



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presentation, and the following written materials, contain KnowBe4's proprietary and confidential information and is not to be published, duplicated, or distributed to any third party without KnowBe4's prior written consent.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 Information in this presentation speaks only as of the date that it was prepared and may become incomplete or out of date; KnowBe4 makes no commitment to update such information.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

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

Ethics

“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

**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

Third-Party Resources

Employees

Other Tools

- Press Releases

- LinkedIn, Glassdoor, Indeed

- Facebook, LinkedIn, Instagram

- 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

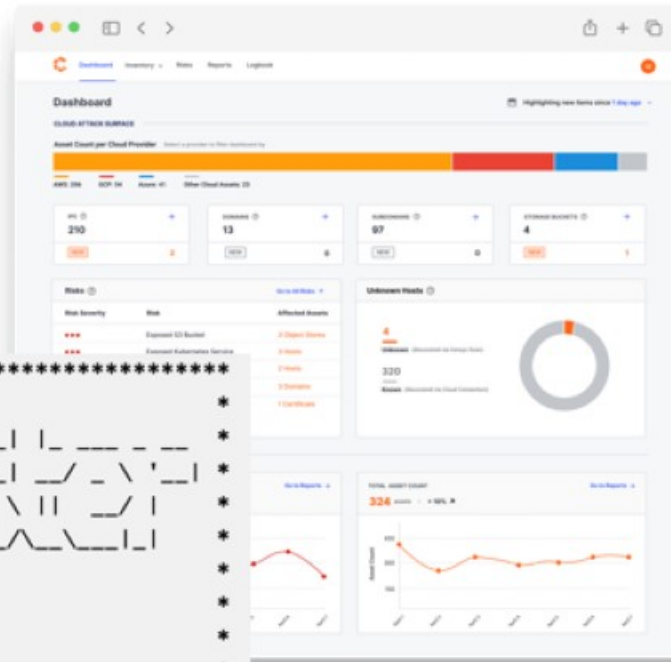


Google Dorking Video

- Video placeholder for Google_Dork demo

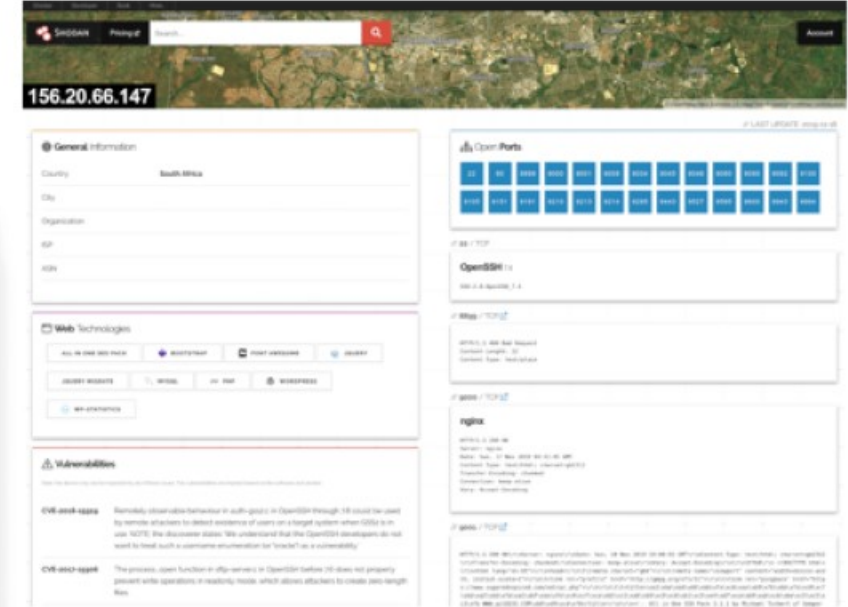
Reconnaissance Tools

- Shodan
- Censys vs. Shodan
- The Harvester



```

*****
*                                     *
* | | | _ _ _ _ _ ^ ^ ^ - - - - | | | | | | *
* | | | ' \ / \ / \ / \ / \ / \ / \ / \ / \ / *
* | | | | | | | | | | | | | | | | | | | | | *
* \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ *
*                                     *
* 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

