KnowBe4

Human error. Conquered.

Open Source Intelligence (OSINT): Learn the Methods Bad Actors Use to Hack Your Organization

KnowBe4

Human error. Conquered.

This presentation, and the following written materials, contain KnowBe4's proprietary and confidential information and is not to be published, duplicated, or distributed to any third party without KnowBe4's prior written consent.

Certain information in this presentation may contain "forward-looking statements" under applicable securities laws. Such statements in this presentation often contain words such as "expect," "anticipate," "intend," "plan," "believe," "will," "estimate," "forecast," "target," or "range" and are merely speculative. Attendees are cautioned not to place undue reliance on such forward-looking statements to reach conclusions or make any investment decisions. Information in this presentation speaks only as of the date that it was prepared and may become incomplete or out of date; KnowBe4 makes no commitment to update such information.

This presentation is for educational purposes only and should not be relied upon for any other use.

James R. McQuiggan
Security Awareness Advocate

Rosa L. Smothers
SVP Cyber Operations

KnowBe4
Human error. Conquered.

Agenda

- OSINT Ethics
- Secure Setup
- Setting the Stage
- Apps and Tools

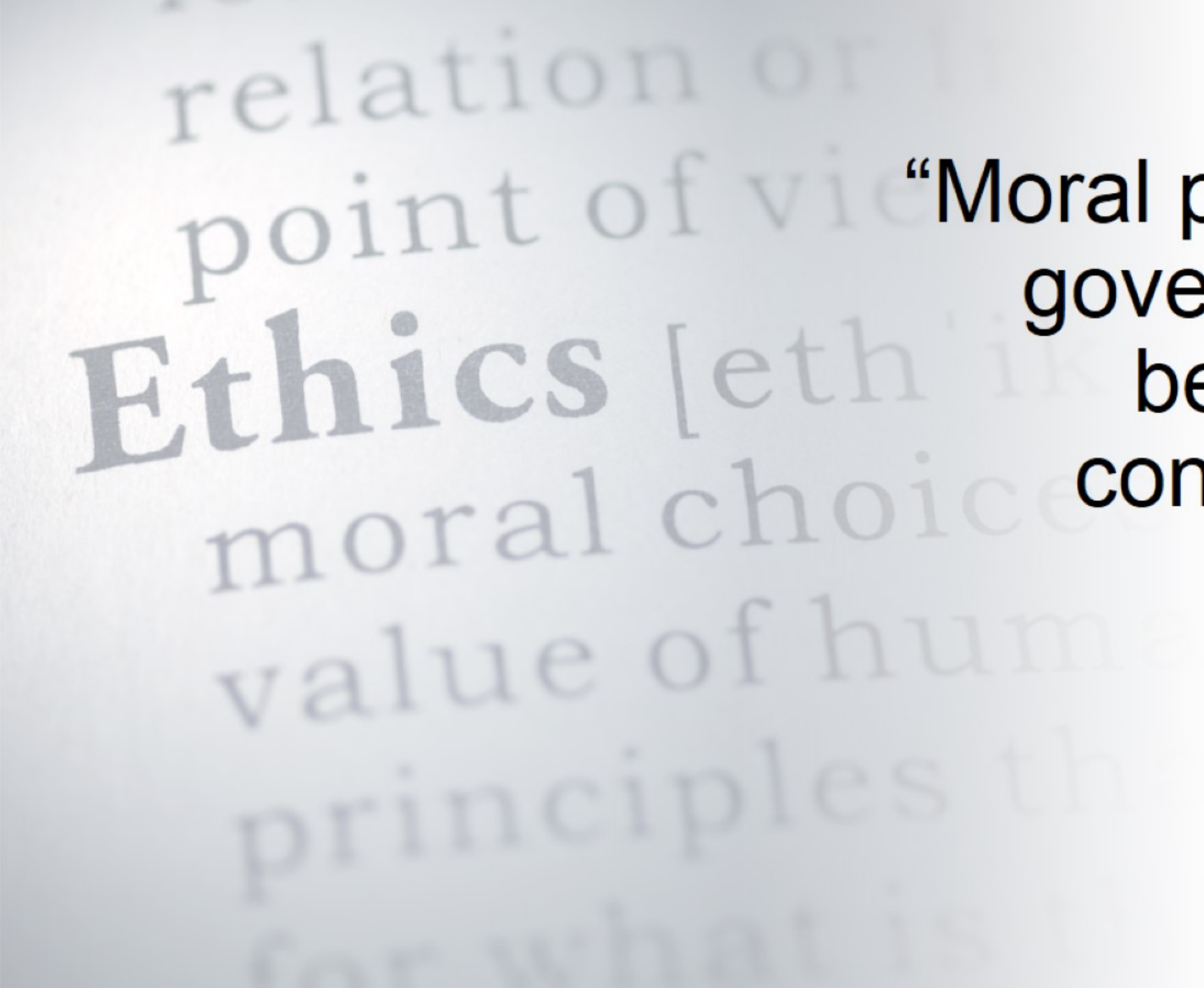
Agenda

- OSINT Ethics
- Secure Setup
- Setting the Stage
- Apps and Tools

Quote

”With great power comes great responsibility”

- A Superhero’s Uncle



"Moral principles that govern a person's behavior or the conducting of an activity"

- Oxford Dictionary

Agenda

- OSINT Ethics
- Secure Setup
- Setting the Stage
- Apps and Tools

KnowBe4
Human error. Conquered.

