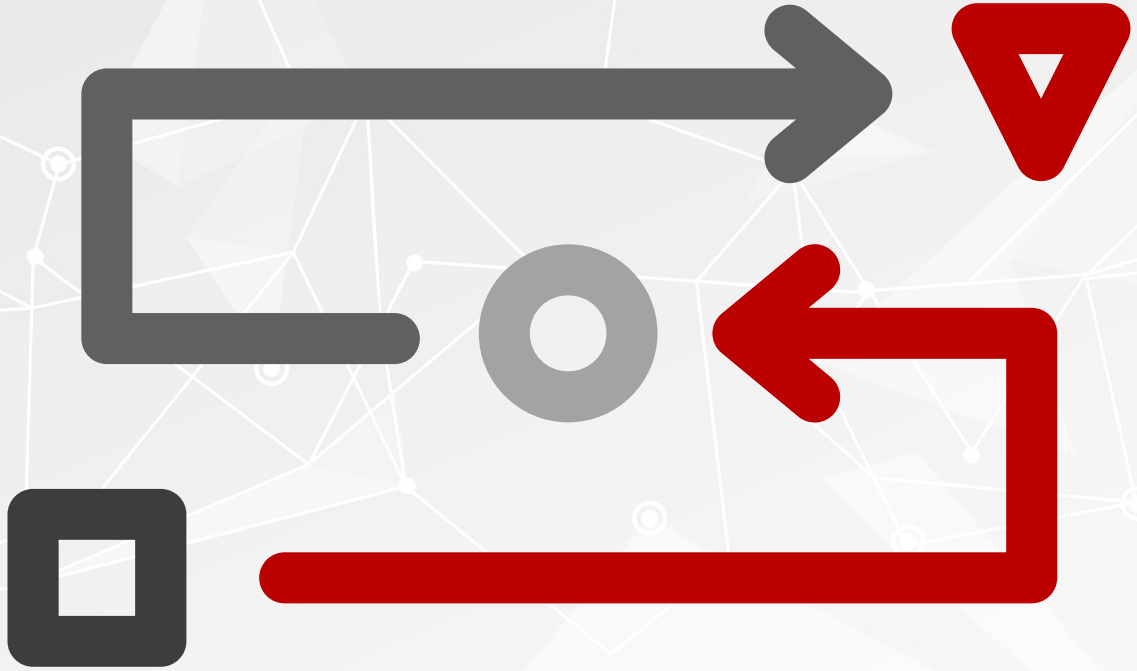
- Company Website Staff Directory
  - Look for IT Accounts

- Web Crawling Files
  - `https:\\<org>\robots.txt`

```
user-agent: *
allow: /*
user-agent: googlebot*
disallow: /secretpath/adminportal/
sitemap: https://example.com/sitemap.xml
```

- Internet Archive
  - Are sensitive leaks permanently logged?
  - `https://archive.org/`

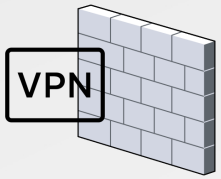
- LinkedIn Bios and Job Postings
  - What kind of technology is used in your organization?



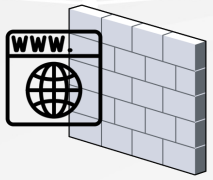
External Security

Lack of MFA (Multi-Factor Authentication)

- Login Portals are Susceptible to Brute force Attacks
  - Potential Data Sources for Accounts:



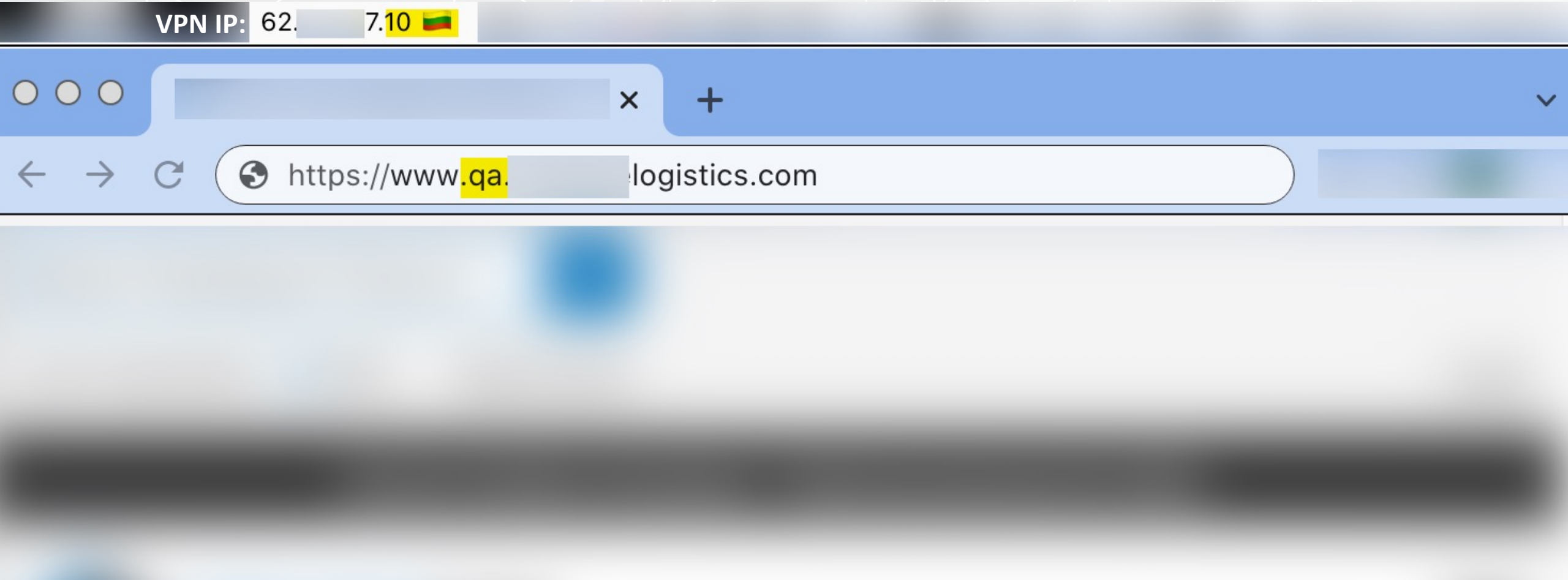
    - COMB (Compilation of Many Breaches) – 3.2 Billion Email/Passwords
    - Build login usernames based on staff names found in LinkedIn
    - Company directories
  - Techniques



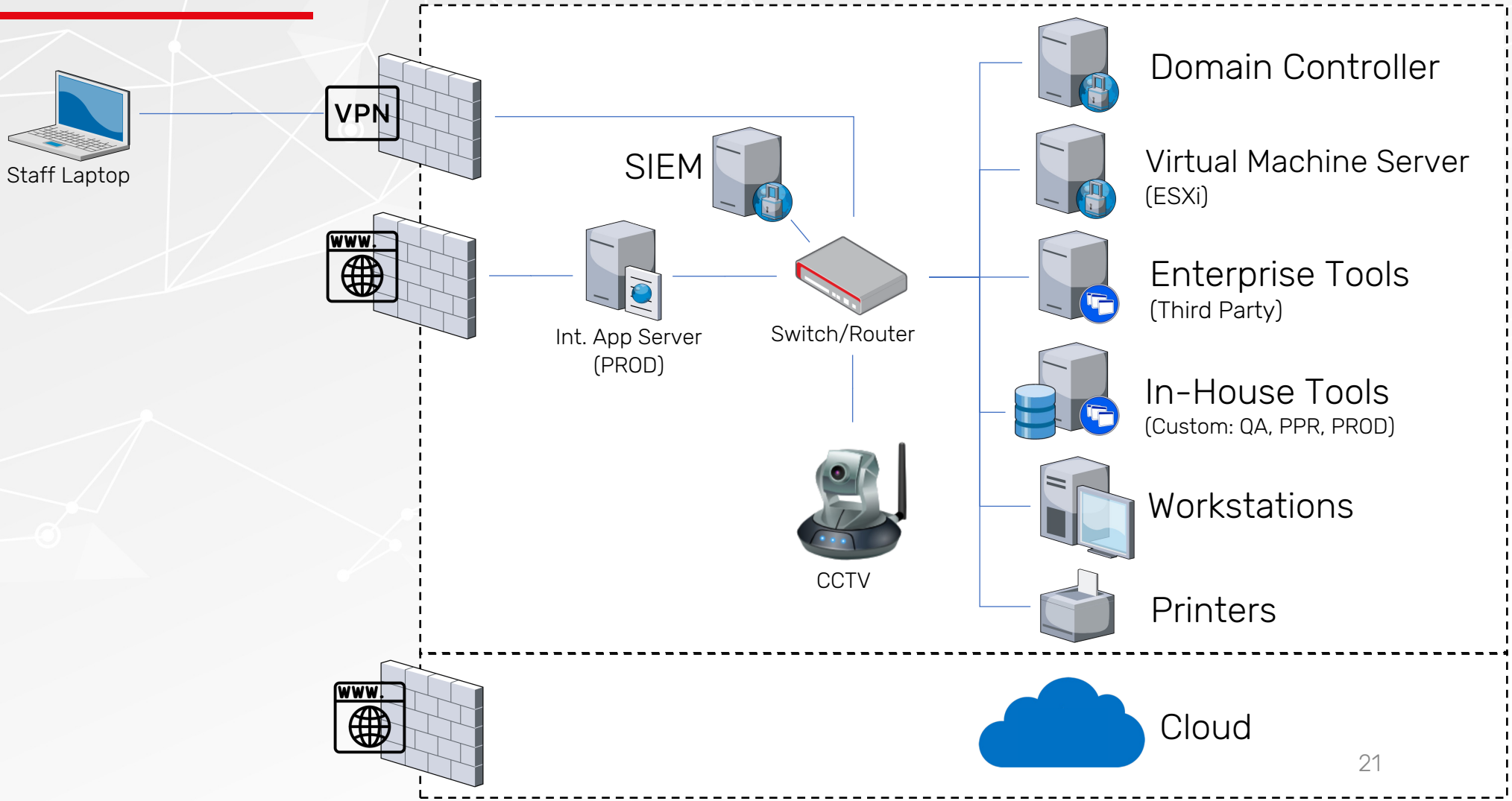
    - Password spray (Takes into account time-out delays)
    - Social-engineering to get answers for password reset security questions

QA Exposed to Internet

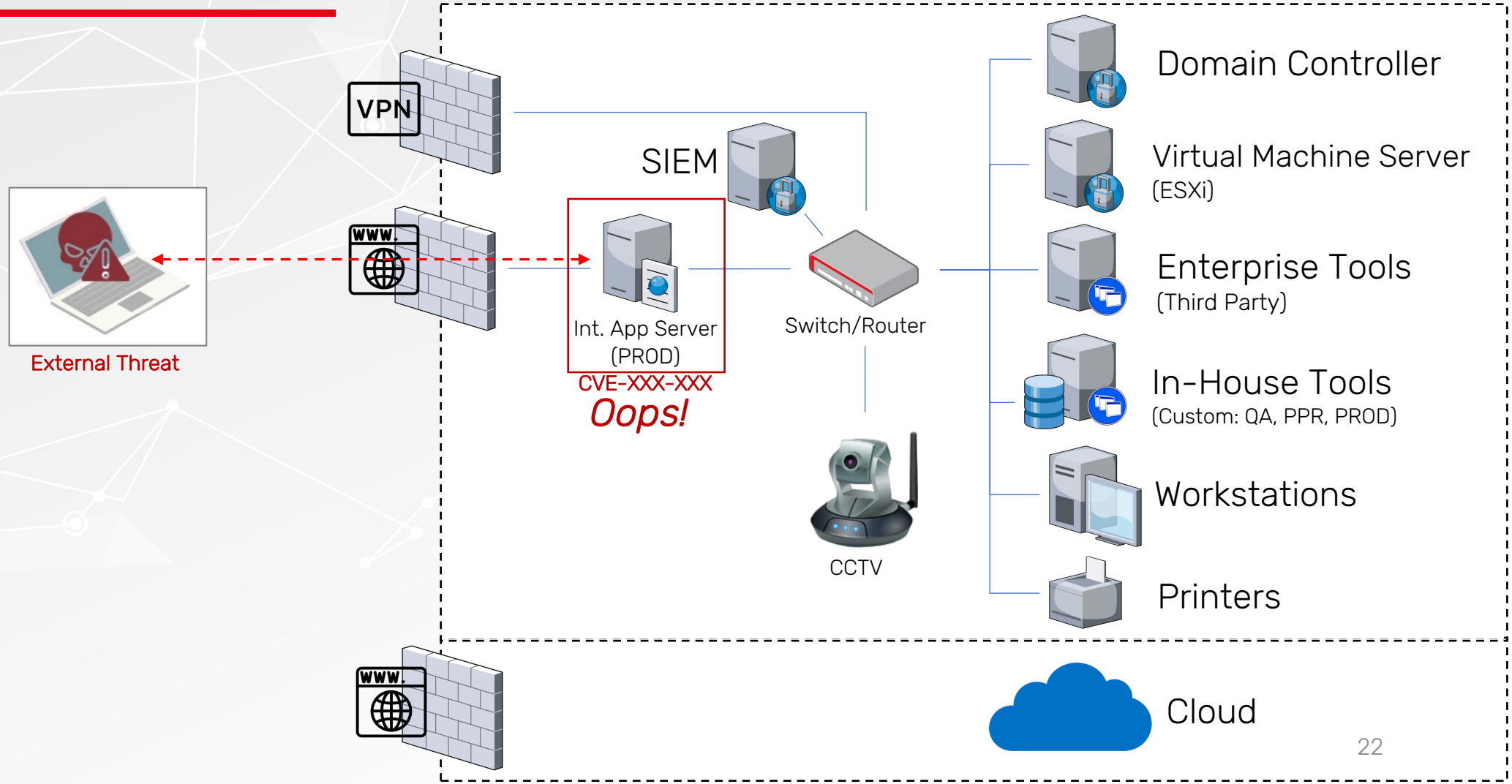
- Does site need to be accessed from all corners of the world?