The screenshot shows the Shodan search engine interface. At the top, there is a search bar with the IP address "156.20.66.147" entered. Below the search bar, there is a map showing the location of the IP address in South Africa. The main content area is divided into several sections:

- General Information:** Country: South Africa, City, Organization, ISP, ASN.
- Web Technologies:** ALL IN ONE WP-PAK, BOOTSTRAP, FONT AWESOME, JQUERY, JQUERY MIGRATE, MYSQL, PHP, WORDPRESS, WP-STATISTICS.
- Vulnerabilities:** CVE-2018-15919: Remotely observable behaviour in auth-gssapi in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSSAPI is in use. CVE-2017-15696: The process_open function in sftp-server in OpenSSH before 7.5 does not properly prevent write operations in read-only mode, which allows attackers to create zero-length files.
- Open Ports:** A grid of 20 buttons representing open ports: 22, 80, 8080, 8081, 8082, 8083, 8084, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8092, 8093, 8094, 8095, 8096, 8097, 8098.
- OpenSSH 7.8:** CVE-2018-15919, 7.x
- nginx:** CVE-2017-15696, Server: nginx, Status: 200, 17 Nov 2019 06:12:45 GMT, Content-Type: text/html; charset=utf-8, Transfer-Encoding: chunked, Expires: Wed, 01 Jun 2010 12:00:00 GMT, Vary: Accept-Encoding.

The screenshot shows the Censys dashboard interface. The main section is titled "Dashboard" and "CLOUD ATTACK SURFACE". It features several key metrics and charts:

- Asset Count per Cloud Provider:** A horizontal bar chart showing asset counts for AWS (206), GCP (54), Azure (41), and Other Cloud Assets (33).