Safety First

Secure Your Setup

- Hardware/Software or Cloud
- Dedicated Machine
- Disk Wiper
- Virtual Machine
- VPN
- WHY do all of this? □□♀

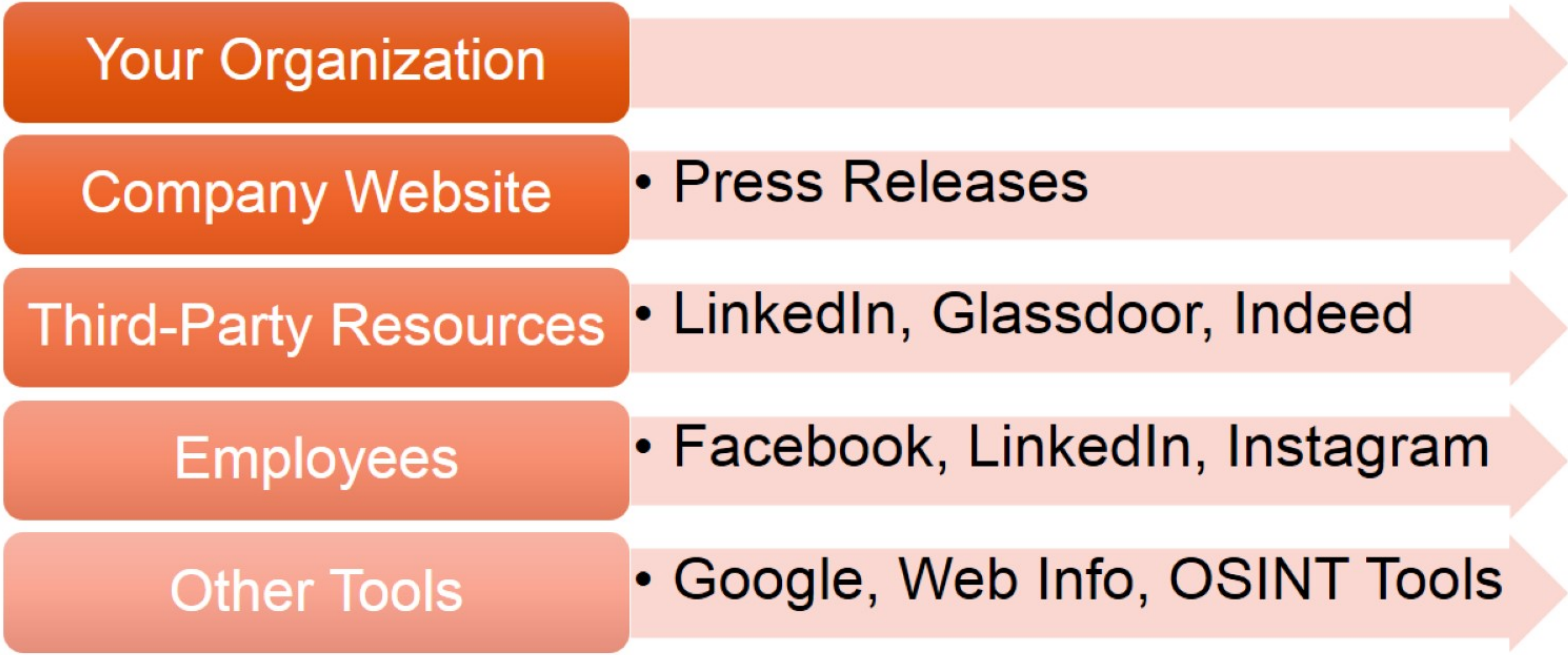
Agenda

- OSINT Ethics
- Secure Setup
- Setting the Stage
- Apps and Tools

Cyber Killchain for a Phishing Attack

Reconnaissance

Setting the Stage



Your Organization

Company Website

- Press Releases

Third-Party Resources

- LinkedIn, Glassdoor, Indeed

Employees

- Facebook, LinkedIn, Instagram

Other Tools

- Google, Web Info, OSINT Tools

Agenda

- OSINT Ethics
- Secure Setup
- Setting the Stage
- Apps and Tools

Google Dorking

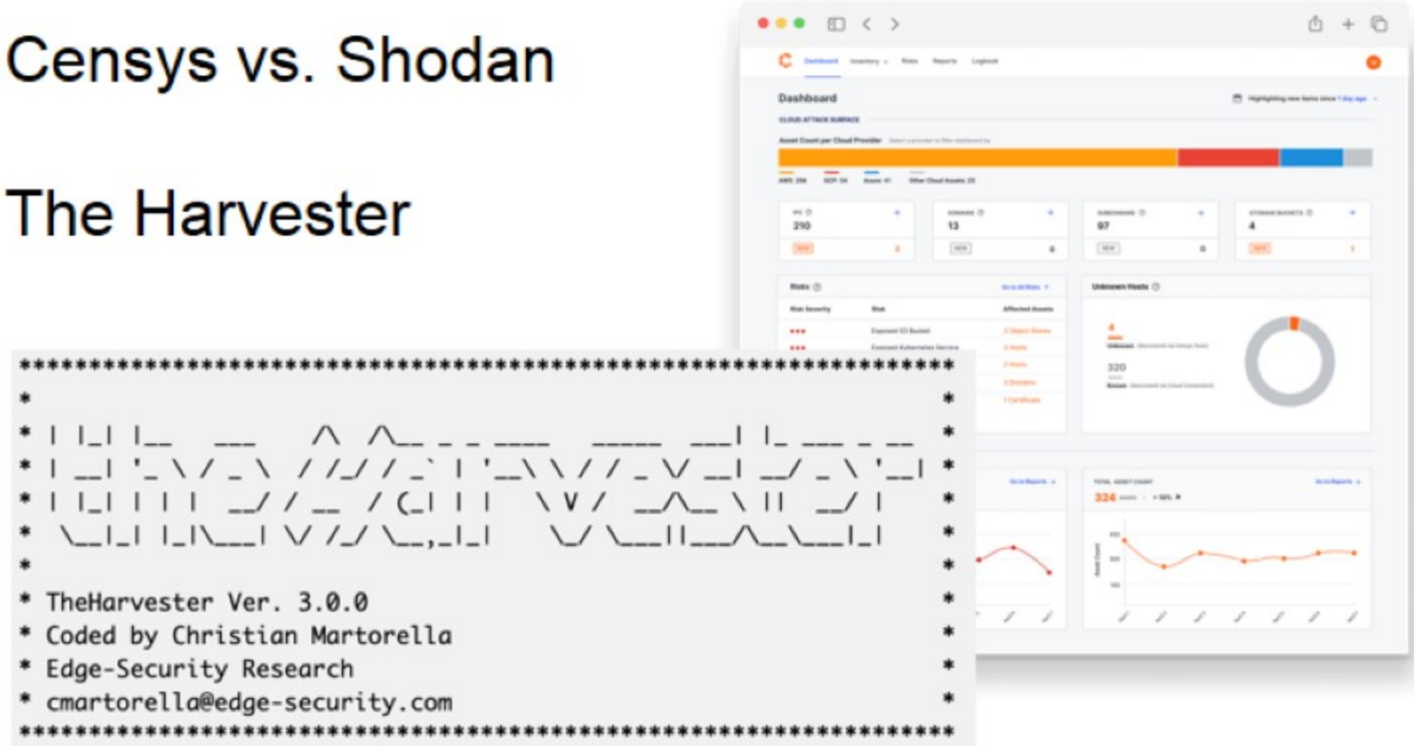
- **Cache -** find out what the most recent cache of a specified webpage is
- **Allinurl** - find pages with your requested search terms within the URL in internal search pages
