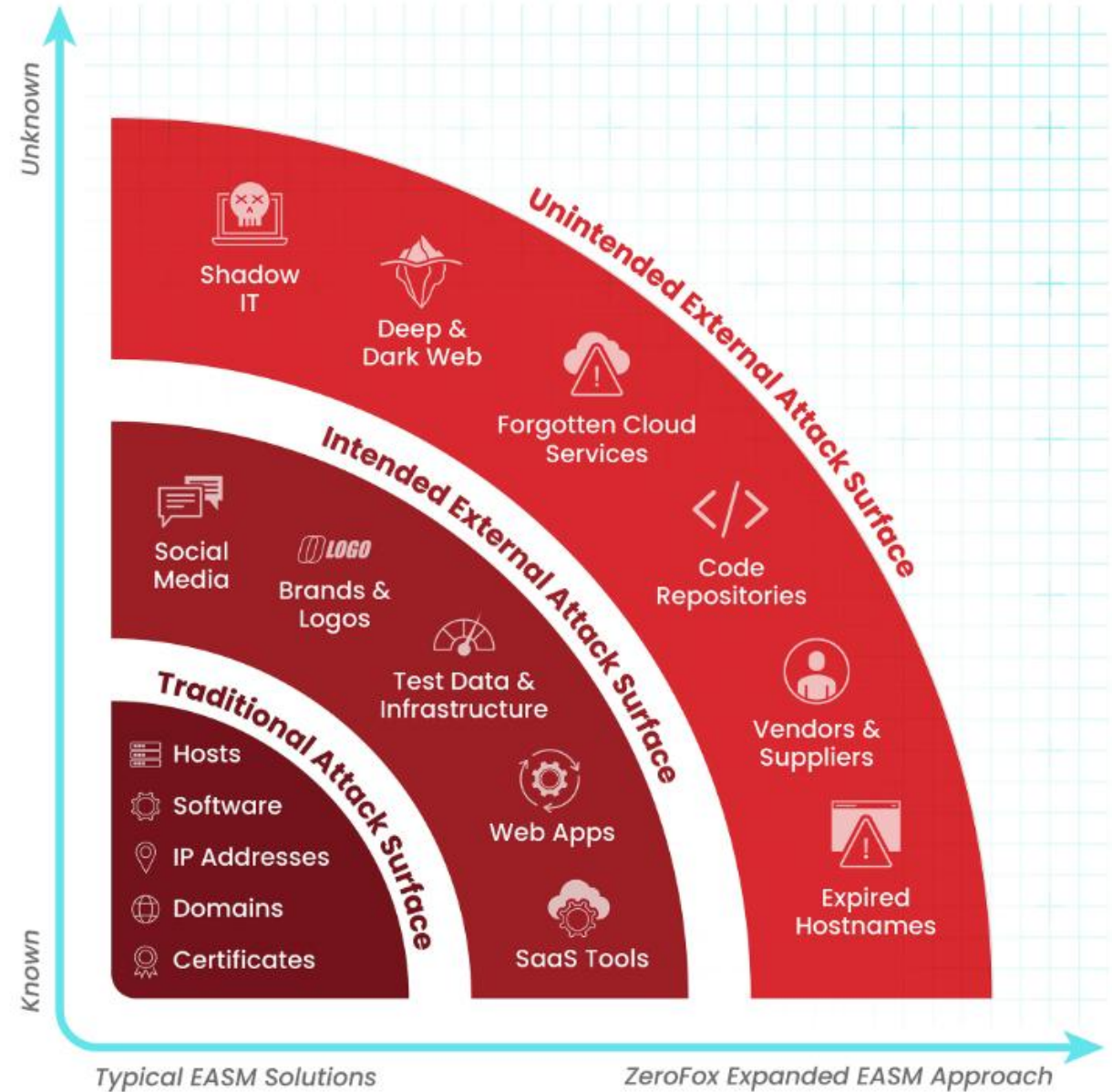


External Attack Surface Management

What can be automated?