- IPs:** 210
- DOMAINS:** 13
- SUBDOMAINS:** 97
- STORAGE BUCKETS:** 4
- Risks:** A table showing risk severity, risk, and affected assets:

Risk Severity	Risk	Affected Assets
High	Exposed S3 Bucket	2 Object Stores
High	Exposed Kubernetes Service	3 Hosts
High	Exposed MySQL Service	2 Hosts
Medium	Expired Domain	2 Domains
Low	Expired Certificate	1 Certificate
- Unknown Hosts:** 4 Unknown (Unconnected via Google Search), 320 Known (Unconnected via Cloud Connections).
- ATTACK SURFACE TRENDS:** Two line charts showing trends over time:
 - TOTAL RISK COUNT:** 15 risks, -26% change.
 - TOTAL ASSET COUNT:** 324 assets, +10% change.

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

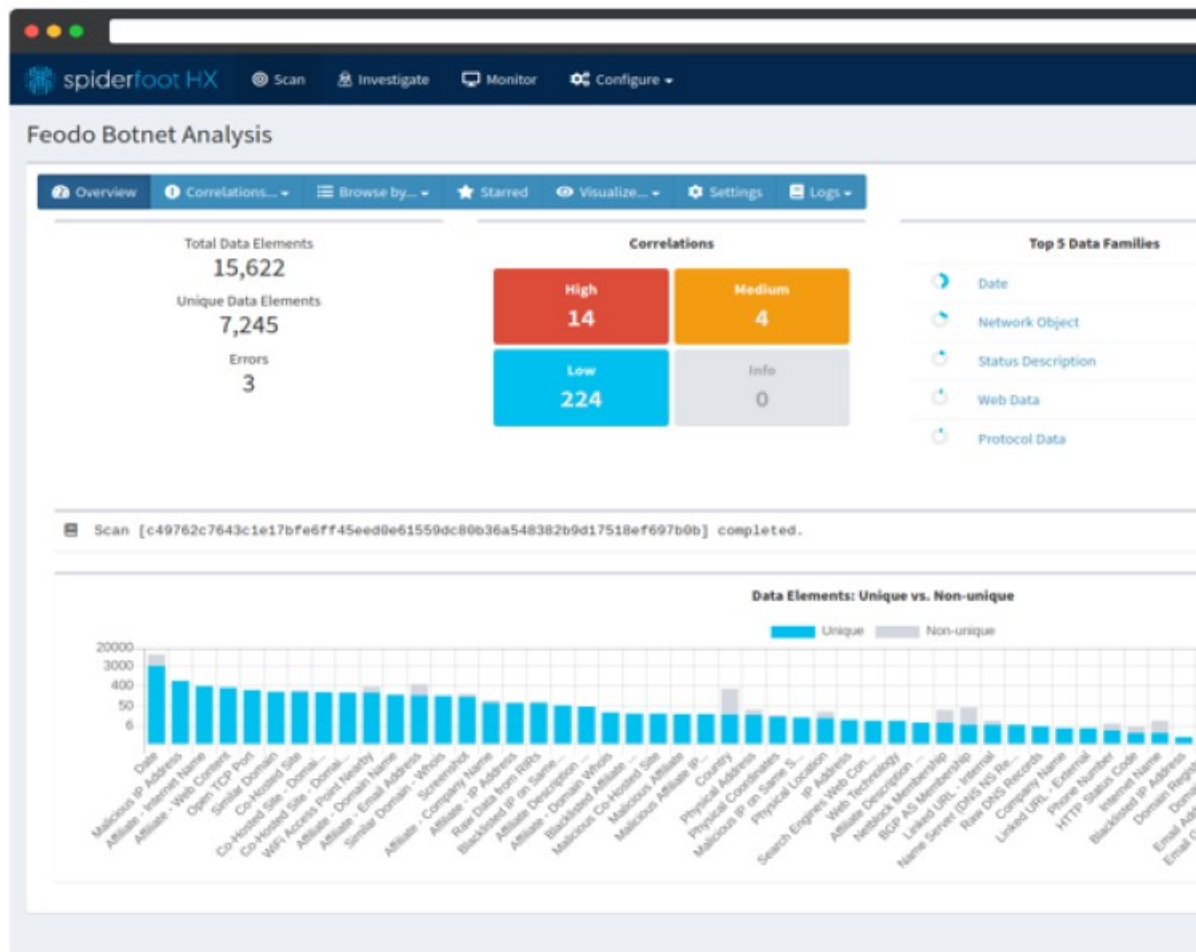


theHarvester

Reconnaissance Tools: The Harvester

- Video placeholder for the Harvester demo

Reconnaissance Tools: Spiderfoot

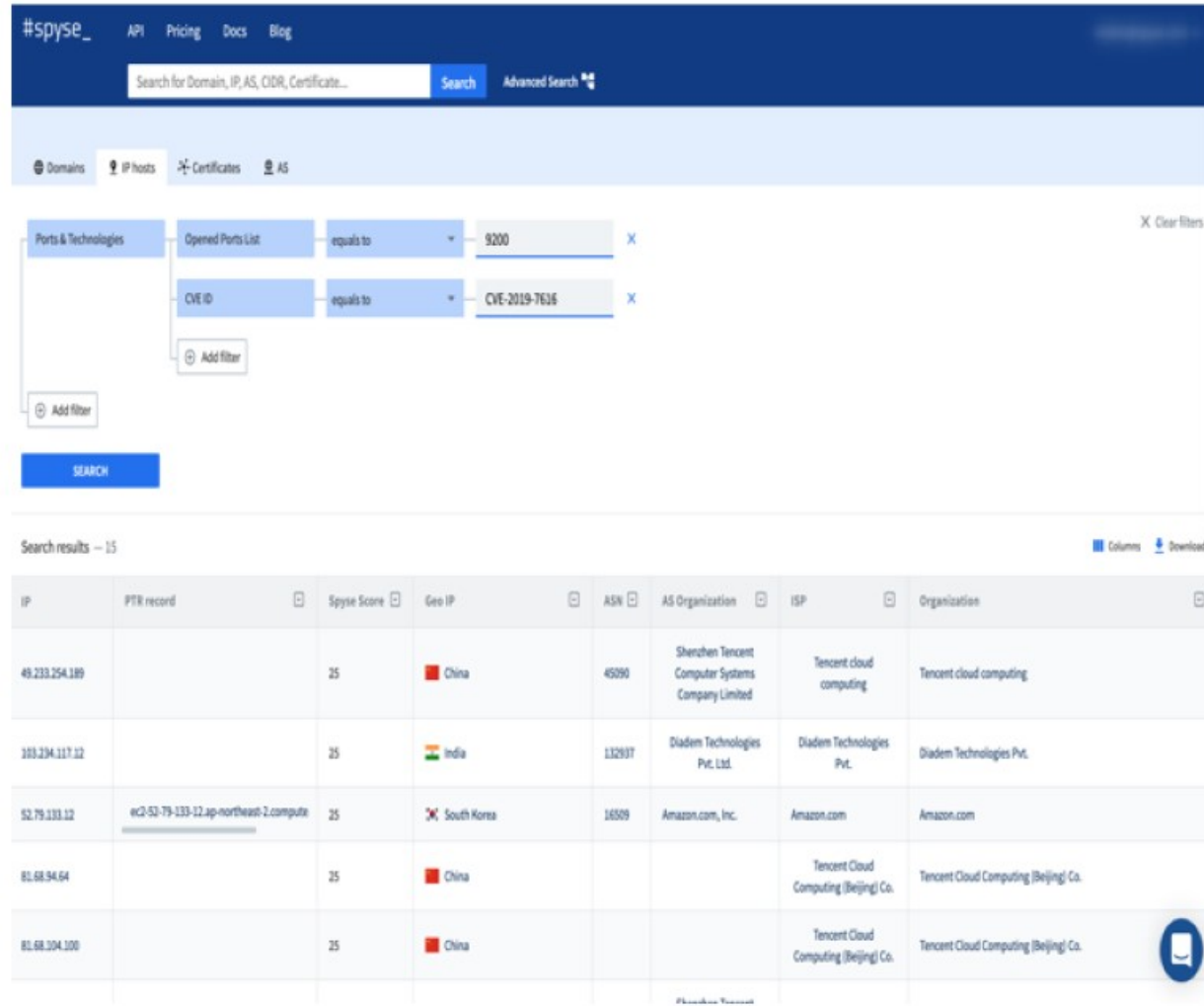


- Cyber Threat Intelligence
- Asset Discovery
- Security Assessments
- Monitor Your Asset Surface

Reconnaissance Tools: Spiderfoot

- Video placeholder for Spiderfoot demo

Reconnaissance Tools: Spyse



The screenshot shows the Spyse web interface. At the top, there is a navigation bar with "#spyse_" and links for "API", "Pricing", "Docs", and "Blog". Below this is a search bar with the placeholder text "Search for Domain, IP, AS, CDR, Certificate..." and a "Search" button. To the right of the search bar is an "Advanced