- **Filetype** - a great way to narrow research on infographics or memes.
- **Inurl -** This is useful for finding sites with strong on-page optimization for the topics you are researching.
- **Intitle -** a narrower operator that will help you find more targeted results

Google Dorking Video

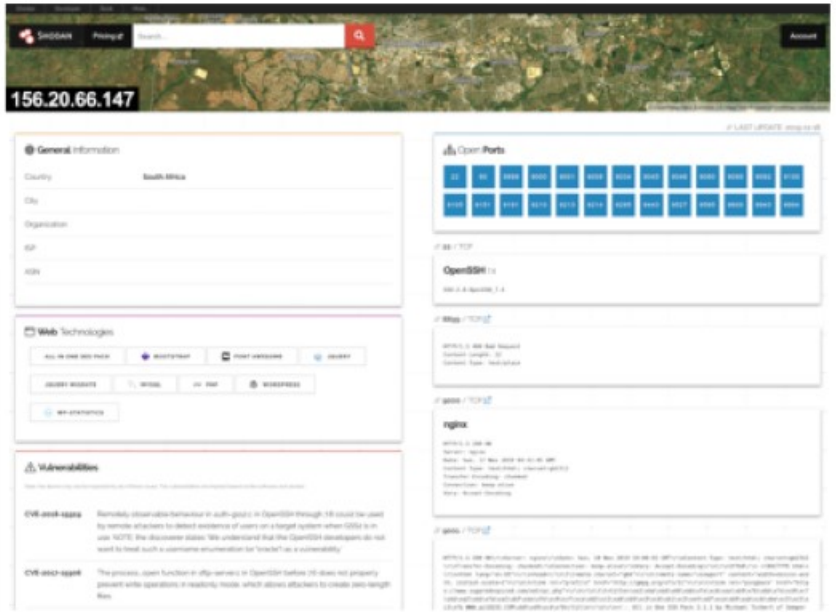
- Video placeholder for Google_Dork demo

Reconnaissance Tools

- Shodan
- Censys vs. Shodan
- The Harvester



```
*******************************************************************
*                                                                 *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __| '_ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* TheHarvester Ver. 3.0.0                                         *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*******************************************************************
```