Lack of Patch Planning



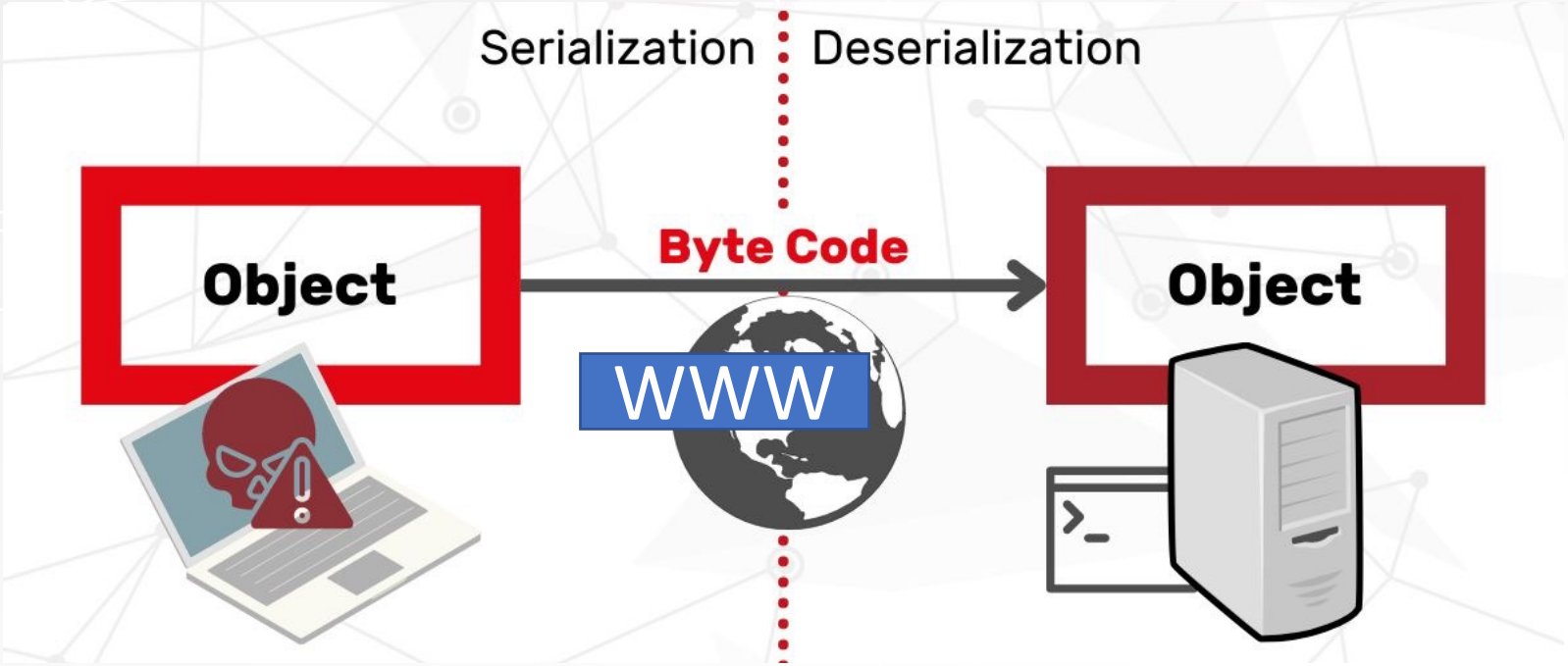
Lack of Patch Planning



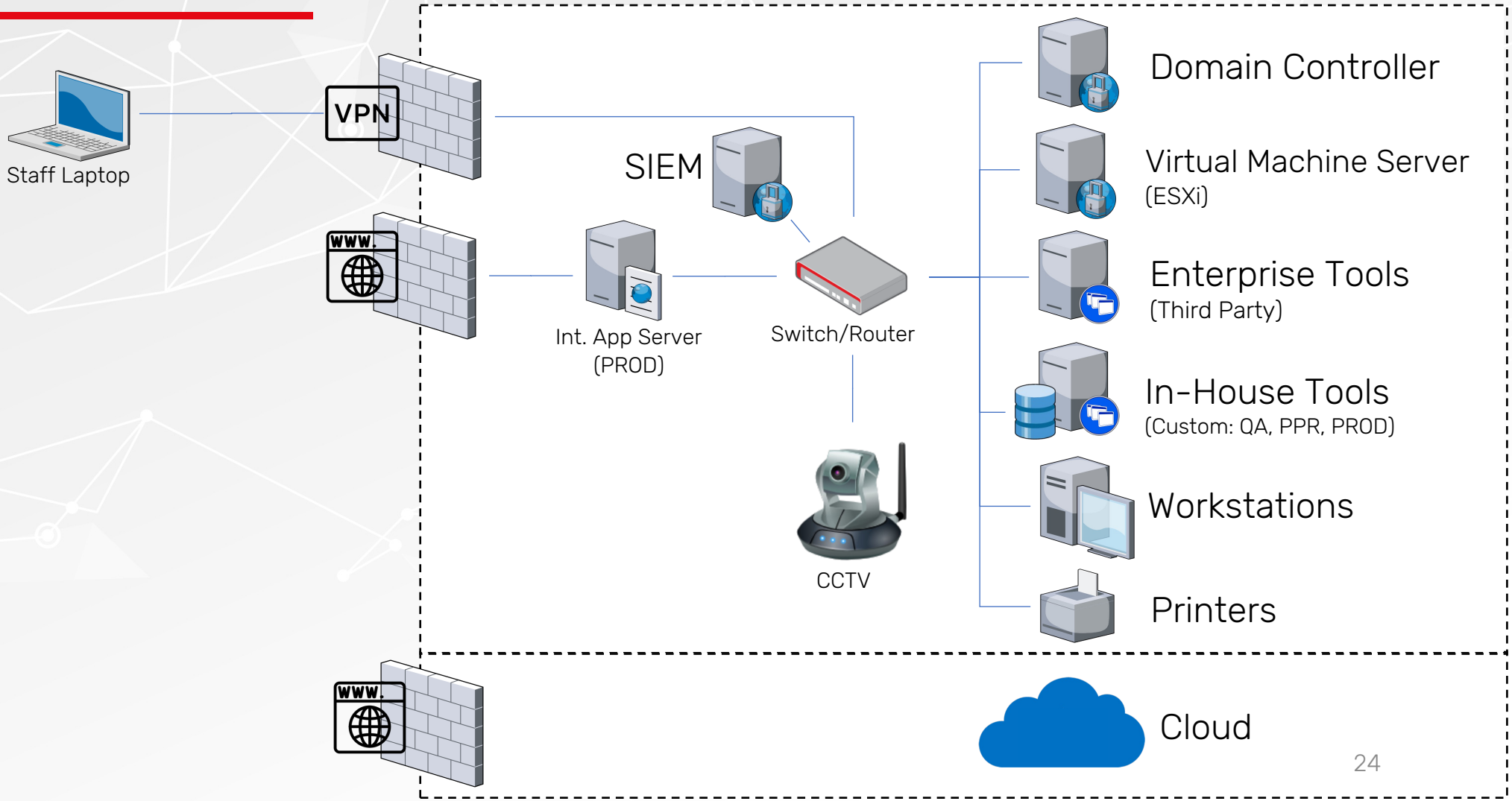
Lack of Patch Planning

Example: Enterprise Resource Planning Software

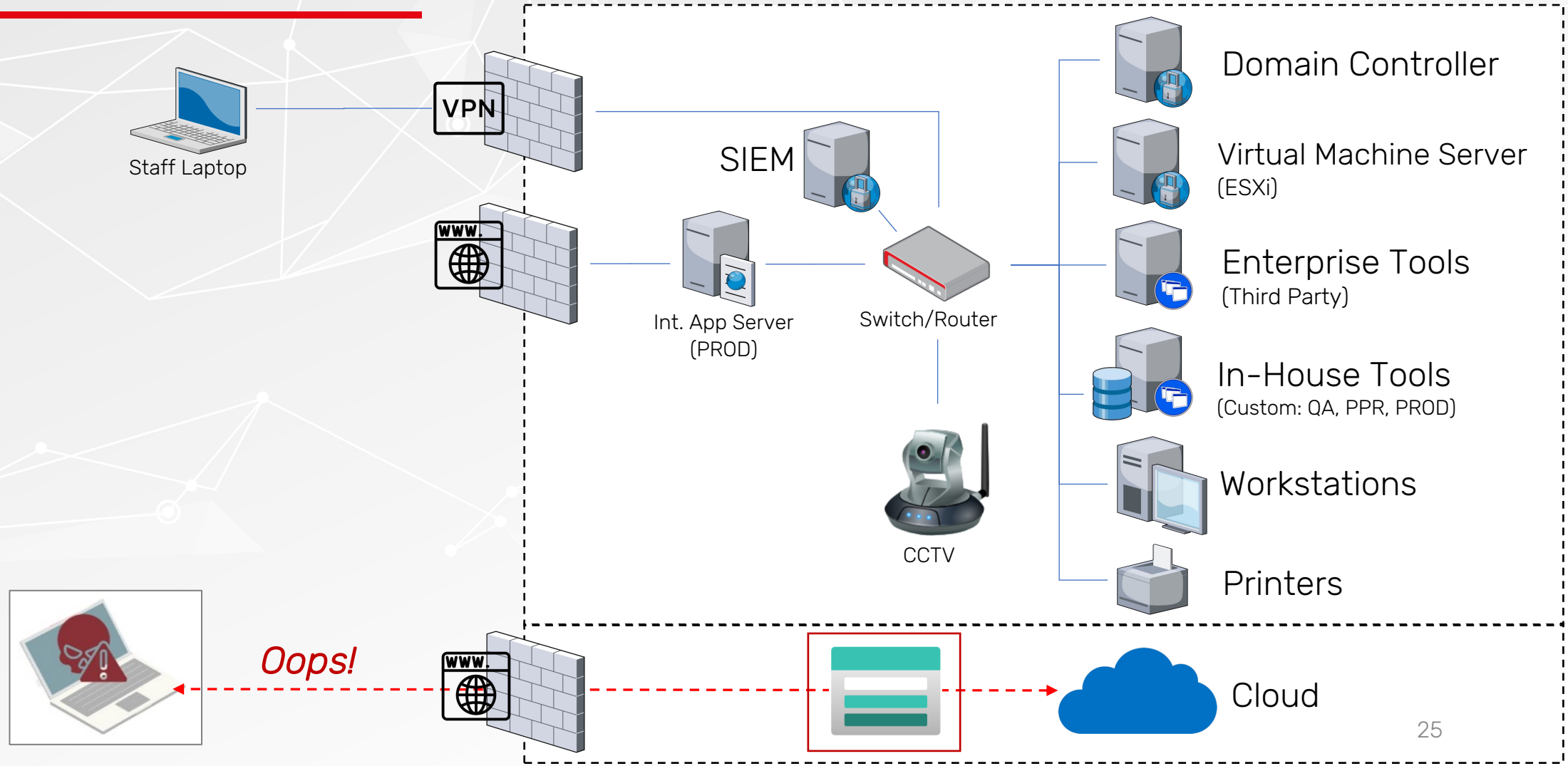
- Oracle PeopleSoft
  - (CVE-2022-21481) Stored Cross-Site Scripting
  - (CVE-2022-21543) Remote Code Execution via Java Deserialization