Search" link. Below the search bar, there are tabs for "Domains", "IP Hosts", "Certificates", and "AS". The main content area shows a filter panel on the left with "Ports & Technologies" selected. Two filters are applied: "Opened Ports List" equals to "9200" and "CVE ID" equals to "CVE-2019-7616". There are "Add filter" buttons and a "Clear filters" button. Below the filter panel is a "SEARCH" button. The search results section shows "Search results — 15" and a "Columns" button. The results are displayed in a table with the following columns: IP, PTR record, Spyse Score, Geo IP, ASN, AS Organization, ISP, and Organization.

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

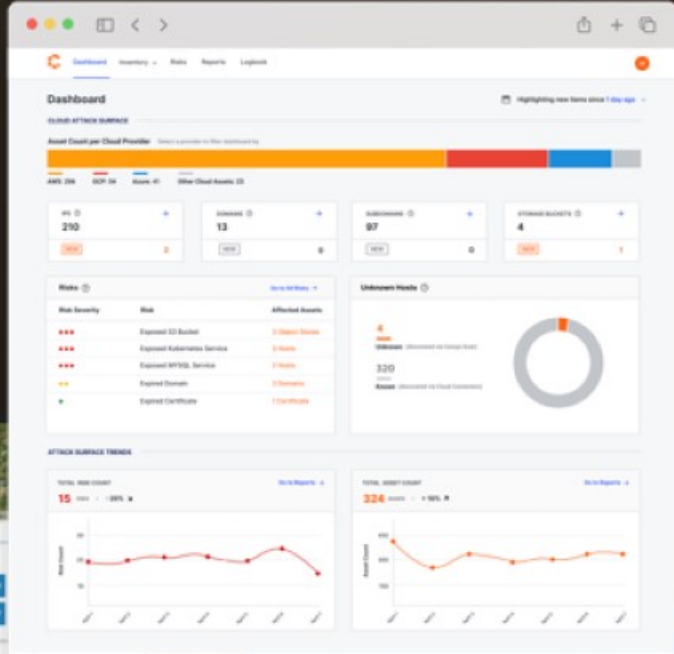
- Video placeholder for Spyse demo

Agenda

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

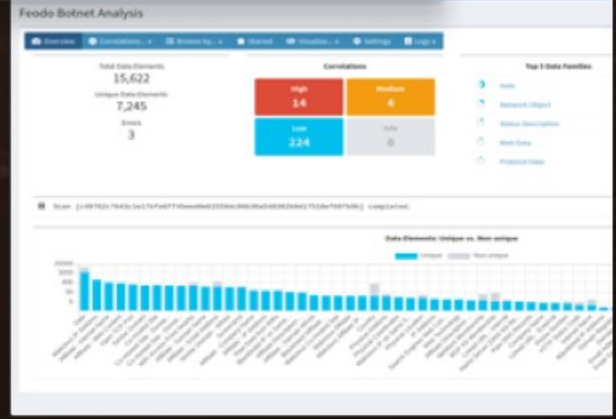
Wrap-up

relation or from
point of view.
Ethics [eth'iks] n
moral choices to
value of human
principles that o
for what is thou



General Information
Country: South Africa
City: [Redacted]
Organization: [Redacted]
ISP: [Redacted]
ASN: [Redacted]

Open Ports
22, 80, 443, 8080, 8443, 8081, 8082, 8083, 8084, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8092, 8093, 8094, 8095, 8096, 8097, 8098, 8099, 9000, 9001, 9002, 9003, 9004, 9005, 9006, 9007, 9008, 9009, 9010, 9011, 9012, 9013, 9014, 9015, 9016, 9017, 9018, 9019, 9020, 9021, 9022, 9023, 9024, 9025, 9026, 9027, 9028, 9029, 9030, 9031, 9032, 9033, 9034, 9035, 9036, 9037, 9038, 9039, 