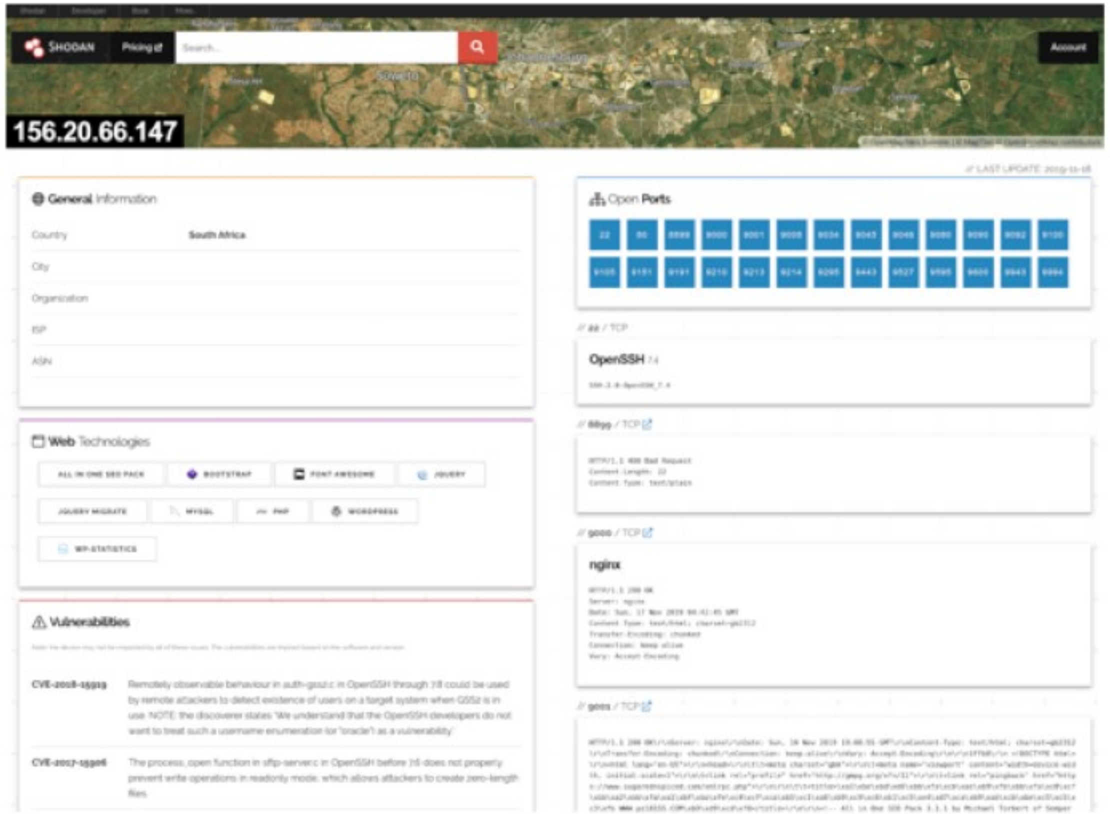


Reconnaissance Tools: Shodan

- Video placeholder for Shodan demo

Reconnaissance Tools: Shodan & Censys

Two Great Tools that OSINT Great Together



156.20.66.147

General Information

Country	South Africa
City	
Organization	
ISP	
ASN	

Web Technologies

Vulnerabilities

CVE-2018-15919	Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'
CVE-2017-15906	The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.

// LAST UPDATE: 2019-11-18

Open Ports

// 22 / TCP

OpenSSH 7.4

```
SSH-2.0-OpenSSH_7.4
```

// 8899 / TCP

```
HTTP/1.1 400 Bad Request
Content-Length: 22
Content-Type: text/plain
```

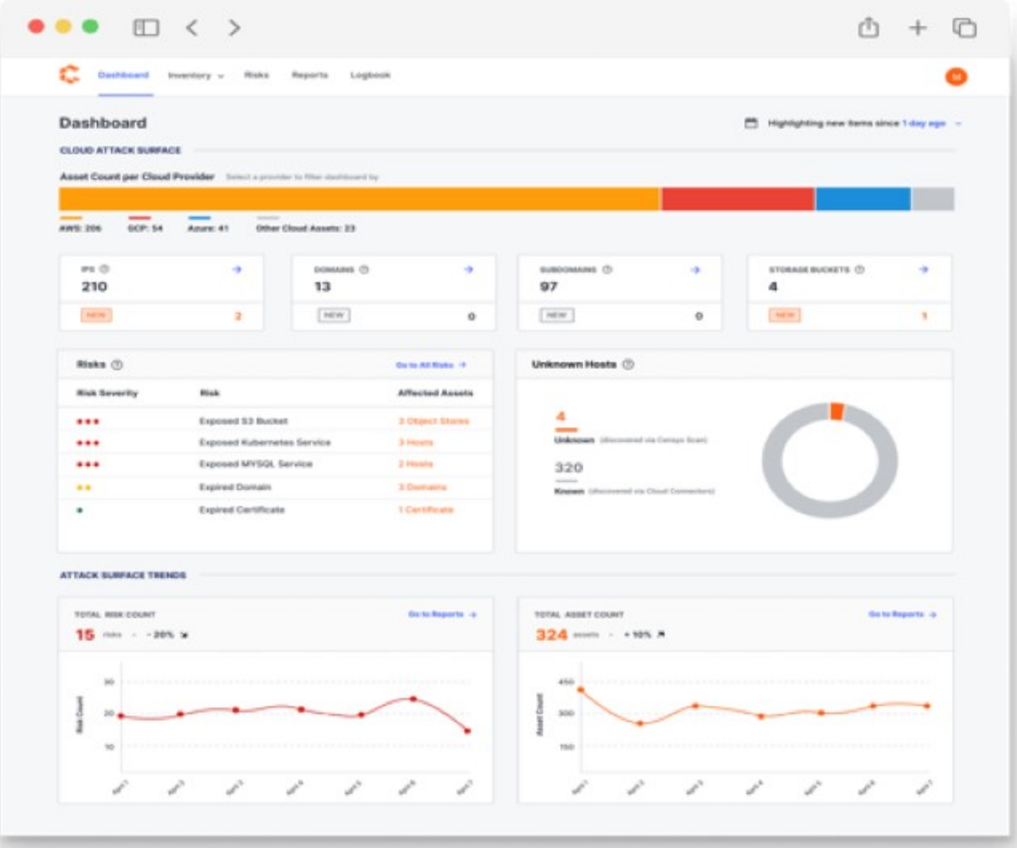
// 9000 / TCP

nginx

```
HTTP/1.1 200 OK
Server: nginx
Date: Sun, 17 Nov 2019 04:42:45 GMT
Content-Type: text/html; charset=gb2312
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
```

// 9001 / TCP

```
HTTP/1.1 200 OK\r\nServer: nginx\r\nDate: Sun, 10 Nov 2019 19:08:55 GMT\r\nContent-Type: text/html; charset=gb2312
... All in One SEO Pack 3.1.1 by Michael Torbert of Semper
```