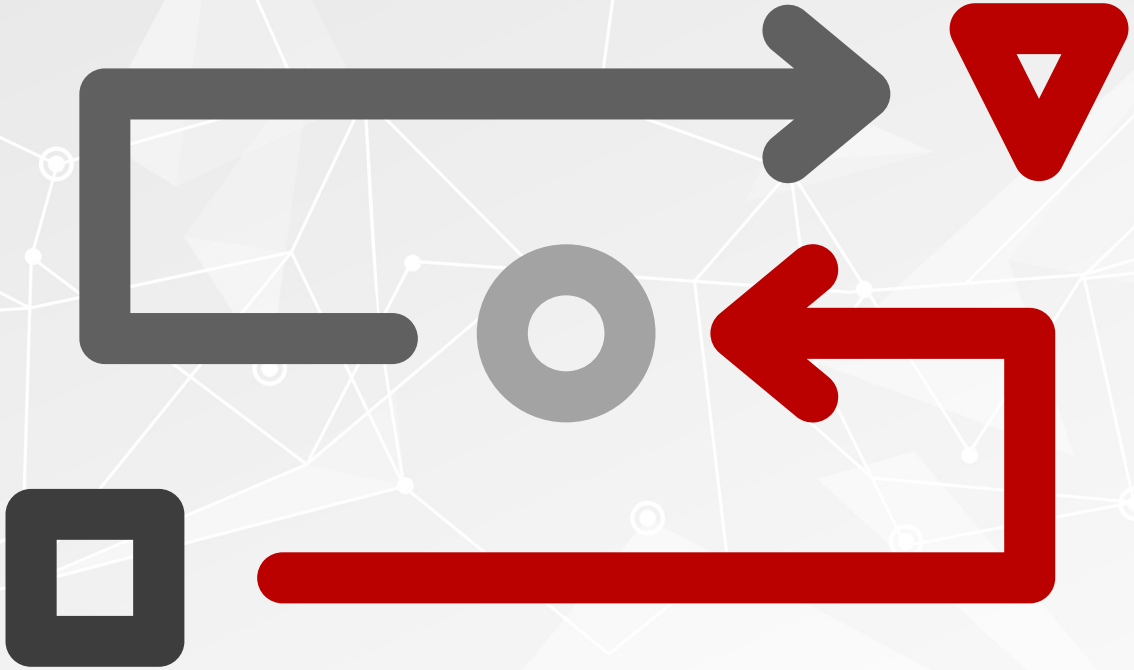


Public Blob Storage Accounts



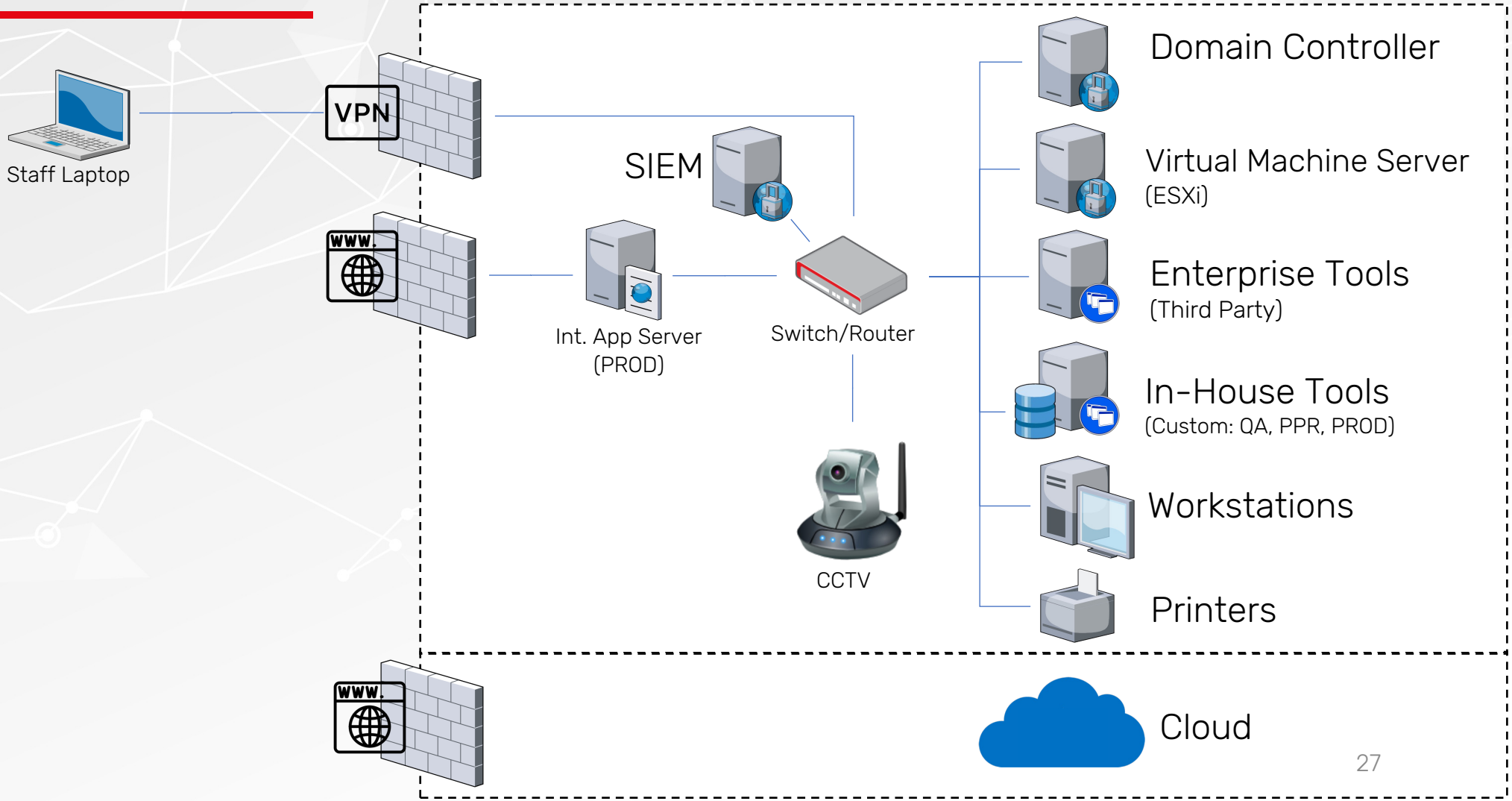
Public Blob Storage Accounts



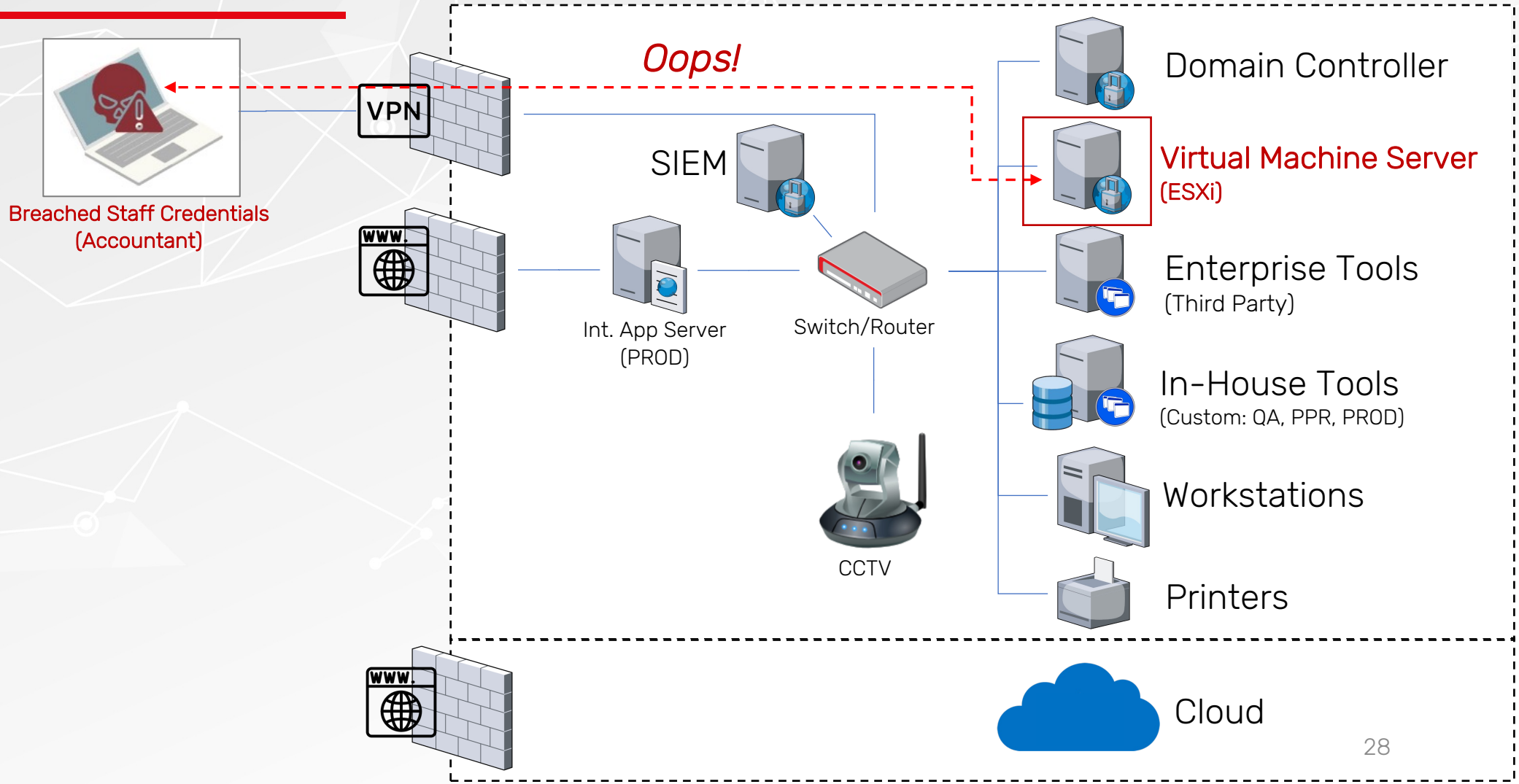


Internal Security

Lack of Network Segregation

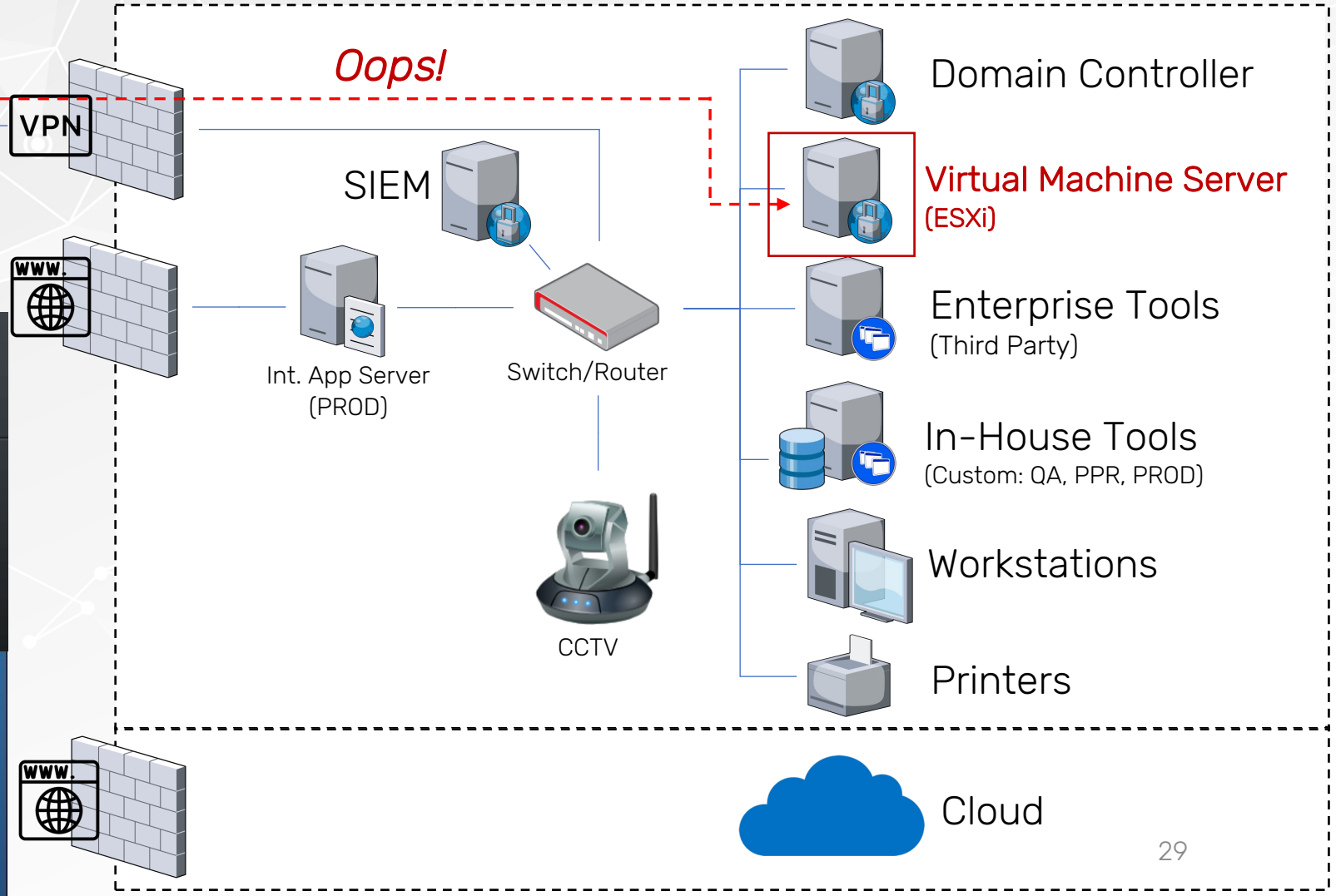


Lack of Network Segregation

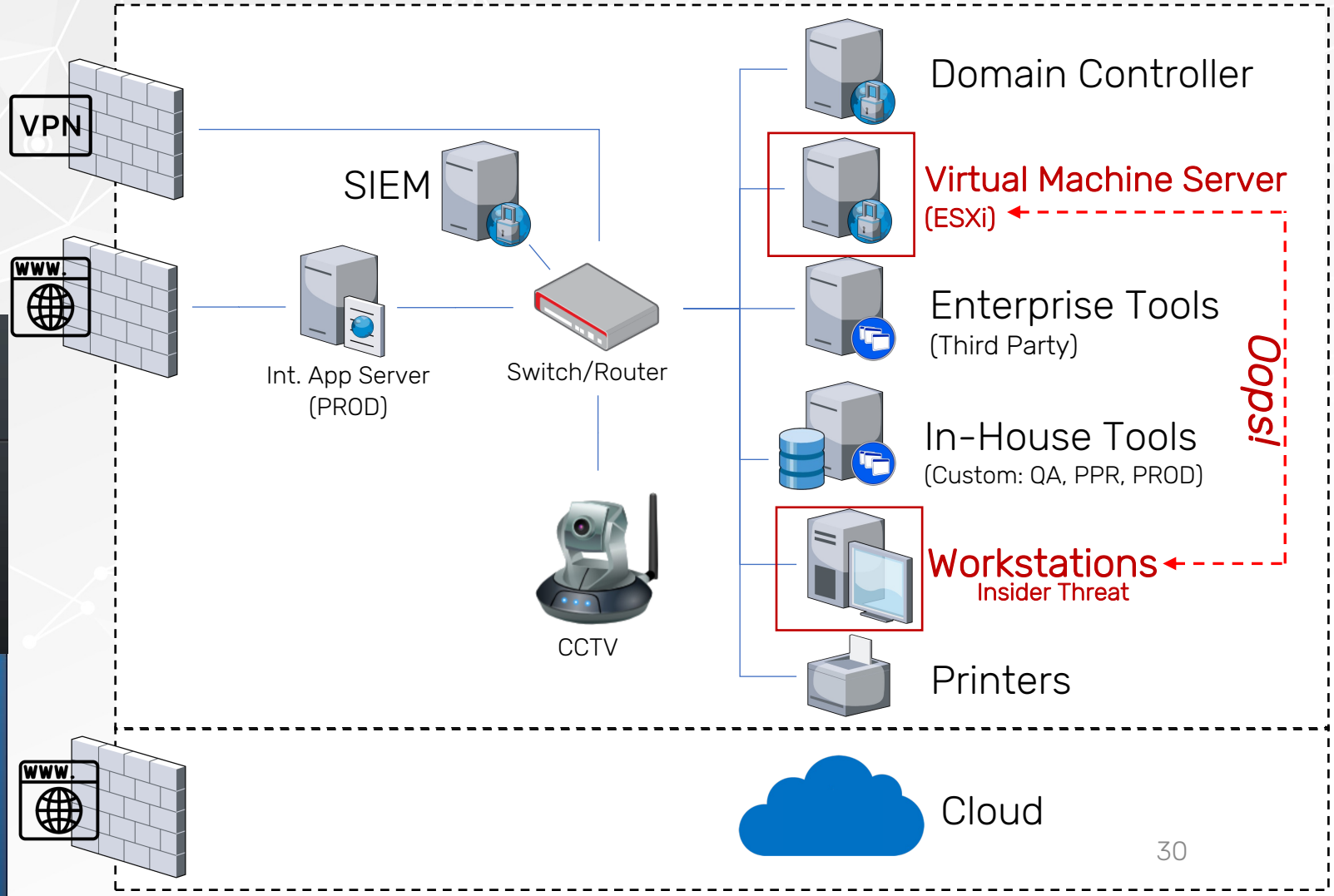


Lack of Network Segregation

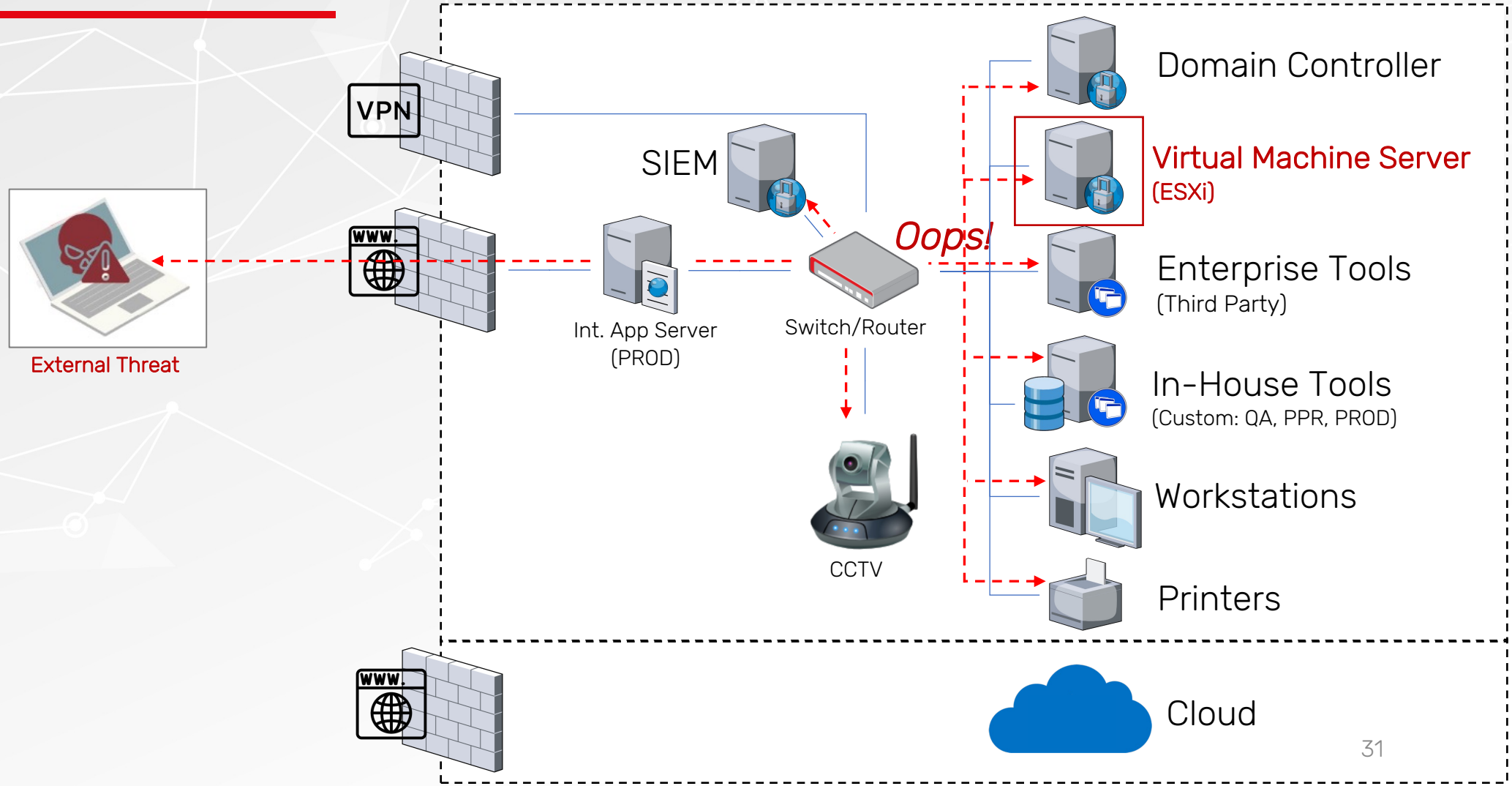
Breached Staff Credentials
(Accountant)