Subdomains / Hosts Enumeration

- Gobuster
 - Subfinder
 - Harvester
 - Assetfinder
 - Amass
- `docker run --rm -v $(pwd):/src ghcr.io/oj/gobuster dns -d mydomain.com -w /src/subdomains-top1million-110000.txt -t 30 -q -z --wildcard -o /src/mydomain.com.txt`
 - `docker run --rm projectdiscovery/subfinder -d mydomain.com -silent -all > mydomain.com.txt`
 - `python3 theHarvester.py -d mydomain.com -l 10000 -b all -f mydomain.com.txt`

Emails and usernames search

The screenshot shows the Hunter.io 'Domain Search' interface. The search domain is 'commerzbank.com', which has yielded 1,953 results. The left sidebar contains navigation links: Dashboard, Discover, Finder (highlighted), Verifier, Bulks, Signals, Leads, Campaigns, Integrations, and API. The main results area displays two entries:

- Amir El-Akhras**, Senior Key Account Manager, email: amir.el-akhras@commerzbank.c... (99% confidence, 1 source). Actions: Save as lead, Add to a campaign.
- Zuzana Erdmann**, Project Manager, email: zuzana.erdmann@commerzban... (99% confidence, 1 source). Actions: Save as lead, Add to a campaign.

On the right, there is a 'Follow Commerzbank for updates' notification and a 'Company' section for Commerzbank, described as a banking institution offering retail and commercial services.

- hunter.io
- app.snov.io
- Harvester
- Office docs metadata
- etc.

DEHASHED

14,453,524,169 COMPROMISED ASSETS

[Click Here to View Our Updated Search](#)

FIELD(S) ▾

commerzba

Search for specific fields by adding 'f'

Leaked
credentials

';--have i been pwned?

Check if your email address is in a data breach

pwned?

Using Have I Been Pwned is subject to the [terms of use](#)

Sergey Egorov

OSINT with ScanSuite

The screenshot displays the ScanSuite web interface. On the left is a dark sidebar with navigation links: Scan History, Products, Static Analysis, Dynamic Scanning, Infrastructure Checks (highlighted with a red box), Upload Report, My Rules, Credentials, Vuln DB, and Logout. The main content area is titled 'Infrastructure Checks' and contains several configuration sections. At the top, under 'IPs, hosts or domains', there is a text input field containing 'commerzbank.com,commerzbank.de' (highlighted with a red box). Below this are settings for 'Frequency' (set to 'Once'), 'Date' (with a calendar icon and 'mm/dd/yyyy' placeholder), 'Run or save' (set to 'Run now'), and 'Time' (set to '00:30'). Further down are 'Product / Eng ID' (set to 'Test (3)'), 'Ping hosts' (set to 'No'), and 'Scan ports' (set to 'All TCP'). At the bottom, under 'Select Scan Type', there is a dropdown menu showing 'Domains OSINT' (highlighted with a red box).

- Performs subdomain enumeration using 4 tools, covering the most of available techniques.
- Creates the list of unique subdomains/ assets/ hosts/ potentially webapps.
- For each subdomain checks information from Shodan.
- Forms the list of publicly available emails and possible usernames via Hunter.io.
- Checks for leaked credentials via Dehashed.

Discovery and Vulnerability Scanning

- Scan History
- Products
- Static Analysis
- Dynamic Scanning
- Infrastructure Checks**
- Upload Report

Frequency:

Date:

Run or save:

Time:

Product / Eng ID:

Ping hosts:

Scan ports:

Home / Infrastructure

Infrastructure Scan

Provide the comma or newline separated IPs or domain names

Saved Scans

New



IPs, hosts or domains



xtpadi01.zit.commerzbank.com
xtpadp01.zit.commerzbank.com
zcbredir.commerzbank.de
zertifikate.commerzbank.com
zertifikate.commerzbank.de
zufriedenheit.commerzbank.de
zwischenbericht.commerzbank.de