Dashboard

Highlighting new items since 1 day ago

CLOUD ATTACK SURFACE

Asset Count per Cloud Provider

AWS: 206 GCP: 54 Azure: 41 Other Cloud Assets: 23

IPS	DOMAINS	SUBDOMAINS	STORAGE BUCKETS
210	13	97	4
NEW 2	NEW 0	NEW 0	NEW 1

Risks

Go to All Risks →

Risk Severity	Risk	Affected Assets
●●●	Exposed S3 Bucket	3 Object Stores
●●●	Exposed Kubernetes Service	3 Hosts
●●●	Exposed MYSQL Service	2 Hosts
●●	Expired Domain	3 Domains
●	Expired Certificate	1 Certificate

Unknown Hosts

4 Unknown (discovered via Censys Scan)

320 Known (discovered via Cloud Connectors)

ATTACK SURFACE TRENDS

TOTAL RISK COUNT

15 risks · -20%

Go to Reports →

TOTAL ASSET COUNT

324 assets · +10%

Go to Reports →

Reconnaissance Tools: Shodan vs. Censys

- Video placeholder for Shodan v Censys demo

Reconnaissance Tools: The Harvester

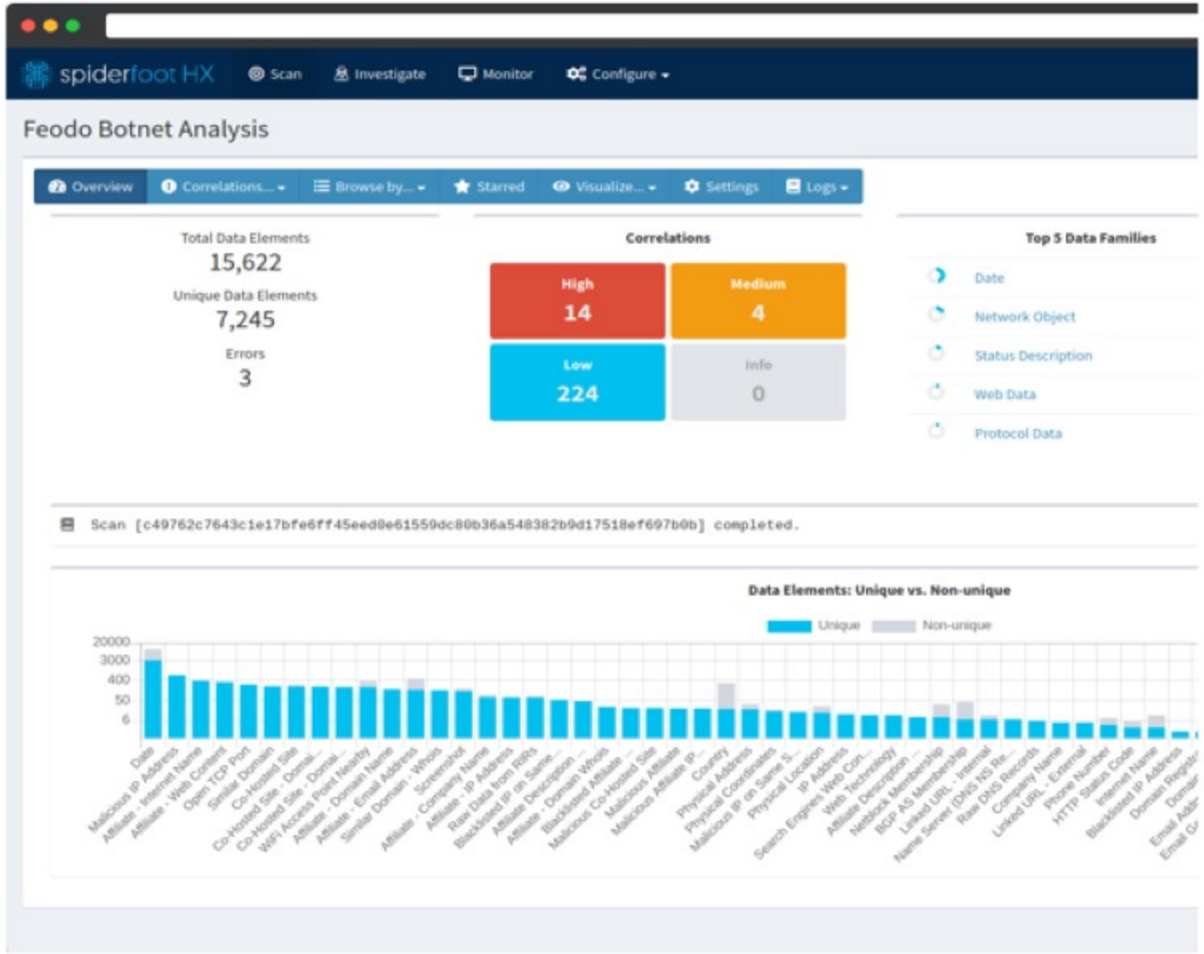
- Determine threat landscape
- Email Addresses
- Domain records
- Subdomains
- IP address & URLs
- Connects with multiple sources

theHarvester

Reconnaissance Tools: The Harvester

- Video placeholder for theHarvester demo

Reconnaissance Tools: Spiderfoot



Feodo Botnet Analysis

Total Data Elements
15,622

Unique Data Elements
7,245

Errors
3

Correlations

High 14	Medium 4
Low 224	Info 0

Top 5 Data Families

- Date
- Network Object
- Status Description
- Web Data
- Protocol Data

```
Scan [c49762c7643c1e17bfe6ff45eed0e61559dc80b36a548382b9d17518ef697b0b] completed.
```