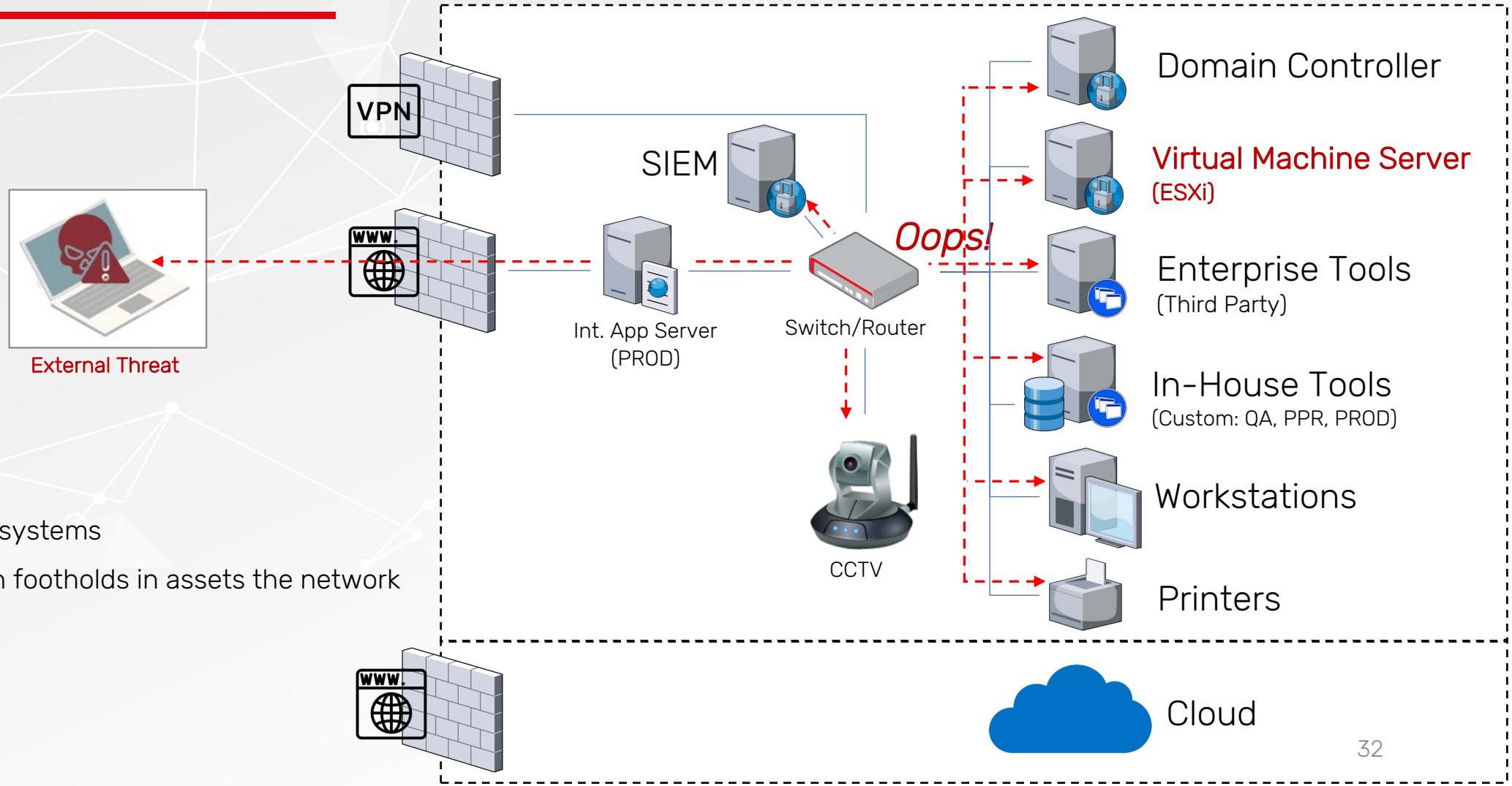
Lack of Network Segregation



Lack of Network Segregation

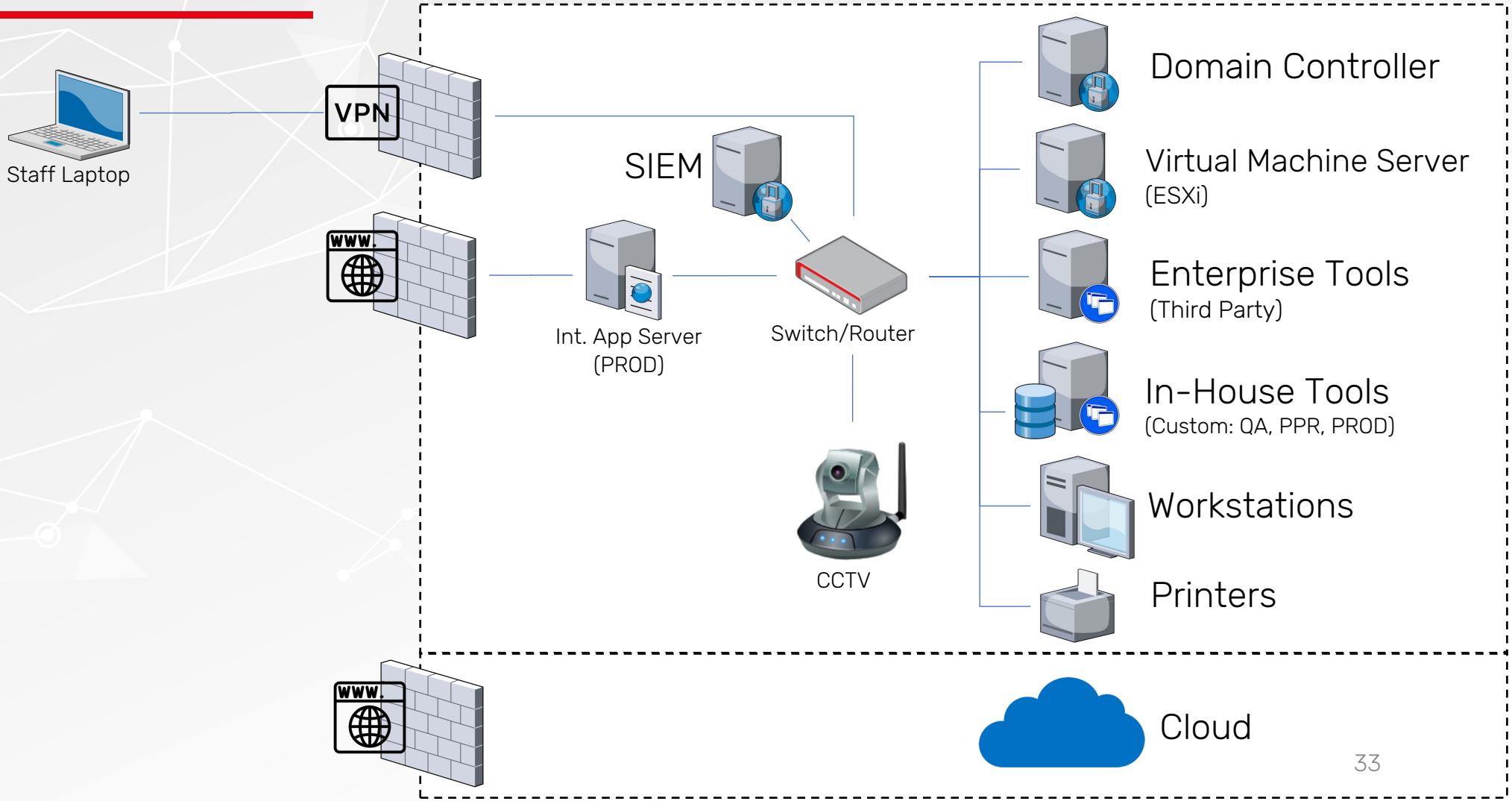


Lack of Network Segregation

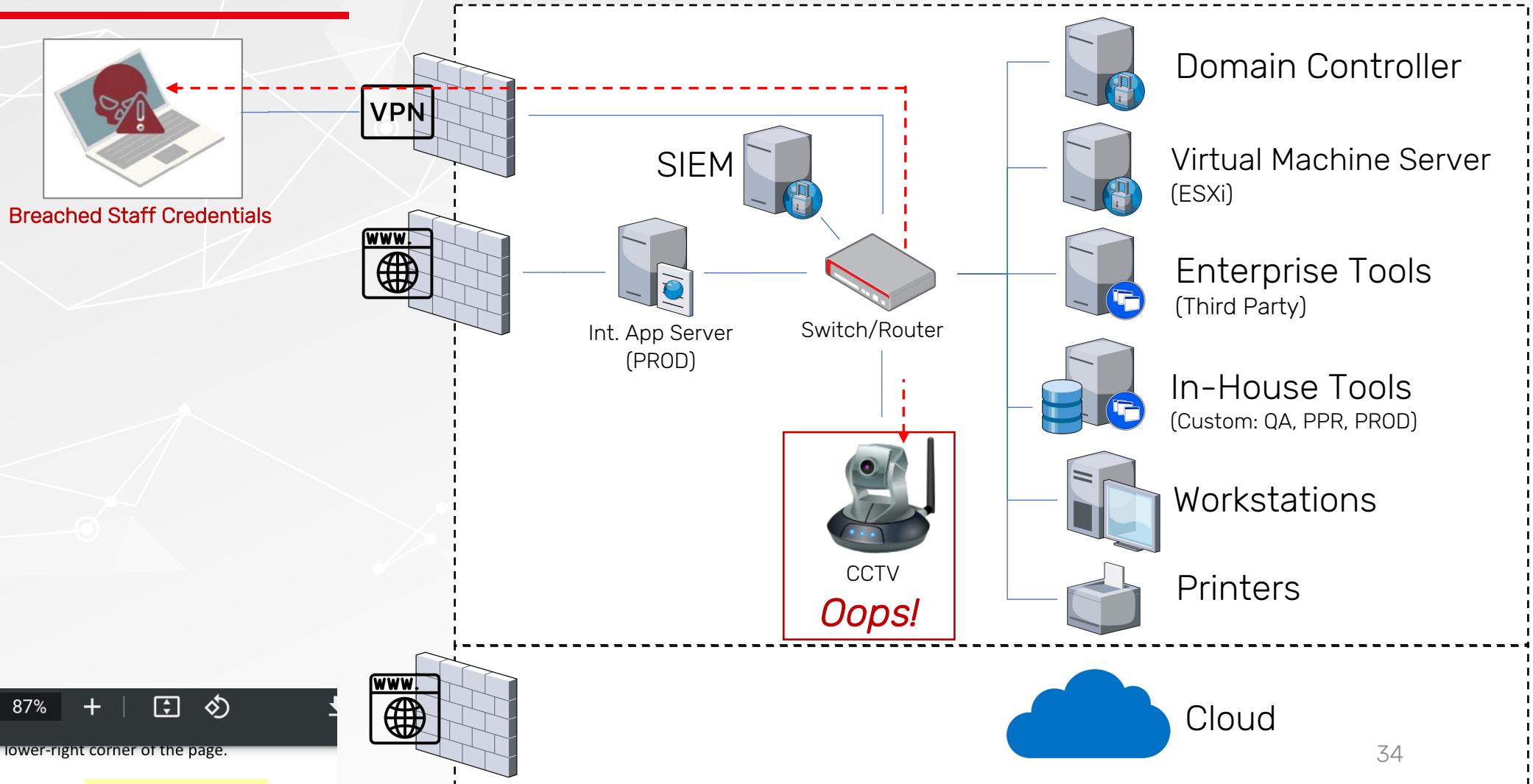


- Wide attack surface
- Ability to pivot to other systems
- Opportunity to establish footholds in assets the network

Default Credentials or Weak Passwords



Default Credentials or Weak Passwords

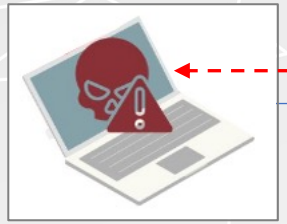


Vision_... 6 / 11 87%

- Click **Web Service Configuration** in the lower-right corner of the page.

Note: The default username is `admin` and the default password is `admin256`. To prevei

Default Credentials or Weak Passwords



Breached Staff Credentials

VPN

SIEM

Int. App Server
(PROD)

Switch/Router
Oops!

CCTV
Oops!

Domain Controller

Virtual Machine Server
(ESXi)

Enterprise Tools
(Third Party)

In-House Tools
(Custom: QA, PPR, PROD)
Oops!

Workstations

Printers
Oops!

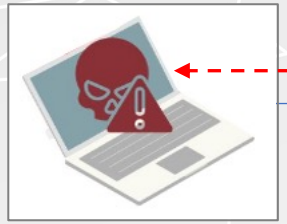
Cloud

Vision_... 6 / 11 87%

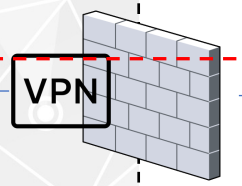
- Click **Web Service Configuration** in the lower-right corner of the page.

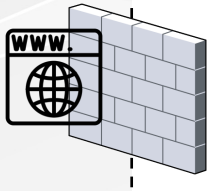
Note: The default username is `admin` and the default password is `admin256`. To prevei

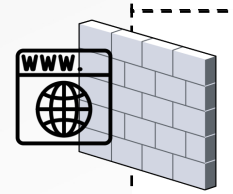
Default Credentials or Weak Passwords

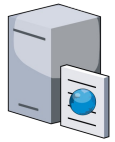


Breached Staff Credentials

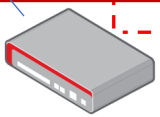








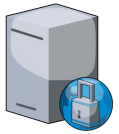
Int. App Server
(PROD)



Switch/Router
Oops!

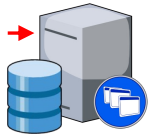
CCTV
Oops!

Domain Controller

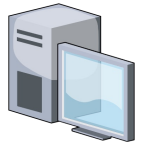


Virtual Machine Server
(ESXi)

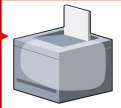
Enterprise Tools
(Third Party)



In-House Tools
(Custom: QA, PPR, PROD)
Oops!



Workstations



Printers
Oops!

Cloud

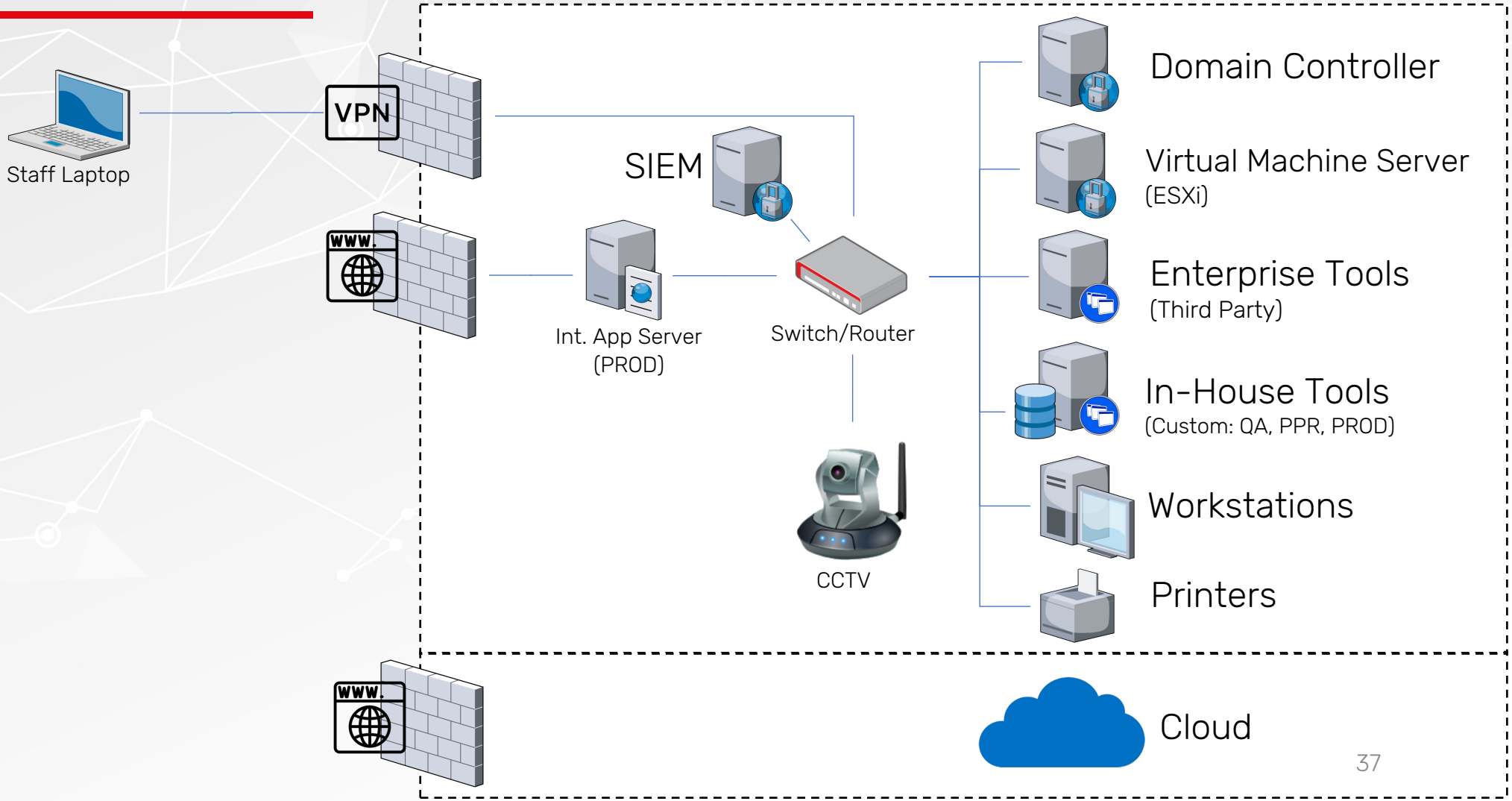
- Ability to change firmware?
- Enable other services?
- Perform further reconnaissance?
  (example: print history logs – doc. name, usernames)
- Does “admin:admin” work?
- Can passwords be found in admin guides?