9040, 9041, 9042, 9043, 9044, 9045, 9046, 9047, 9048, 9049, 9050, 9051, 9052, 9053, 9054, 9055, 9056, 9057, 9058, 9059, 9060, 9061, 9062, 9063, 9064, 9065, 9066, 9067, 9068, 9069, 9070, 9071, 9072, 9073, 9074, 9075, 9076, 9077, 9078, 9079, 9080, 9081, 9082, 9083, 9084, 9085, 9086, 9087, 9088, 9089, 9090, 9091, 9092, 9093, 9094, 9095, 9096, 9097, 9098, 9099, 9100, 9101, 9102, 9103, 9104, 9105, 9106, 9107, 9108, 9109, 9110, 9111, 9112, 9113, 9114, 9115, 9116, 9117, 9118, 9119, 9120, 9121, 9122, 9123, 9124, 9125, 9126, 9127, 9128, 9129, 9130, 9131, 9132, 9133, 9134, 9135, 9136, 9137, 9138, 9139, 9140, 9141, 9142, 9143, 9144, 9145, 9146, 9147, 9148, 9149, 9150, 9151, 9152, 9153, 9154, 9155, 9156, 9157, 9158, 9159, 9160, 9161, 9162, 9163, 9164, 9165, 9166, 9167, 9168, 9169, 9170, 9171, 9172, 9173, 9174, 9175, 9176, 9177, 9178, 9179, 9180, 9181, 9182, 9183, 9184, 9185, 9186, 9187, 9188, 9189, 9190, 9191, 9192, 9193, 9194, 9195, 9196, 9197, 9198, 9199, 9200, 9201, 9202, 9203, 9204, 9205, 9206, 9207, 9208, 9209, 9210, 9211, 9212, 9213, 9214, 9215, 9216, 9217, 9218, 9219, 9220, 9221, 9222, 9223, 9224, 9225, 9226, 9227, 9228, 9229, 9230, 9231, 9232, 9233, 9234, 9235, 9236, 9237, 9238, 9239, 9240, 9241, 9242, 9243, 9244, 9245, 9246, 9247, 9248, 9249, 9250, 9251, 9252, 9253, 9254, 9255, 9256, 9257, 9258, 9259, 9260, 9261, 9262, 9263, 9264, 9265, 9266, 9267, 9268, 9269, 9270, 9271, 9272, 9273, 9274, 9275, 9276, 9277, 9278, 9279, 9280, 9281, 9282, 9283, 9284, 9285, 9286, 9287, 9288, 9289, 9290, 