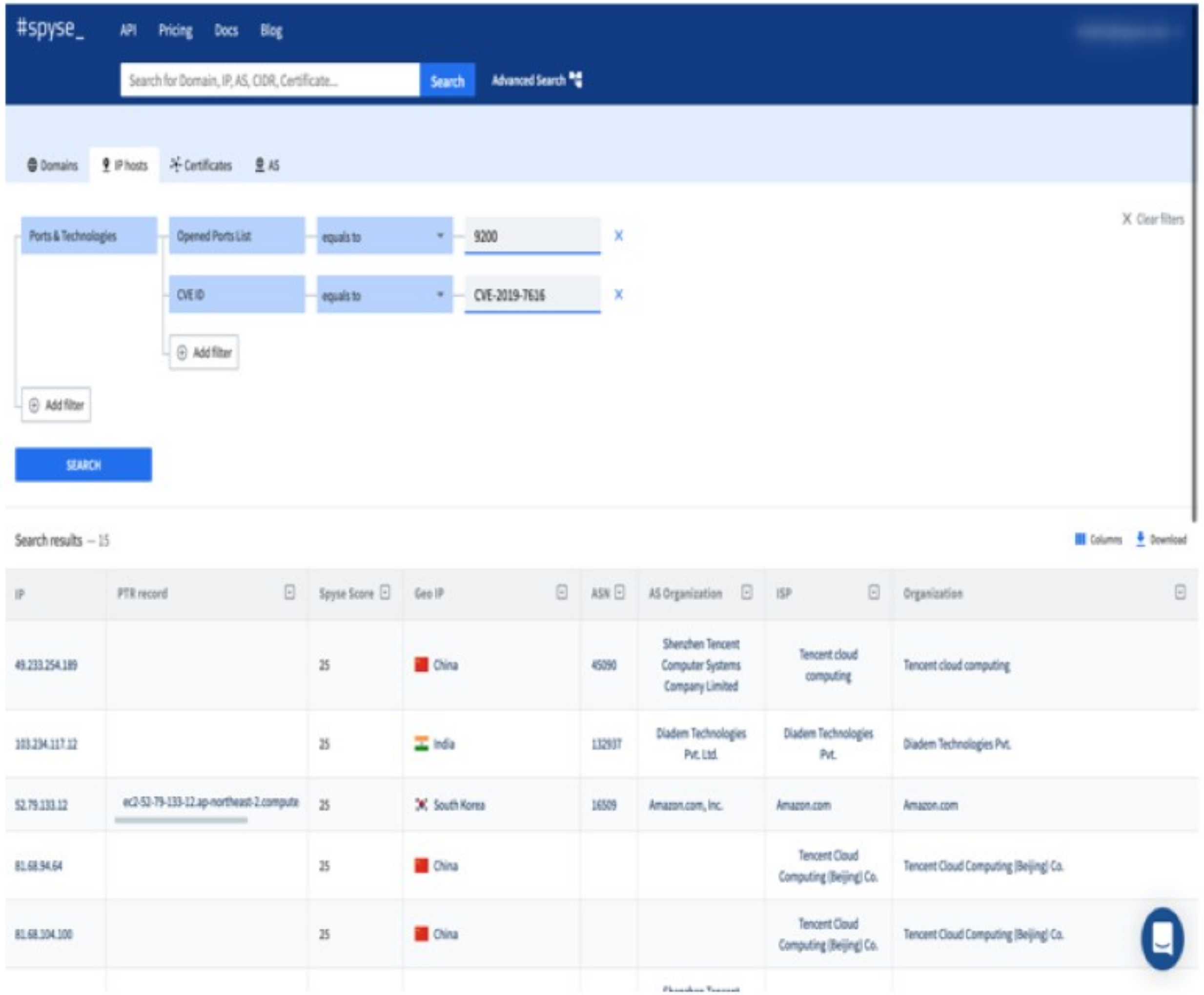
- Cyber Threat Intelligence
- Asset Discovery
- Security Assessments
- Monitor Your Asset Surface

KnowBe4
Human error. Conquered.

Reconnaissance Tools: Spiderfoot

- Video placeholder for Spiderfoot demo

Reconnaissance Tools: Spyse



Ports & Technologies — Opened Ports List — equals to — 9200

CVE ID — equals to — CVE-2019-7616

Search results — 15

IP	PTR record	Spyse Score	Geo IP	ASN	AS Organization	ISP	Organization
49.233.254.189		25	China	45090	Shenzhen Tencent Computer Systems Company Limited	Tencent cloud computing	Tencent cloud computing
103.234.117.12		25	India	132937	Diadem Technologies Pvt. Ltd.	Diadem Technologies Pvt.	Diadem Technologies Pvt.
52.79.133.12	ec2-52-79-133-12.ap-northeast-2.compute	25	South Korea	16509	Amazon.com, Inc.	Amazon.com	Amazon.com
81.68.94.64		25	China			Tencent Cloud Computing (Beijing) Co.	Tencent Cloud Computing (Beijing) Co.
81.68.104.100		25	China			Tencent Cloud Computing (Beijing) Co.	Tencent Cloud Computing (Beijing) Co.