Vision_... 6 / 11 87%

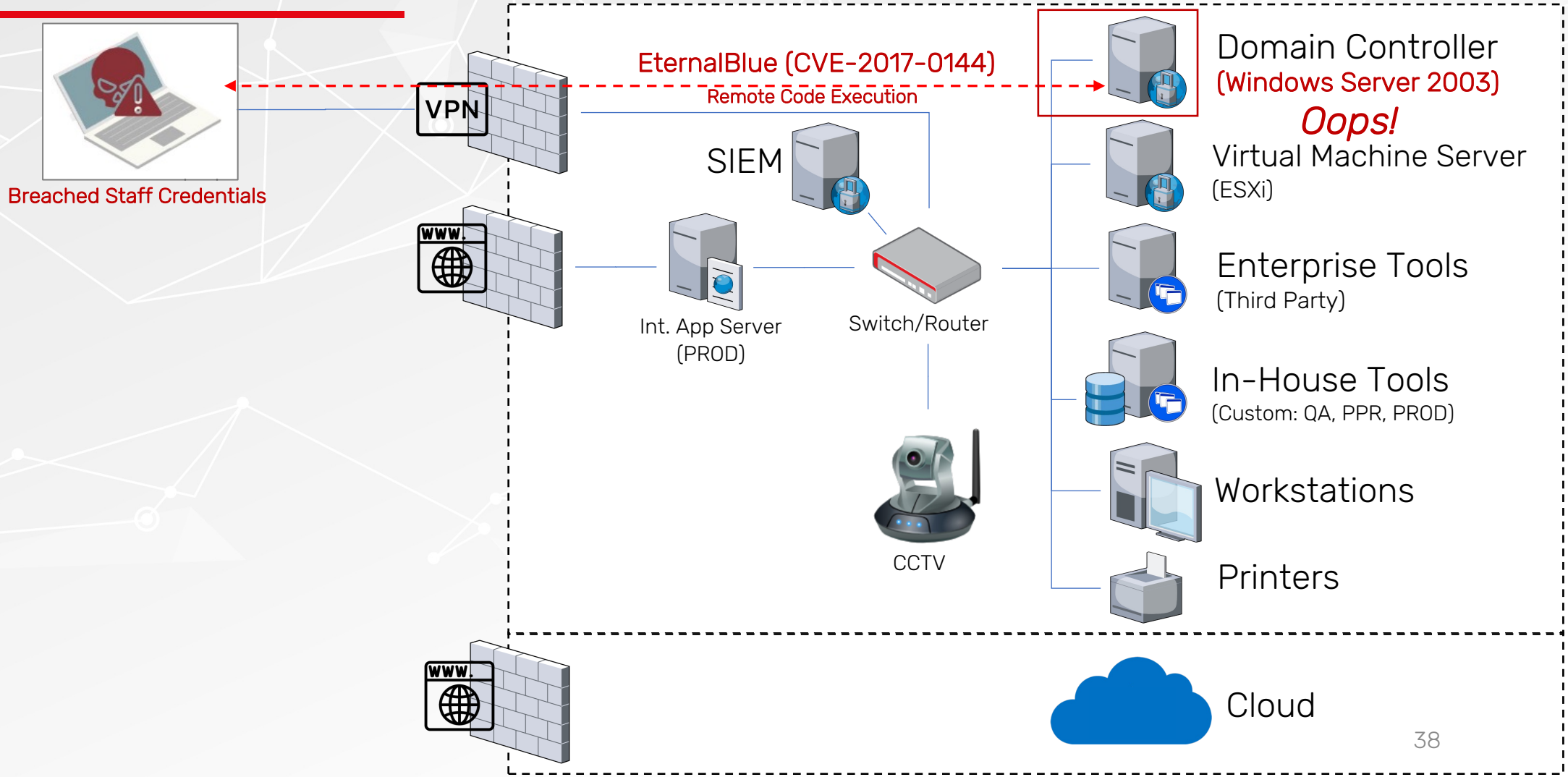
- Click **Web Service Configuration** in the lower-right corner of the page.

Note: The default username is `admin` and the default password is `admin256`. To prevei

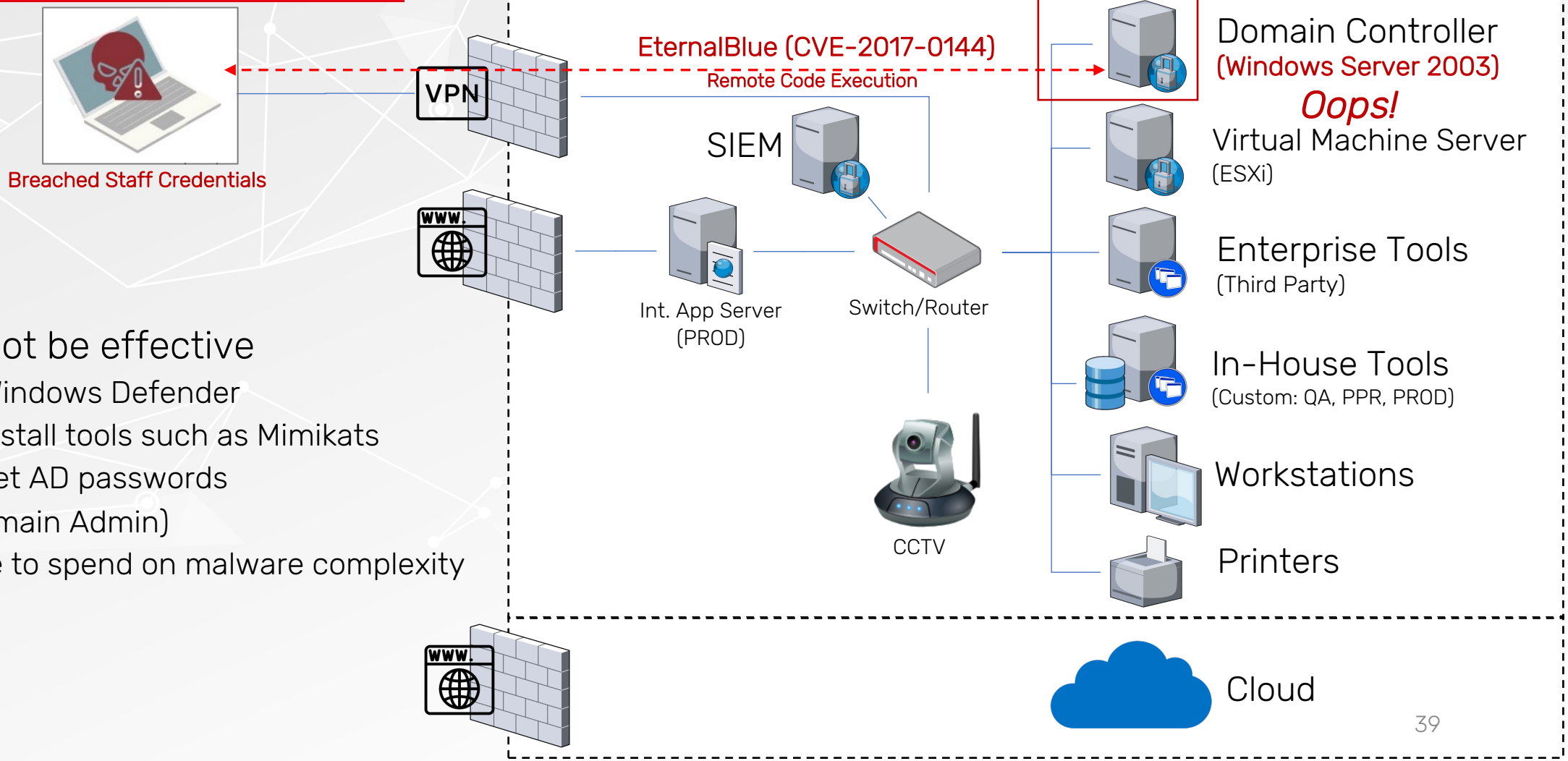
Operating System(s) No Longer Supported



Operating System(s) No Longer Supported



Operating System(s) No Longer Supported



EDRs might not be effective

- Lack of Windows Defender
- Able to install tools such as Mimikats
- Able to get AD passwords
  (i.e, Domain Admin)
- Less time to spend on malware complexity

Permissive Outbound Network Access

Breached Staff Credentials

VPN

SIEM

Int. App Server
(PROD)

Switch/Router

Domain Controller
(Windows Server 2003)

Oops!

Virtual Machine Server
(ESXi)

Enterprise Tools
(Third Party Applications)

In-House Tools
(Custom: QA, PPR, PROD)

Workstations

Printers

Outbound traffic
to internet

Oops!