9291, 9292, 9293, 9294, 9295, 9296, 9297, 9298, 9299, 9300, 9301, 9302, 9303, 9304, 9305, 9306, 9307, 9308, 9309, 9310, 9311, 9312, 9313, 9314, 9315, 9316, 9317, 9318, 9319, 9320, 9321, 9322, 9323, 9324, 9325, 9326, 9327, 9328, 9329, 9330, 9331, 9332, 9333, 9334, 9335, 9336, 9337, 9338, 9339, 9340, 9341, 9342, 9343, 9344, 9345, 9346, 9347, 9348, 9349, 9350, 9351, 9352, 9353, 9354, 9355, 9356, 9357, 9358, 9359, 9360, 9361, 9362, 9363, 9364, 9365, 9366, 9367, 9368, 9369, 9370, 9371, 9372, 9373, 9374, 9375, 9376, 9377, 9378, 9379, 9380, 9381, 9382, 9383, 9384, 9385, 9386, 9387, 9388, 9389, 9390, 9391, 9392, 9393, 9394, 9395, 9396, 9397, 9398, 9399, 9400, 9401, 9402, 9403, 9404, 9405, 9406, 9407, 9408, 9409, 9410, 9411, 9412, 9413, 9414, 9415, 9416, 9417, 9418, 9419, 9420, 9421, 9422, 9423, 9424, 9425, 9426, 9427, 9428, 9429, 9430, 9431, 9432, 9433, 9434, 9435, 9436, 9437, 9438, 9439, 9440, 9441, 9442, 9443, 9444, 9445, 9446, 9447, 9448, 9449, 9450, 9451, 9452, 9453, 9454, 9455, 9456, 9457, 9458, 9459, 9460, 9461, 9462, 9463, 9464, 9465, 9466, 9467, 9468, 9469, 9470, 9471, 9472, 9473, 9474, 9475, 9476, 9477, 9478, 9479, 9480, 9481, 9482, 9483, 9484, 9485, 9486, 9487, 9488, 9489, 9490, 9491, 9492, 9493, 9494, 9495, 9496, 9497, 9498, 9499, 9500, 9501, 9502, 9503, 9504, 9505, 9506, 9507, 9508, 9509, 9510, 9511, 9512, 9513, 9514, 9515, 9516, 9517, 9518, 9519, 9520, 9521, 9522, 9523, 9524, 9525, 9526, 9527, 9528, 9529, 9530, 9531, 9532, 9533, 9534, 9535, 9536, 9537, 9538, 9539, 9540, 9541, 