- One of Internet’s Largest DBs
- Web Interface, API & Python
- “Scoring” Productivity Feature
- Precision Scanning

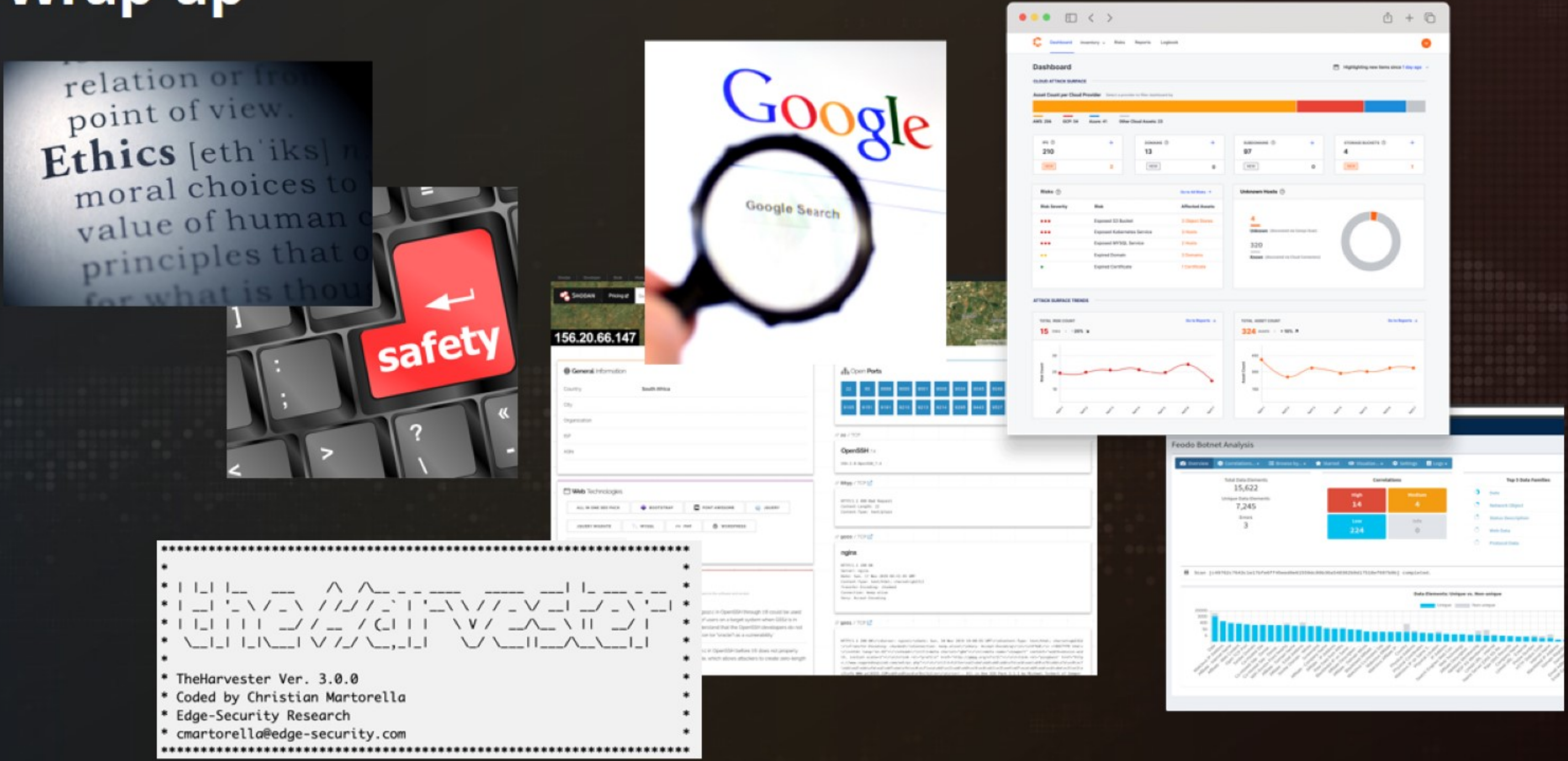
Reconnaissance Tools: Spyse

- Video placeholder for Spyse demo

Agenda

- OSINT Ethics
- Secure Setup
- Setting the Stage
- Apps and Tools
- Wrap-up

Wrap-up



```
*******************************************************************
*                                                                 *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* TheHarvester Ver. 3.0.0                                         *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*******************************************************************
```