Select Scan Type

Vulnerability Scan

Choose scanners:

- ☒ OpenVAS
- ☒ Nessus
- ☒ Nuclei
- ☐ Bruteforcer
- ☒ Nuclei (My Rules)
- ☐ Nmap pre-scan

Submit

Feeding subdomains and URLs to web scanners

Scan History

Products

Static Analysis

Dynamic Scanning

Infrastructure Checks

Upload Report

My Rules

Credentials

Vuln DB

Logout

Test Web Scan (5)

cookie1=asd, cookie2=qwe

Custom header (optional)

Authorization: Basic ...

Quick

ZAP base

SSLyze

Dastardly

My Rules

Nuclei custom

Balanced

Arachni

Nuclei

Pro / Licensed

Nessus

Deep / Specialized

Gobuster

ZAP full

ZAP OpenAPI

WordPress

Submit

Password guessing with Bruteforcer

17:45:41 Exported 3 Low, 2 Medium, 0 High and 0 Critical findings

17:45:41 OpenVAS Parser report uploaded.

17:45:42 OpenVAS Scan Finished with status: Done

Credentials confirmed!! {'port': 22, 'service': 'ssh', 'host': '194.67.204.110', 'login': 'sc

All scans completed

Written in Bash and embedded in ScanSuite







Collects leaked credentials and forms wordlists

Uses additional common usernames / passwords
wordlists

Checks over 20 known network services (ftp, ssh, smb, rdp
etc.) using Hydra and Patator

Checks web admin panels (work in progress)

Alerts on credentials match and updates Credentials table

 Infrastructure Checks	 Search credentials 			
 Upload Report				
 My Rules				
 Credentials				
NAME		SECRET	VERIFIED	DETAILS
scanbot		vBTLbXudqcOVmai	True	{'port': 22, 'service

Local Patching Checks

Leverages Vuln.io and OpenVAS scanners

Supports both ssh keys and login/password authentication

Results parsed to XLS and exported to Defect Dojo

- Dynamic Scanning
- Infrastructure Checks**
- Upload Report
- My Rules
- Credentials
- Vuln DB
- Logout

Run now 00:30

Product / Eng ID Ping hosts Scan ports

Test Web Scan (5) No Top 1000 TCP/UDP

Select Scan Type

Local Linux Patching Checks

Submit

Server SSH key

-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1r ...
-----END OPENSSH PRIVATE KEY-----

Server username

server_user

Server password or SSH key passphrase

server_password

Save

Sergey Egorov

Custom Nuclei rules

- Scan History
- Products
- Static Analysis
- Dynamic Scanning
- Infrastructure Checks
- Upload Report
- My Rules**
- Credentials
- Vuln DB
- Logout

Type

Nuclei

Rule

New

Rule text

Path Traversal vulnerability identified in a web application's file download function.

Here's the PoC:

HTTP Request:

```
GET /download?file=../../etc/passwd HTTP/1.1
Host: example.com
User-Agent: Mozilla/5.0
```

HTTP Response:

```
HTTP/1.1 200 OK
Content-Type: text/plain
Content-Length: 1827
Server: Apache
```

```
root:x:0:0:root:/root:/bin/bash
...
```

☒ Active

Delete rule

Gen with AI

Scan with custom rules across all targets

Scan History

Products

Static Analysis

Dynamic Scanning

Infrastructure Checks

Upload Report

My Rules

Credentials

Vuln DB

Logout

Product / Eng ID

Test (3) ▾

Ping hosts

No ▾

Scan ports

Top 1000 TCP/UDP ▾

Select Scan Type

Vulnerability Scan ▾

Choose scanners:

☐ OpenVAS

☐ Nessus

☐ Nuclei

☐ Bruteforcer

☒ Nuclei (My Rules)

☐ Nmap pre-scan

Submit

Questions?

<https://scansuite.gitbook.io/scansuite>