9542, 9543, 9544, 9545, 9546, 9547, 9548, 9549, 9550, 9551, 9552, 9553, 9554, 9555, 9556, 9557, 9558, 9559, 9560, 9561, 9562, 9563, 9564, 9565, 9566, 9567, 9568, 9569, 9570, 9571, 9572, 9573, 9574, 9575, 9576, 9577, 9578, 9579, 9580, 9581, 9582, 9583, 9584, 9585, 9586, 9587, 9588, 9589, 9590, 9591, 9592, 9593, 9594, 9595, 9596, 9597, 9598, 9599, 9600, 9601, 9602, 9603, 9604, 9605, 9606, 9607, 9608, 9609, 9610, 9611, 9612, 9613, 9614, 9615, 9616, 9617, 9618, 9619, 9620, 9621, 9622, 9623, 9624, 9625, 9626, 9627, 9628, 9629, 9630, 9631, 9632, 9633, 9634, 9635, 9636, 9637, 9638, 9639, 9640, 9641, 9642, 9643, 9644, 9645, 9646, 9647, 9648, 9649, 9650, 9651, 9652, 9653, 9654, 9655, 9656, 9657, 9658, 9659, 9660, 9661, 9662, 9663, 9664, 9665, 9666, 9667, 9668, 9669, 9670, 9671, 9672, 9673, 9674, 9675, 9676, 9677, 9678, 9679, 9680, 9681, 9682, 9683, 9684, 9685, 9686, 9687, 9688, 9689, 9690, 9691, 9692, 9693, 9694, 9695, 9696, 9697, 9698, 9699, 9700, 9701, 9702, 9703, 9704, 9705, 9706, 9707, 9708, 9709, 9710, 9711, 9712, 9713, 9714, 9715, 9716, 9717, 9718, 9719, 9720, 9721, 9722, 9723, 9724, 9725, 9726, 9727, 9728, 9729, 9730, 9731, 9732, 9733, 9734, 9735, 9736, 9737, 9738, 9739, 9740, 9741, 9742, 9743, 9744, 9745, 9746, 9747, 9748, 9749, 9750, 9751, 9752, 9753, 9754, 9755, 9756, 9757, 9758, 9759, 9760, 9761, 9762, 9763, 9764, 9765, 9766, 9767, 9768, 9769, 9770, 9771, 9772, 9773, 9774, 9775, 9776, 9777, 9778, 9779, 9780, 9781, 9782, 9783, 9784, 9785, 9786, 9787, 9788, 9789, 9790, 9791, 9792, 9793, 