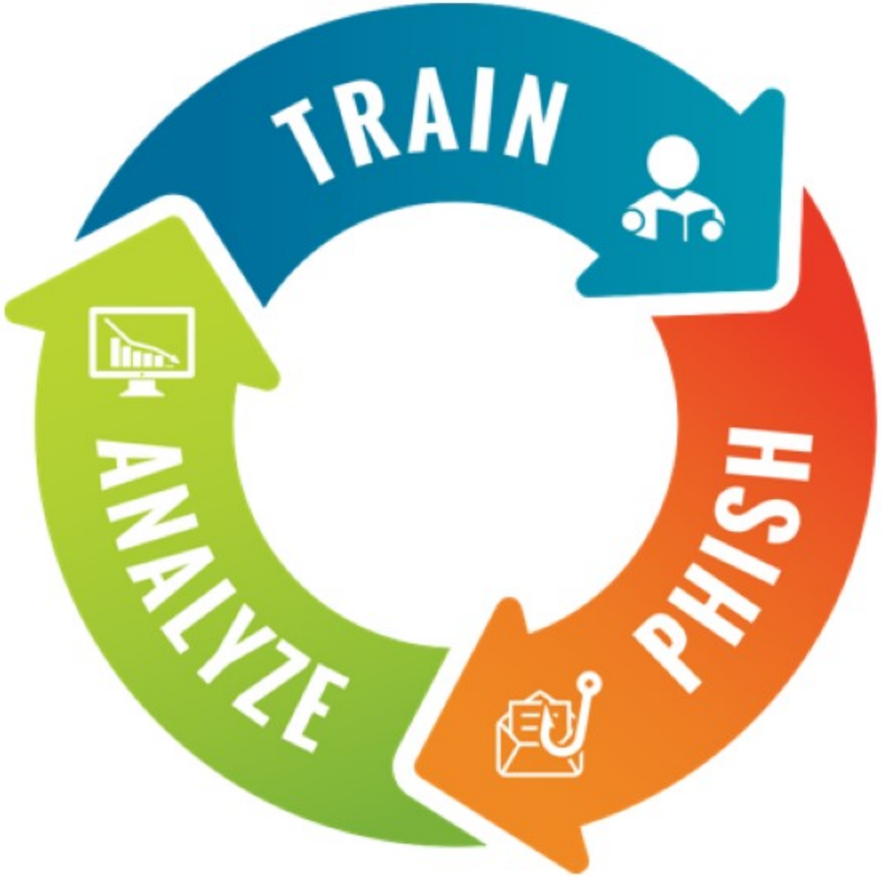
KnowBe4 Security Awareness Training

Baseline Testing
We provide baseline testing to assess the Phish-Prone™ percentage of your users through a free simulated phishing attack.

Train Your Users
The world's largest library of security awareness training content; including interactive modules, videos, games, posters and newsletters. Automated training campaigns with scheduled reminder emails.

Phish Your Users
Best-in-class, fully automated simulated phishing attacks, thousands of templates with unlimited usage, and community phishing templates.

See the Results
Enterprise-strength reporting, showing stats and graphs for both training and phishing, ready for management. Show the great ROI!



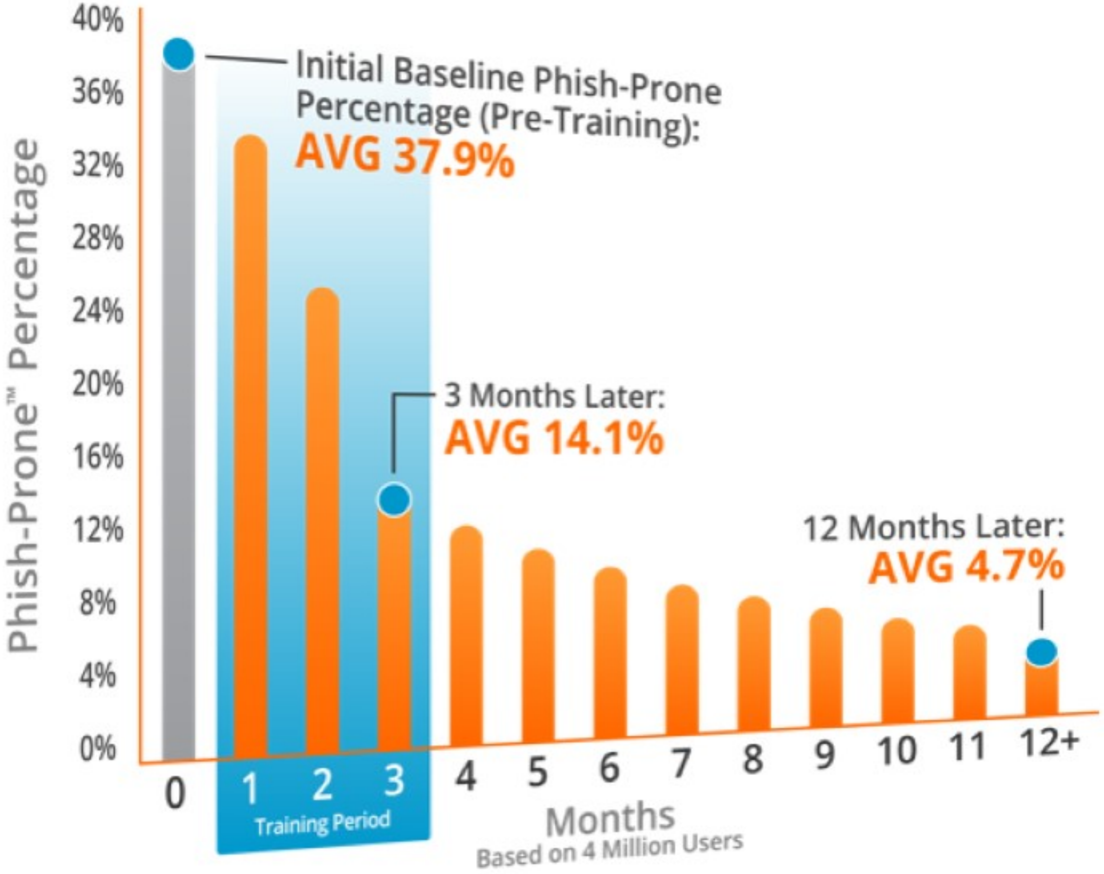
Phishing assessments to reduce ransomware attacks

- Reduced Malware Infections
- Reduced Data Loss
- Reduced Potential Cyber-theft
- Increased User Productivity
- Users Have Security Top of Mind

87% Average Improvement

Across all industries and sizes from baseline testing to one year or more of ongoing training and testing

Note: The initial Phish-Prone percentage is calculated on the basis of all users evaluated. These users had not received any training with the KnowBe4 platform prior to the evaluation. Subsequent time periods reflect Phish-Prone percentages for the subset of users who received training with the KnowBe4 platform.



Source: 2020 KnowBe4 Phishing by Industry Benchmarking Report

KnowBe4
Human error. Conquered.

Thank You For Your Attention

James R. McQuiggan
Security Awareness Advocate
jmcquiggan@knowbe4.com

Rosa Smothers
VP of Cyber Operations
rosas@knowbe4.com

KnowBe4
Human error. Conquered.

Know more about KnowBe4.
www.knowbe4.com