CCTV

Cloud

Attacker Command-&-Control Infrastructure

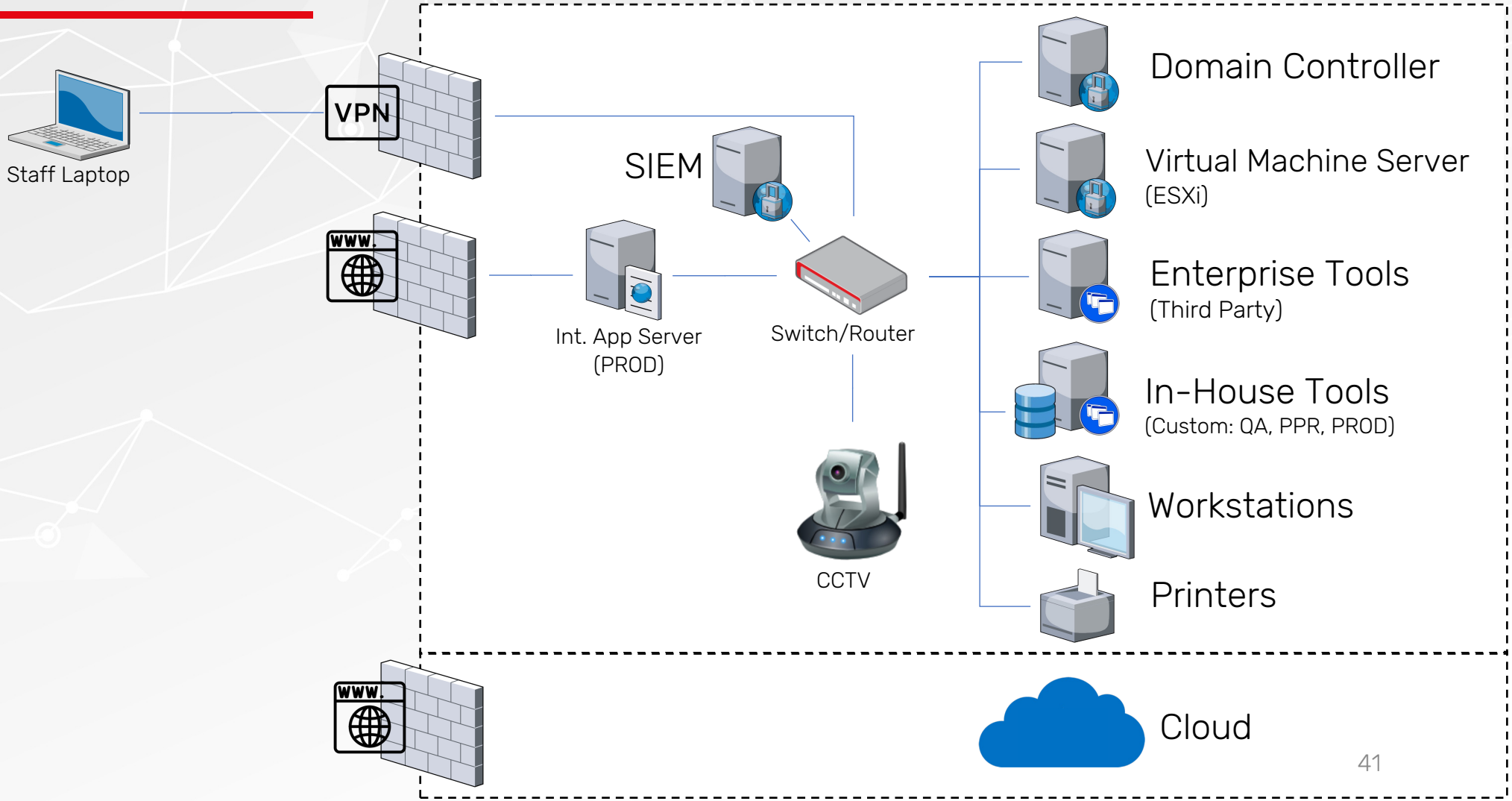
Redirector

Command-&-control
C2 Server

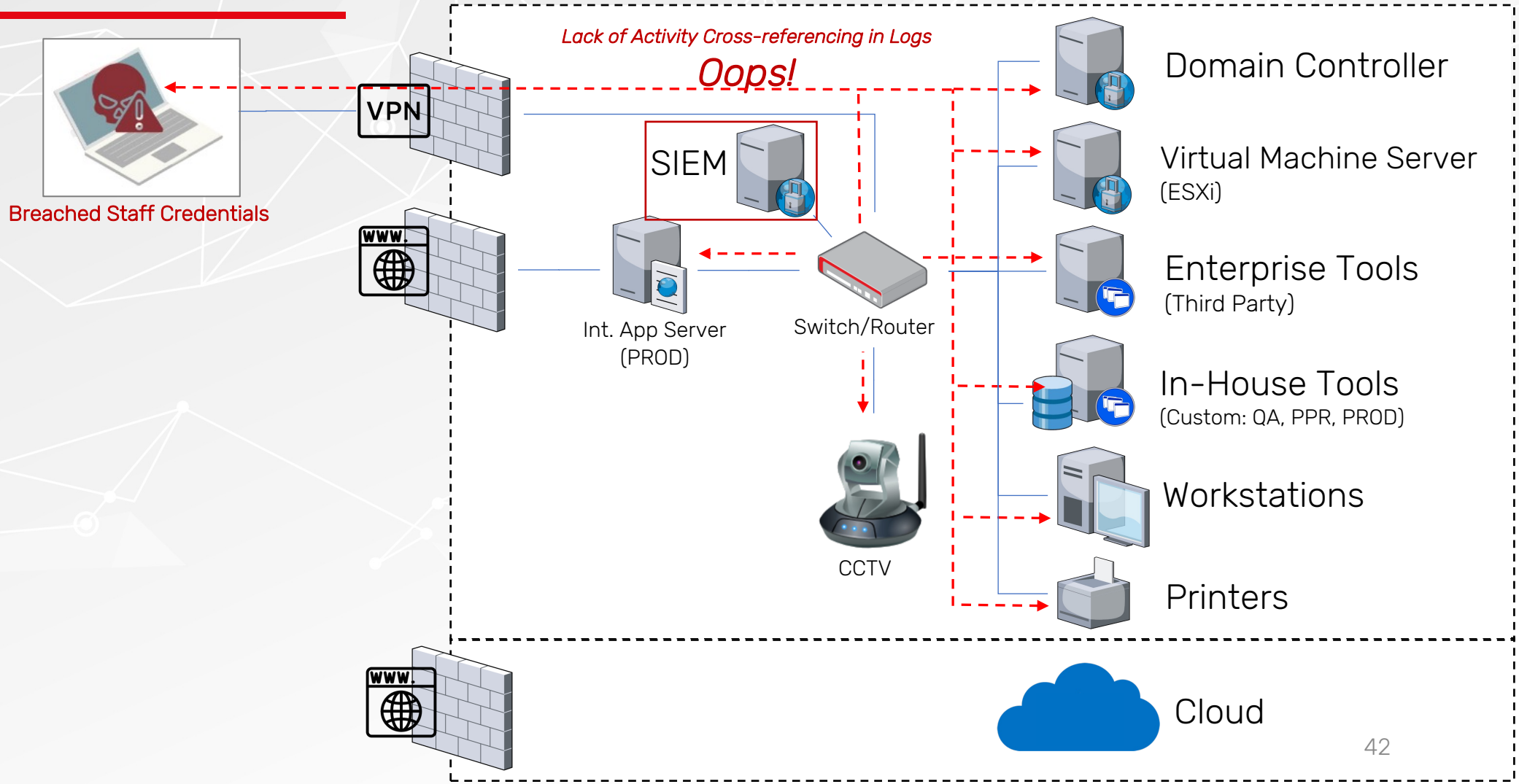
Attacker
Domains

- legittransport.com
- legitfinance.com

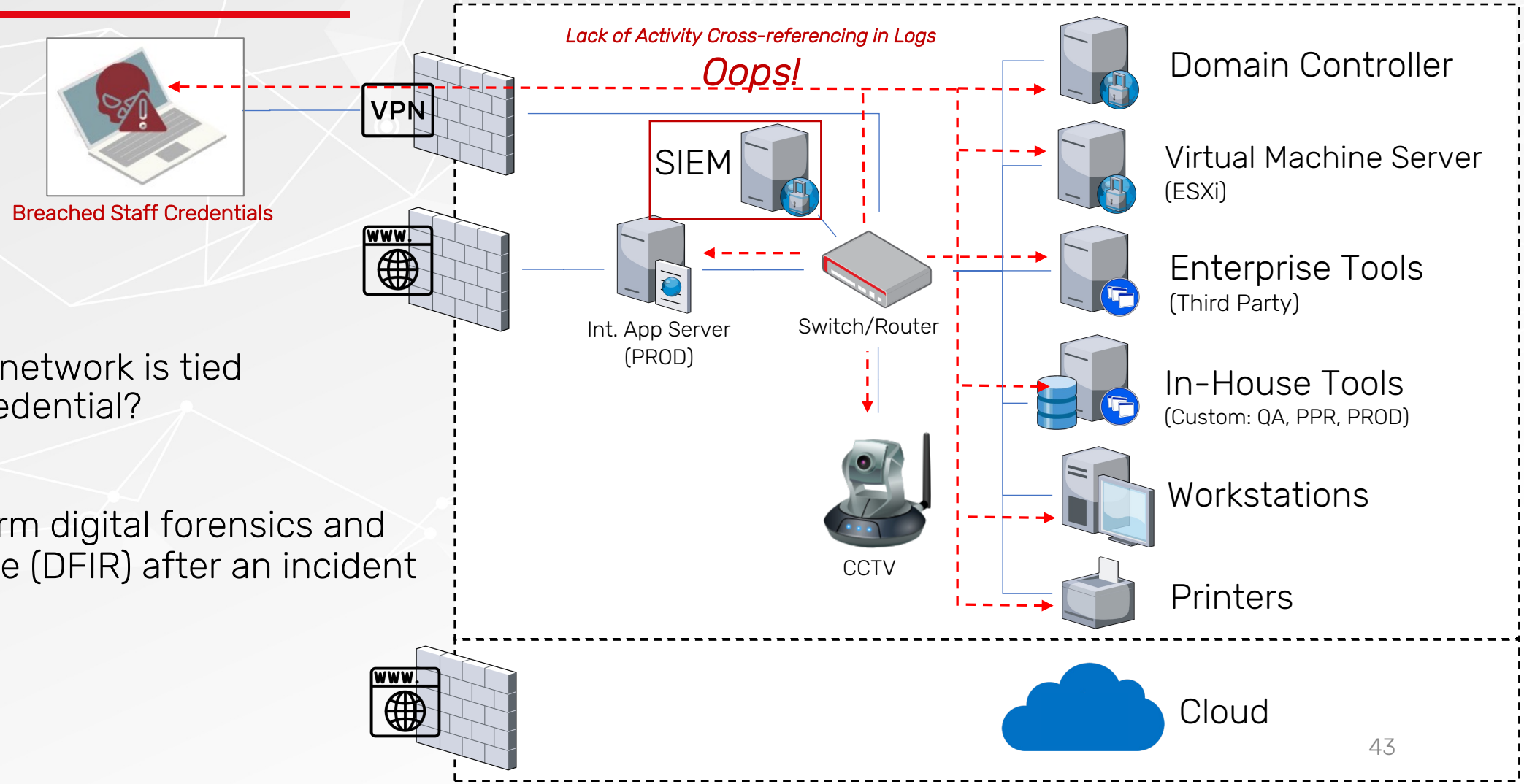
Lack of Adequate Logging



Lack of Adequate Logging

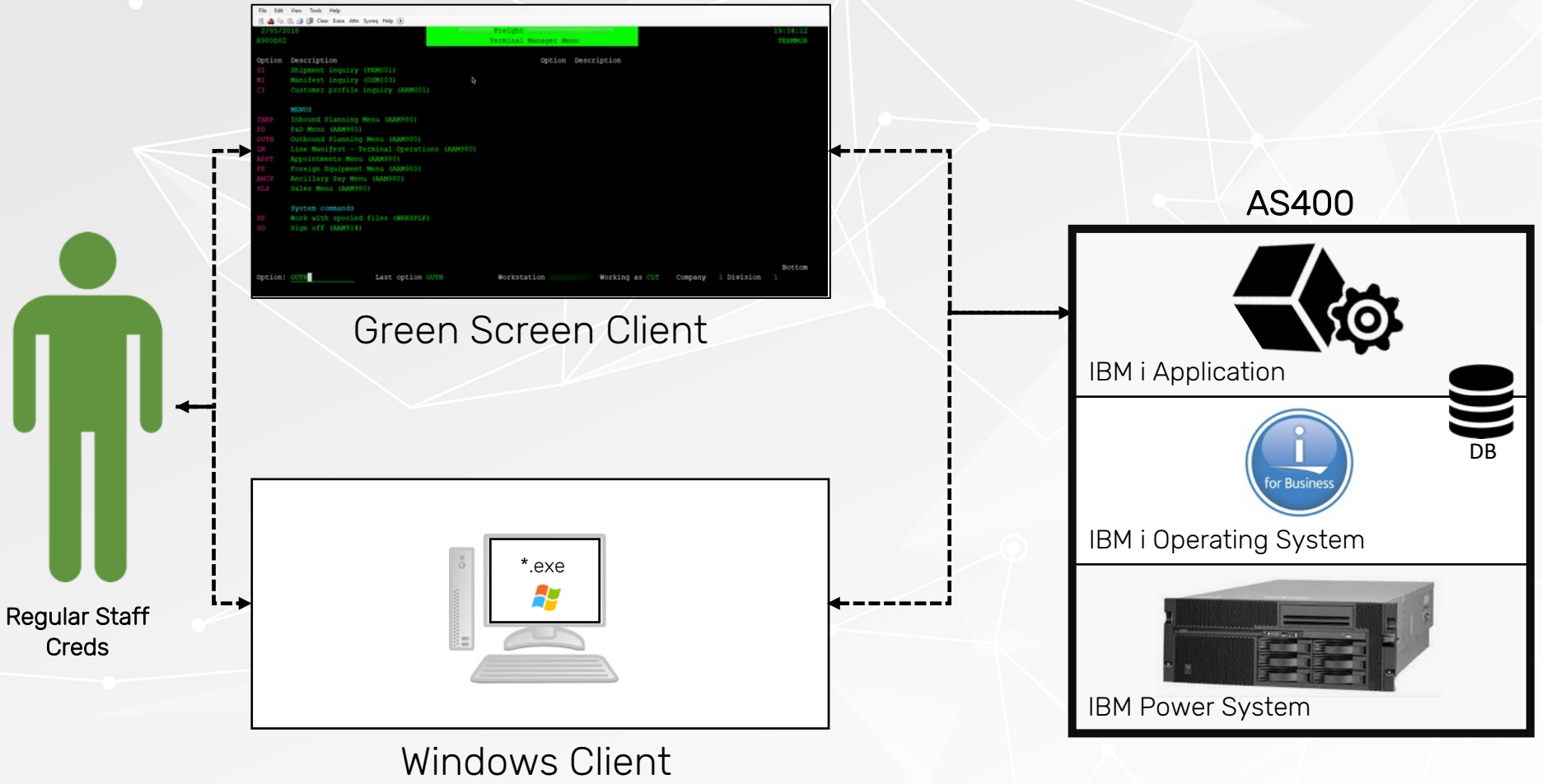


Lack of Adequate Logging

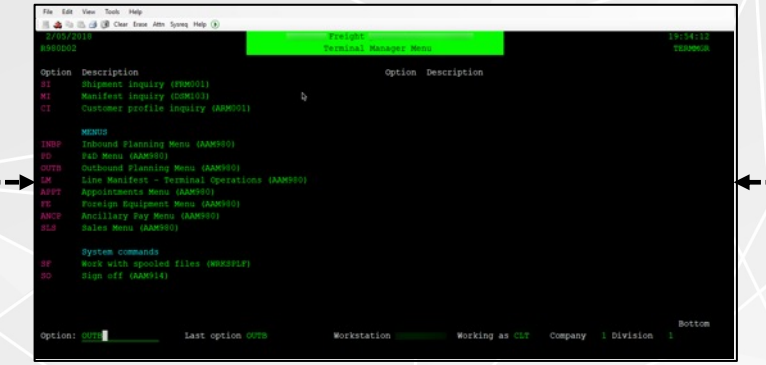


- Which attack on network is tied to which VPN credential?
- Difficult to perform digital forensics and incident response (DFIR) after an incident

Excessive Open Ports



Excessive Open Ports



Green Screen Client

AS400

IBM i Application

DB

IBM i Operating System

IBM Power System

QSECOFR

Administrator

Breached Staff Creds

*.exe

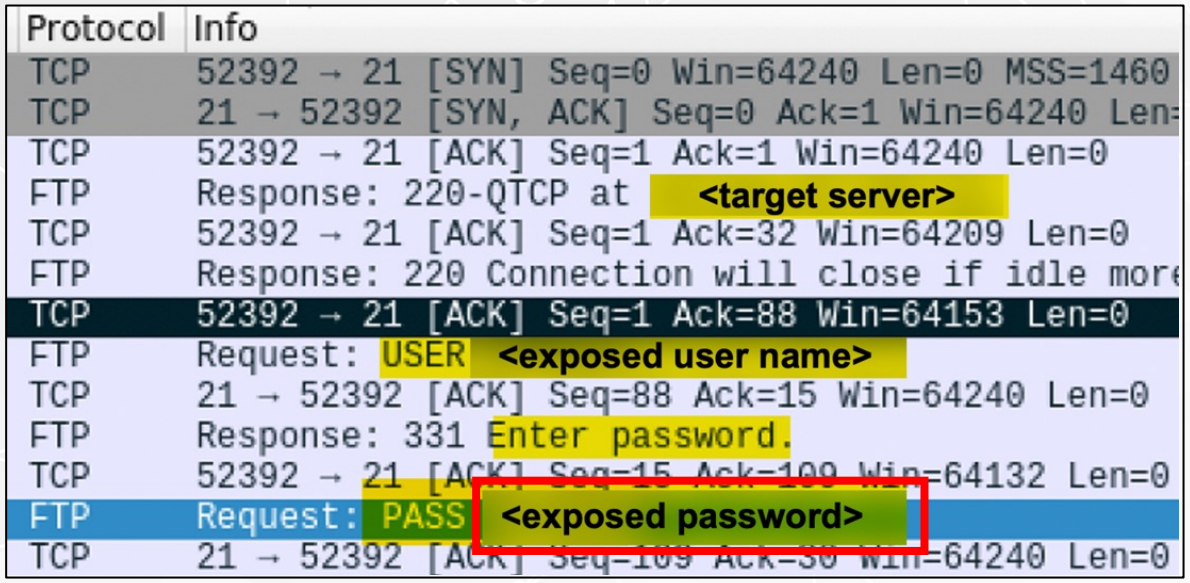
Windows Client

Oops!

(ssh, db, ftp, admin portal ext..)

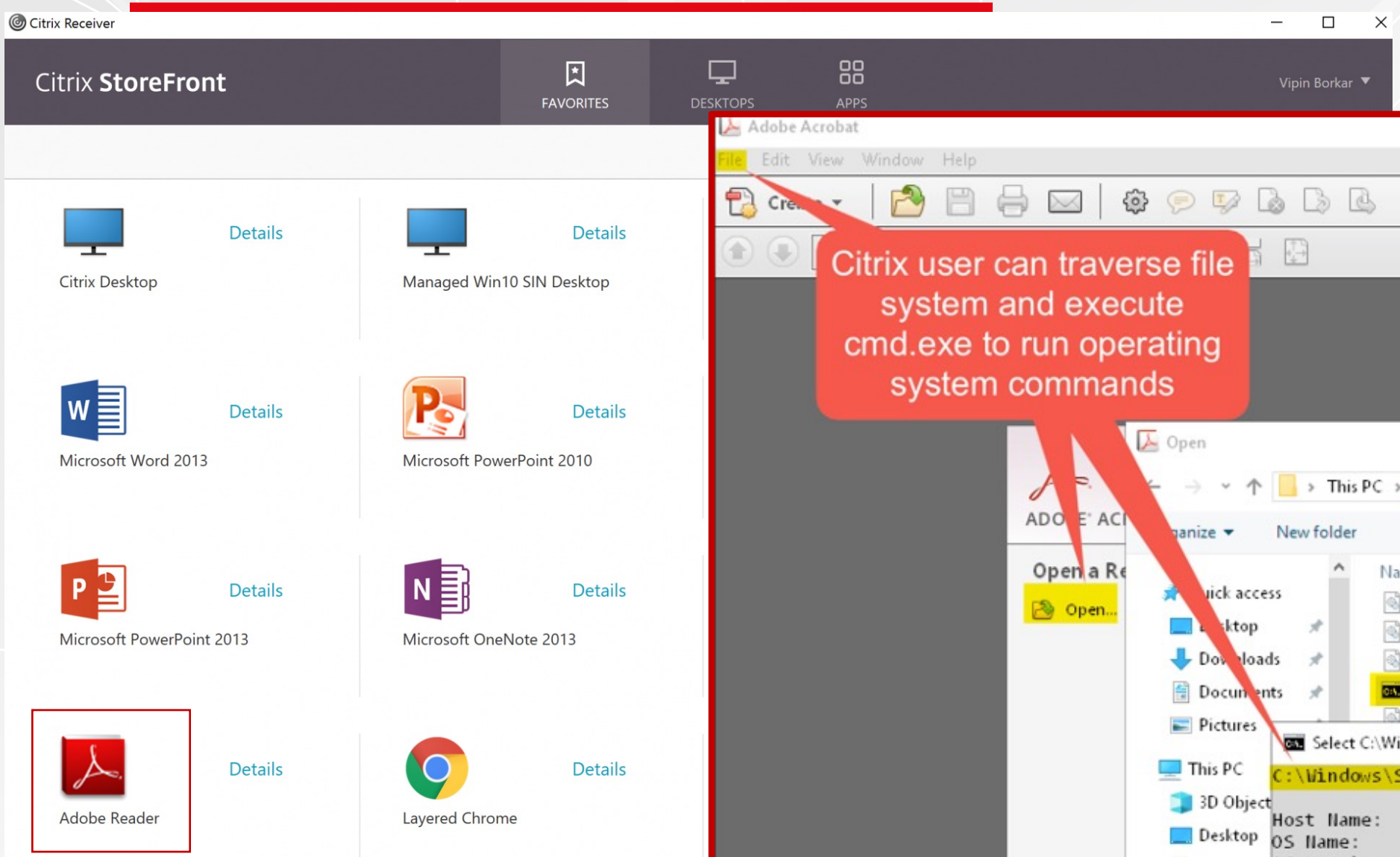
Insecure Data in Transit

- Use of Insecure Protocols
  - Using HTTP (80) instead of HTTPS (443)
    - HTTP: `<IP>:2004/ibm/console/logon.jsp`
  - FTP : `Port 21`