9794, 9795, 9796, 9797, 9798, 9799, 9800, 9801, 9802, 9803, 9804, 9805, 9806, 9807, 9808, 9809, 9810, 9811, 9812, 9813, 9814, 9815, 9816, 9817, 9818, 9819, 9820, 9821, 9822, 9823, 9824, 9825, 9826, 9827, 9828, 9829, 9830, 9831, 9832, 9833, 9834, 9835, 9836, 9837, 9838, 9839, 9840, 9841, 9842, 9843, 9844, 9845, 9846, 9847, 9848, 9849, 9850, 9851, 9852, 9853, 9854, 9855, 9856, 9857, 9858, 9859, 9860, 9861, 9862, 9863, 9864, 9865, 9866, 9867, 9868, 9869, 9870, 9871, 9872, 9873, 9874, 9875, 9876, 9877, 9878, 9879, 9880, 9881, 9882, 9883, 9884, 9885, 9886, 9887, 9888, 9889, 9890, 9891, 9892, 9893, 9894, 9895, 9896, 9897, 9898, 9899, 9900, 9901, 9902, 9903, 9904, 9905, 9906, 9907, 9908, 9909, 9910, 9911, 9912, 9913, 9914, 9915, 9916, 9917, 9918, 9919, 9920, 9921, 9922, 9923, 9924, 9925, 9926, 9927, 9928, 9929, 9930, 9931, 9932, 9933, 9934, 9935, 9936, 9937, 9938, 9939, 9940, 9941, 9942, 9943, 9944, 9945, 9946, 9947, 9948, 9949, 9950, 9951, 9952, 9953, 9954, 9955, 9956, 9957, 9958, 9959, 9960, 9961, 9962, 9963, 9964, 9965, 9966, 9967, 9968, 9969, 9970, 9971, 9972, 9973, 9974, 9975, 9976, 9977, 9978, 9979, 9980, 9981, 9982, 9983, 9984, 9985, 9986, 9987, 9988, 9989, 9990, 9991, 9992, 9993, 9994, 9995, 9996, 9997, 9998, 9999, 10000



* 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!



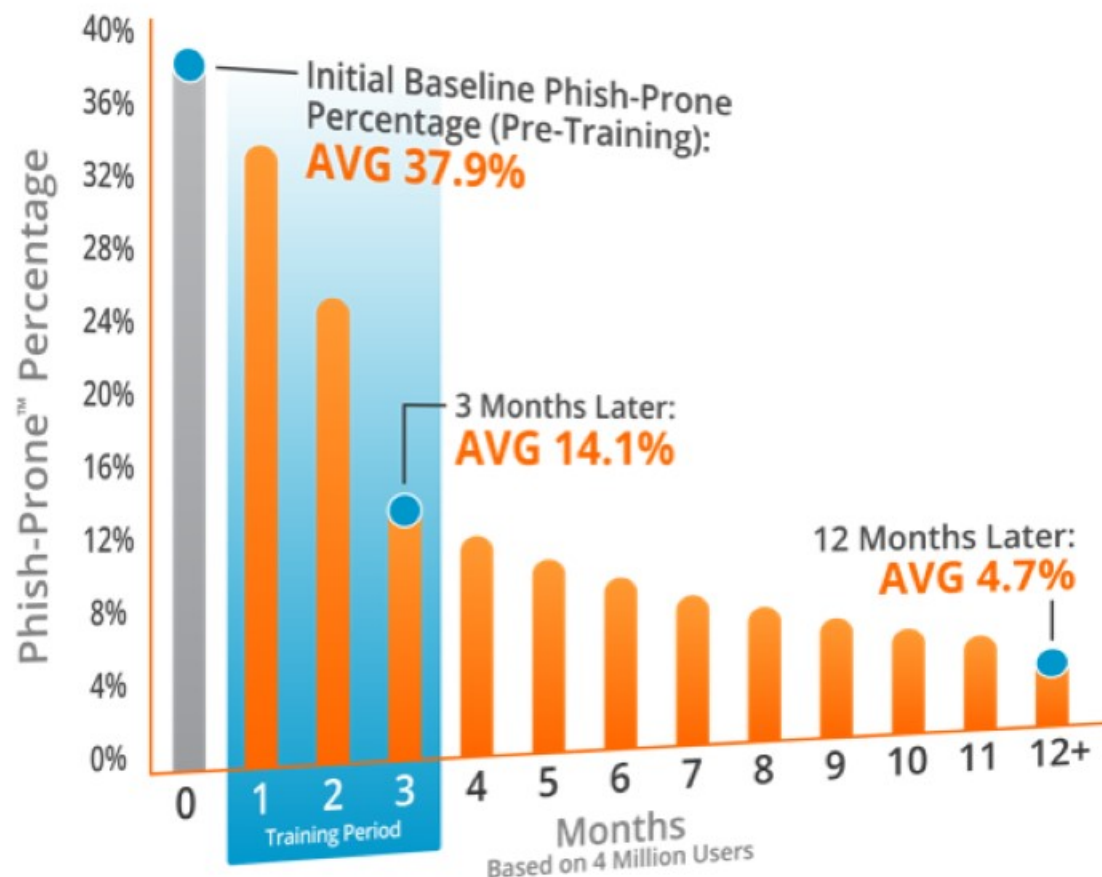
Phishing assessments to reduce ransomware attacks

- 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

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