  - Telnet (TN5250, TN3270): `Port 23`

Citrix Breakout

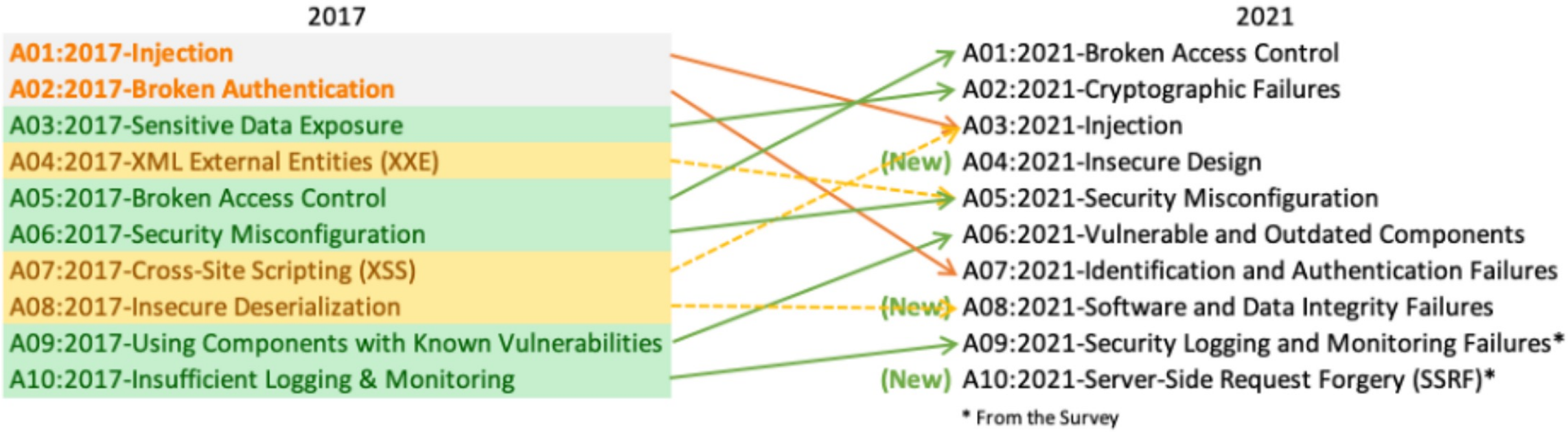


Common Issues With In-house Tools

owasp.org/www-project-top-ten/

Top 10 Web Application Security Risks

There are three new categories, four categories with naming and scoping changes, and some consolidation in the Top 10 for 2021.



Common Issues With In-house Tools

- Broken Access Control – Example HTTP Request

Request

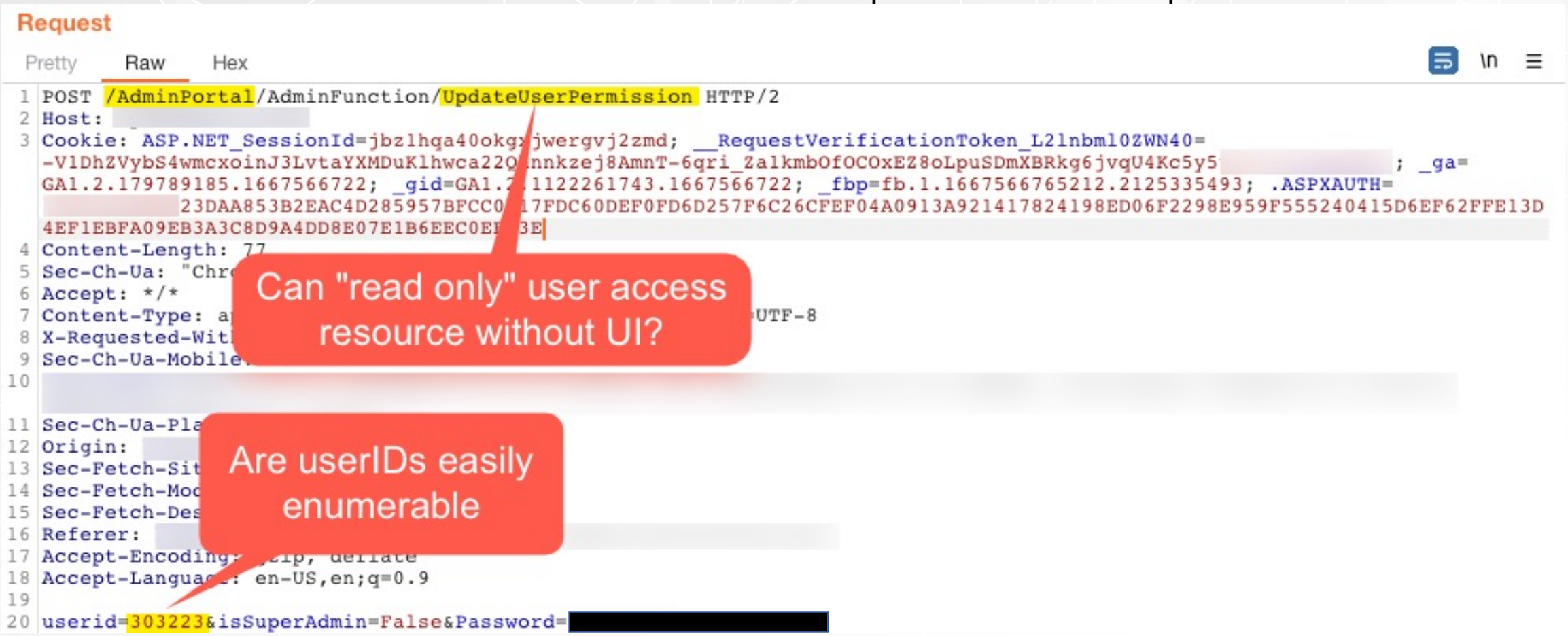
Pretty Raw Hex

```
1  POST /AdminPortal/AdminFunction/UpdateUserPermission HTTP/2
2  Host:
3  Cookie: ASP.NET_SessionId=jbzlhqa40okgxjwergvj2zmd; __RequestVerificationToken_L2lnbml0ZWN40=
   -V1DhZVybS4wmcxoinJ3LvtaYXMDuKlhwca22Q_nnkzej8AmnT-6qri_Za1kmbOfOCOxEZ8oLpuSDmXBRkg6jvqU4Kc5y5                ; _ga=
   GA1.2.179789185.1667566722; _gid=GA1.2.1122261743.1667566722; _fbp=fb.1.1667566765212.2125335493; .ASPXAUTH=
   23DAA853B2EAC4D285957BFCC0 17FDC60DEF0FD6D257F6C26CFEF04A0913A921417824198ED06F2298E959F555240415D6EF62FFE13D
   4EF1EBFA09EB3A3C8D9A4DD8E07E1B6EEC0E 3E
4  Content-Length: 77
5  Sec-Ch-Ua: "Chr
6  Accept: */*
7  Content-Type: a                                                    UTF-8
8  X-Requested-Wit
9  Sec-Ch-Ua-Mobile
10
11 Sec-Ch-Ua-Platform: "macOS"
12 Origin:
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer:
17 Accept-Encoding: gzip, deflate
18 Accept-Language: en-US,en;q=0.9
19
20 userid=303223&isSuperAdmin=False&Password=[redacted]
```

Can "read only" user access resource without UI?

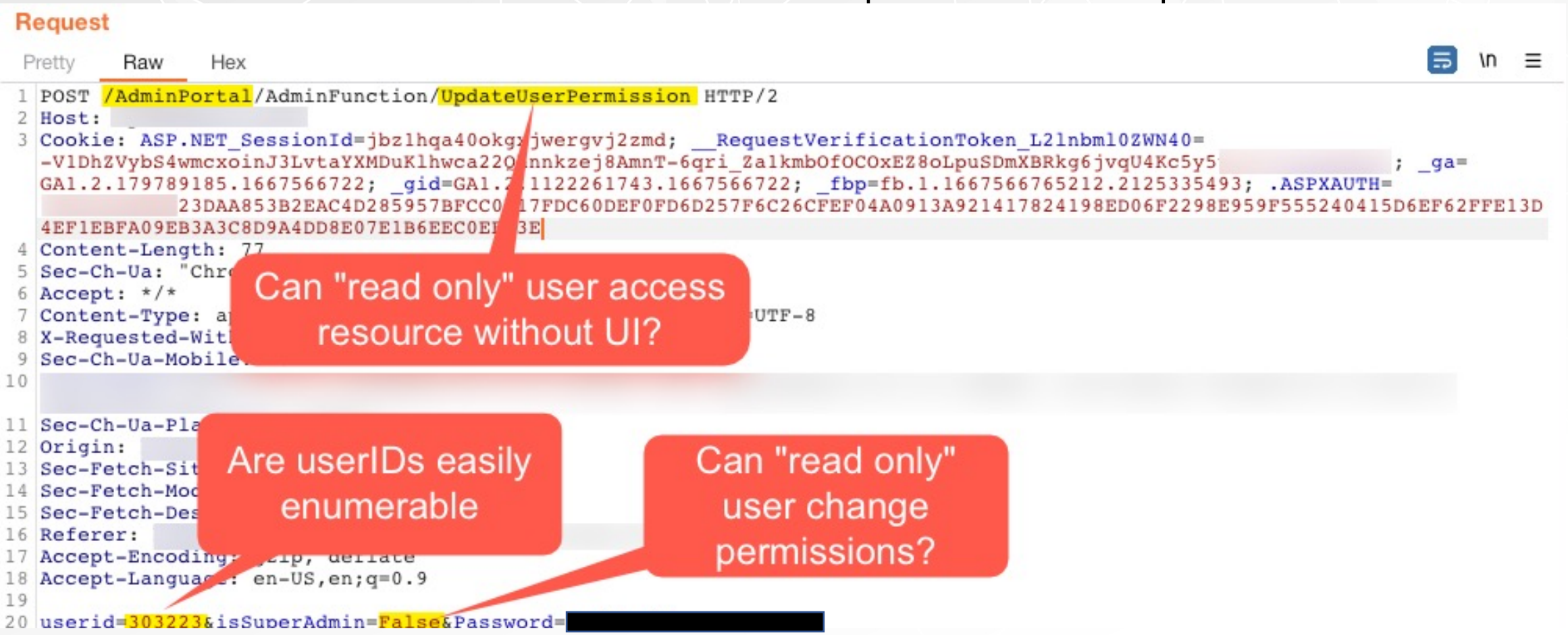
Common Issues With In-house Tools

- Broken Access Control – Example HTTP Request



Common Issues With In-house Tools

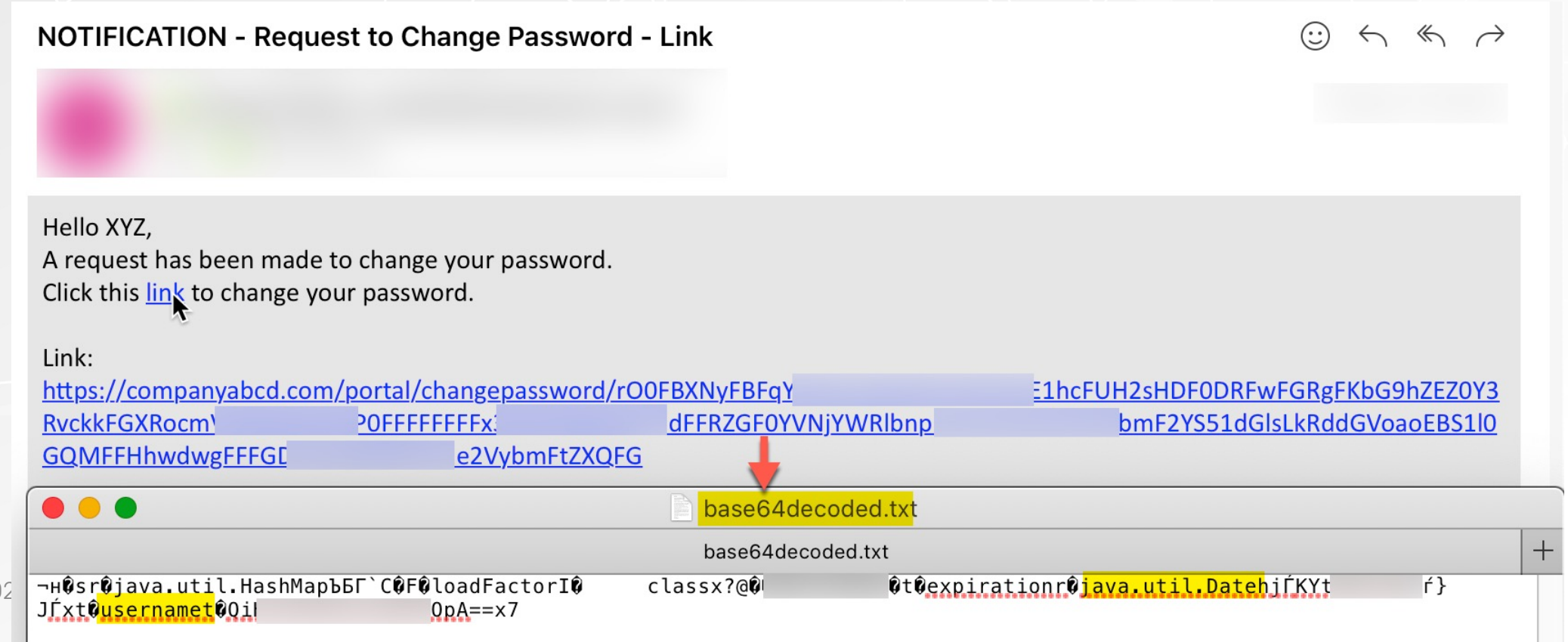
- Broken Access Control – Example HTTP Request



Common Issues With In-house Tools

Poor Software Design

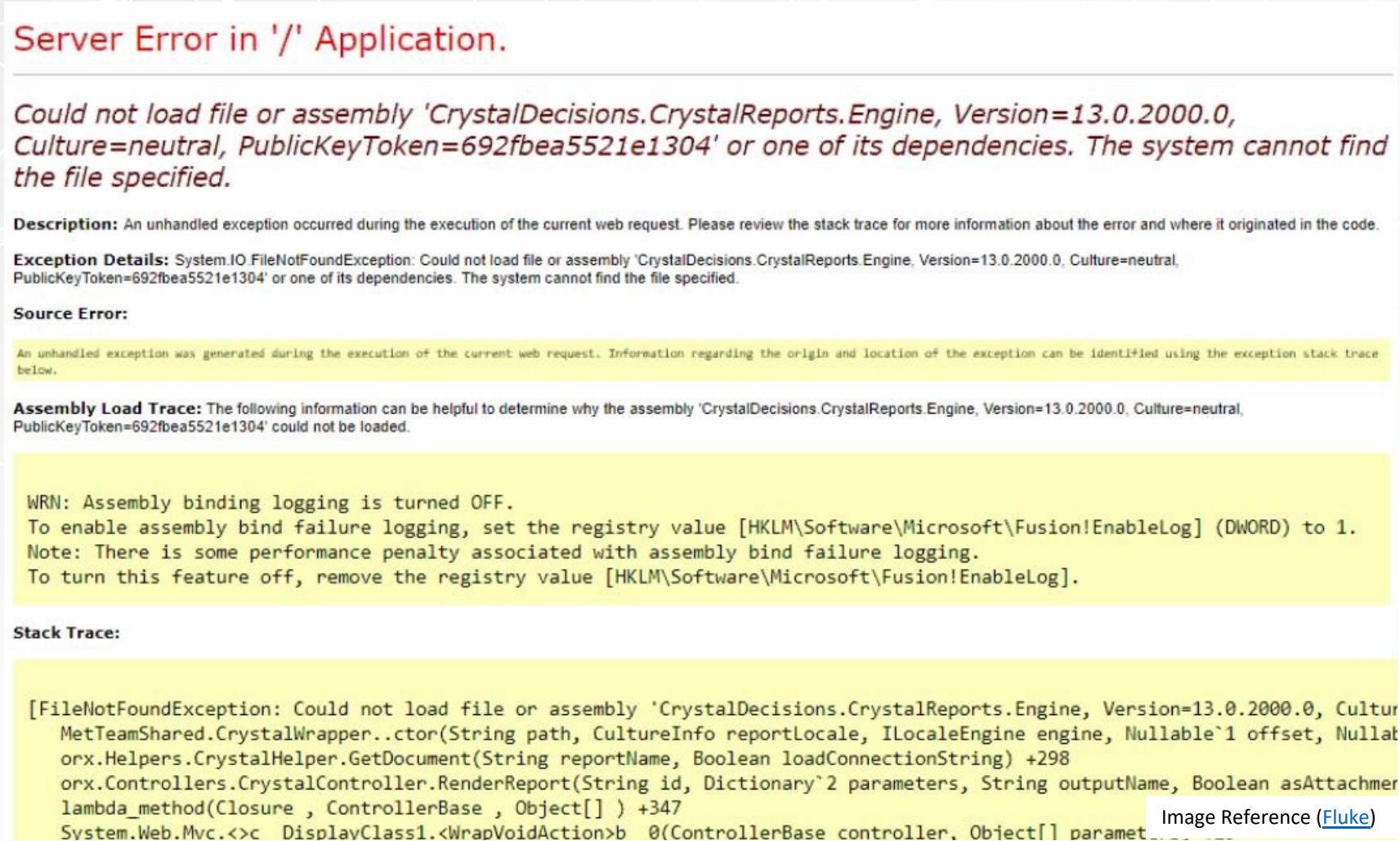
- Example: Object Deserialization Vulnerability (Password Reset Link)



Verbose Errors

Identify technologies used

- Classes
- Libraries
- SQL schemas
- System file paths



Server Error in '/' Application.

Could not load file or assembly 'CrystalDecisions.CrystalReports.Engine, Version=13.0.2000.0, Culture=neutral, PublicKeyToken=692fbea5521e1304' or one of its dependencies. The system cannot find the file specified.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.IO.FileNotFoundException: Could not load file or assembly 'CrystalDecisions.CrystalReports.Engine, Version=13.0.2000.0, Culture=neutral, PublicKeyToken=692fbea5521e1304' or one of its dependencies. The system cannot find the file specified.

Source Error:

An unhandled exception was generated during the execution of the current web request. Information regarding the origin and location of the exception can be identified using the exception stack trace below.

Assembly Load Trace: The following information can be helpful to determine why the assembly 'CrystalDecisions.CrystalReports.Engine, Version=13.0.2000.0, Culture=neutral, PublicKeyToken=692fbea5521e1304' could not be loaded.

```
WRN: Assembly binding logging is turned OFF.
To enable assembly bind failure logging, set the registry value [HKLM\Software\Microsoft\Fusion!EnableLog] (DWORD) to 1.
Note: There is some performance penalty associated with assembly bind failure logging.
To turn this feature off, remove the registry value [HKLM\Software\Microsoft\Fusion!EnableLog].
```

Stack Trace:

```
[FileNotFoundException: Could not load file or assembly 'CrystalDecisions.CrystalReports.Engine, Version=13.0.2000.0, Cultur
   MetTeamShared.CrystalWrapper..ctor(String path, CultureInfo reportLocale, ILocaleEngine engine, Nullable`1 offset, Nullab
   orx.Helpers.CrystalHelper.GetDocument(String reportName, Boolean loadConnectionString) +298
   orx.Controllers.CrystalController.RenderReport(String id, Dictionary`2 parameters, String outputName, Boolean asAttachmen
   lambda_method(Closure , ControllerBase , Object[] ) +347
   System.Web.Mvc.<>c__DisplayClass1.<WrapVoidAction>b__0(ControllerBase controller, Object[] paramet
```

Image Reference (Fluke)

Third Party Applications

- Can attacker easily decompile the binary?
  - JAVA (Example Decompiler: Intellij)
  - . NET (Example Decompiler: dotPeek)

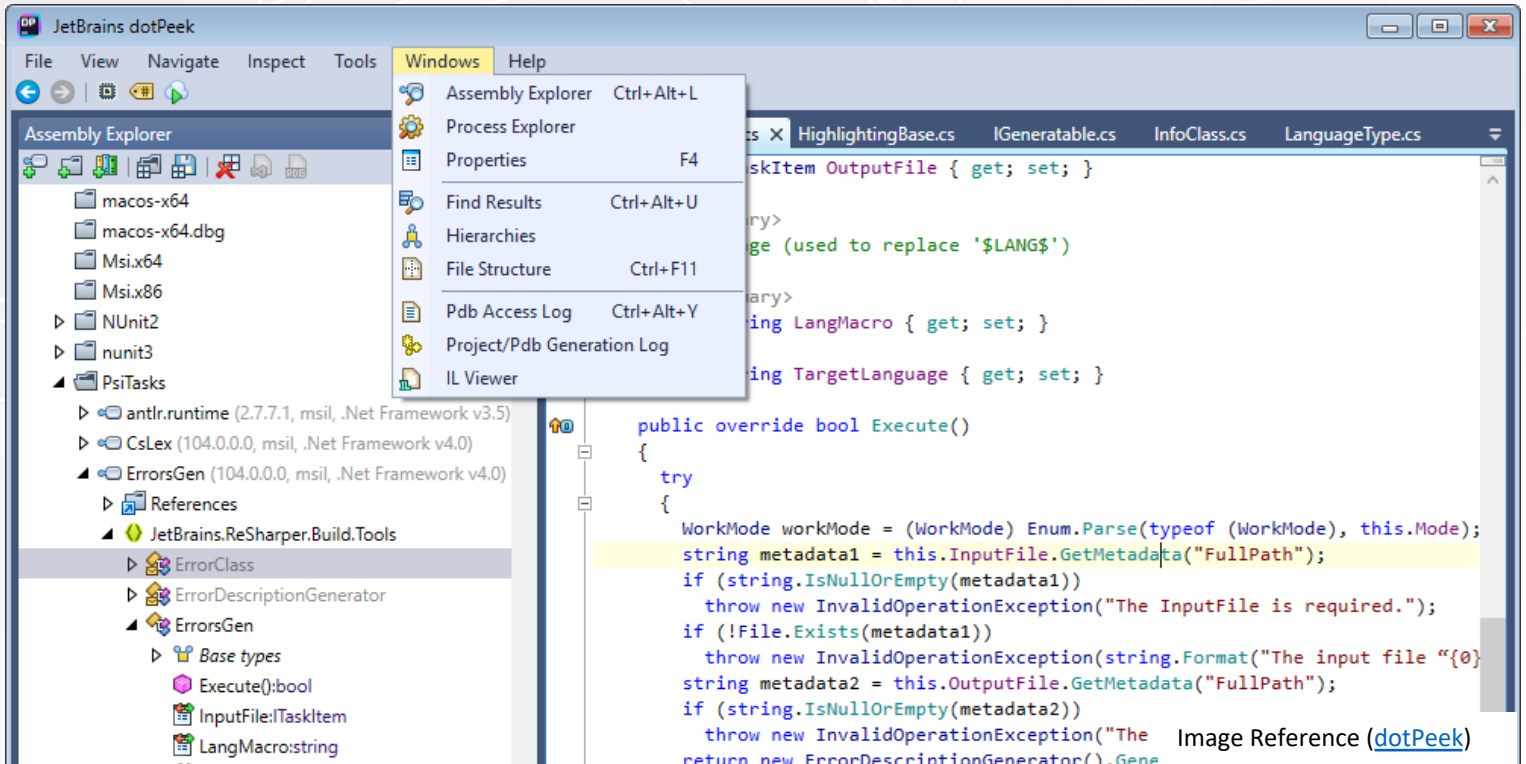
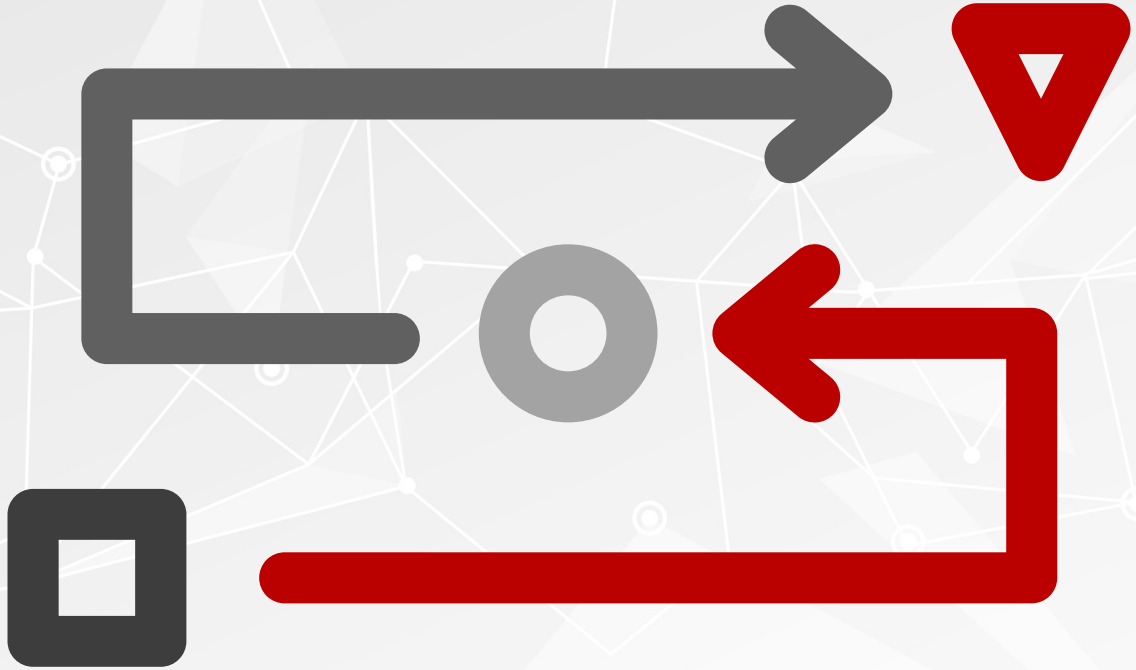


Image Reference (dotPeek)



Organizational Conduct

Permissive Global File Shares

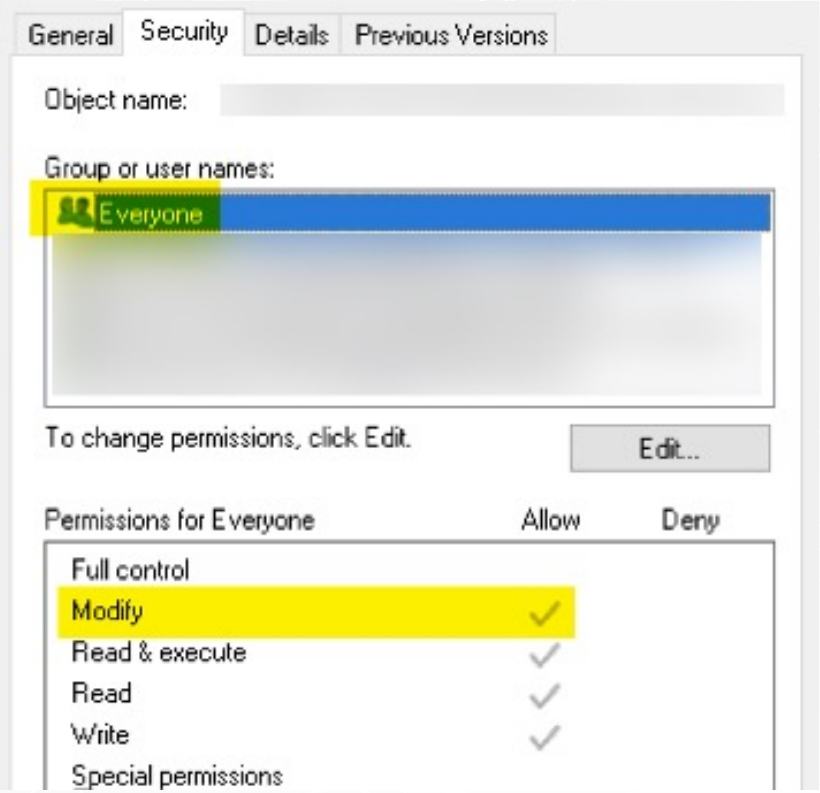
- \\org\globalshare\...

\ITDepartmentTools\
- <directory to put to malware>

\QuarterlyFinancialReports\
- <"CONFIDENTIAL" financial reports>

\Inventory\
- <"CONFIDENTIAL" supply chain information>

\devFolder\
- <Configuration files with passwords and keys>



Opportunity to tamper with file integrity

Password Policy

- Make sure staff don't use usernames or popular passwords

  Example:

  - Nov2022
  - Fall2022
  - Nov22!

```
┌──(                              )-[                                ]
└─# h8mail -t transport.com -sk -lb ./CompilationOfManyBreaches/ --loose | grep "Found" | grep "fall\|summer\|winter\|spring"
[>] Found occurrence [./CompilationOfManyBreaches/data/j/o/g] Line 40877:        @      transport.com:summer01
[>] Found occurrence [./CompilationOfManyBreaches/data/a/m/a] Line 1337588:       @    transport.com.au:summer06
[>] Found occurrence [./CompilationOfManyBreaches/data/b/f] Line 86340:          @
[>] Found occurrence [./CompilationOfManyBreaches/data/r/h] Line 1053906:        @          transport.com:summer
[>] Found occurrence [./CompilationOfManyBreaches/data/h/s] Line 903126:         @
[>] Found occurrence [./CompilationOfManyBreaches/data/h/e/n] Line 1358505:                    @
[>] Found occurrence [./CompilationOfManyBreaches/data/p/symbols] Line 1772328:          @         transport.com:summer140707
[>] Found occurrence [./CompilationOfManyBreaches/data/p/symbols] Line 1772329:          @         transport.com:summerlilly
[>] Found occurrence [./CompilationOfManyBreaches/data/p/a/r] Line 2033285:                  @   transport.com:fall2009
[>] Found occurrence [./CompilationOfManyBreaches/data/m/f] Line 123173:
[>] Found occurrence [./CompilationOfManyBreaches/data/m/h] Line 914043:         @     transport.com:21spring
[>] Found occurrence [./CompilationOfManyBreaches/data/c/v] Line 115713:             @      transport.com:fall2011
[>] Found occurrence [./CompilationOfManyBreaches/data/s/a/n] Line 2694542:                 @        transport.com:summer12
grep: (standard input): binary file matches
```

- Make sure helpdesk provides complex temp. passwords

Incident Response

- Can you get a hold of the CISO on a Sunday at 4AM ET?
- Red Team exercises been performed in the past?
- How fast can your team respond and recover from an attack?

Recommendations

OSINT

- Check what is publicly exposed/leaked that can be leveraged by attackers
- Make sure staff does not expose sensitive details of projects in LinkedIn, Stackoverflow, or Github

Recommendations

External Security / Internal Security

- Enforce MFA
- Prepare a Continuous Vulnerability Assessment (CVA) Program
  - Find vulnerabilities, track trends, Identify rouge assets
- Patch and Update Applications Frequently
- Apply Network Segregation
- Decommission End of Support Assets
- Perform Rigorous Configuration Reviews
- Make Sure Adequate Logging is in Place
- Lookout for “OutputStream”/”InputStream” (deserialization) in code
- Cloud: Review “Security Center”/”Security Hub” Reports

Recommendations

Organization Conduct

Training

- Discourage Weak Passwords
- Send Developers “OWASP Top 10”
  - Use modern web frameworks
  - i.e., Input/Output filtering (i.e., change “<“ to “&lt”) to prevent <script></script>
- Validate Access Controls
- Discourage using global share folders for sharing sensitive files

Planning

- Prepare Incident Response Plan

Exercises

- Tabletop Exercises
- Red Teaming

Thank You

Ahmed Shah | ashah@redcanari.com

https://www.redcanari.com

E: intel@rc.ai

P: +1-877-RED-TEAM