Social <engineering> Dilemma

Michael Melore, CISSP
IBM Public Sector Cybersecurity Ambassador
& Senior Cybersecurity Advisor
Co-Founder SecRT (Security <Leaders> Round Table)
www.SecRT.us

IBM

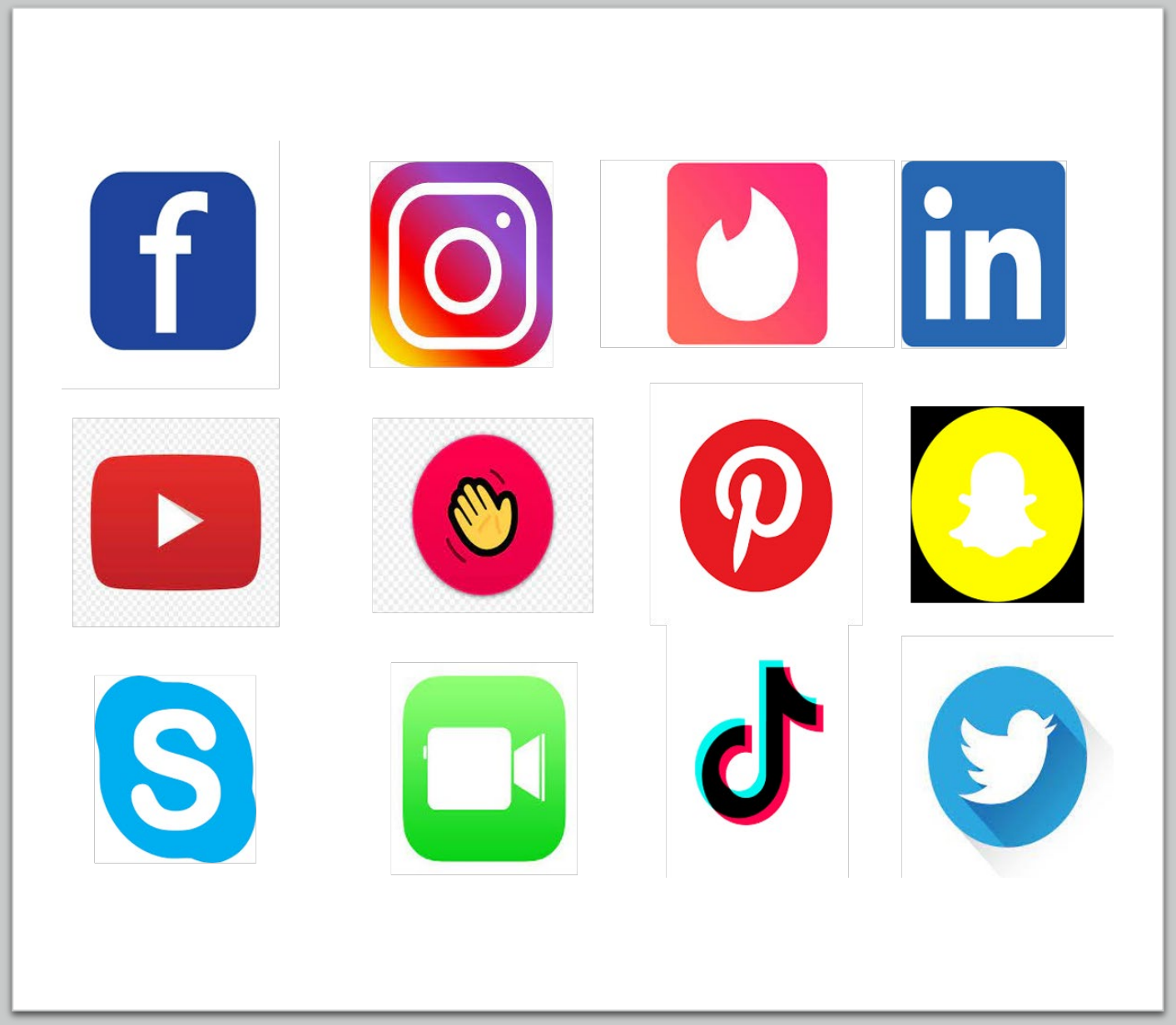
IBM Security No Cost Trusted Advisory Programs

- **Architect led collaborative workshops**
  Interactive no products pitched education
- **XForce Cyber Range Exercises**
  Exclusive Sessions available at cost
- **Solution and Threat Briefings**
- **IBM Center for Government Cybersecurity**
  Understand cyber threats with the IBM Center for Government Cybersecurity
  https://www.ibm.com/security/services/us-federal-cybersecurity-center
- **Onsite collaborative exercises/knowledge sharing/tech days**
  Can be jointly delivered with State Officials
- **IBM Sponsored External Committees**
  www.IJIS.org IJIS Institute Cybersecurity Task Force
  www.NASCIO.org National Assoc State CIOs
  Privacy and Cybersecurity Working Groups
  www.ATARC.org Advanced Technology Academic Research Center
  Government Grants, Higher Ed, and Cyber Defense Working Groups California
  California Cybersecurity Task Force- Workforce Development-Education Subcommittee
- **XForce Exchange Threat Intelligence Forum**
  https://exchange.xforce.ibmcloud.com
- **IBM Security Learning Academy**
  Hundreds of no cost Tutorials/Hand on Labs
  https://www.securitylearningacademy.com
- **IBM's New Collar / Apprentice programs**
  https://IBM.BIZ/USAPPRENTICESHIP
- **IBM's Skills Build (Resources for Learners, Educators and Organizations)**
  https://skillsbuild.org
- **XForce Webinars on Threat Landscapes**
- **IBM Security Solution User Groups**
- **Regional/Nationwide Security Leaders Round Tables**
  www.SECRT.us
  Grass roots, non sponsored, no cost Security Executive Round Tables Nationwide, initially founded by Mike Melore and a dozen CISOs, now at 18 active Nationwide chapters, 1400+ opt in security leaders as members.

Social Media

<engineering>

- **Identity**
- **Profile**
- **Locations**
- **Interests**
- **Friends/Family**
- **Work**
- **Finances**



IOT

YouTube
Aol HD.
vudu

amazon

Flexible ways of collaboration
Third-party platform integration
SMART LIGHTING
ONE-STOP SOLUTION
Support all mainstream wireless connectivity protocols
Global deployment
Rich in control and automation functionalities

ring

Dangerous Toys

- USB Device Impersonators
- USB Killers
- Man in the Middle Faceplates
- Wireless Pineapples
- Payload Phone Chargers

Dangerous Toys

- USB Device Impersonators
- USB Killers
- Man in the Middle Faceplates
- Wireless Pineapples
- Payload Phone Chargers

ebay Shop by category | Search for anything | All Categories | Search | Advanced

eBay › Computers/Tablets & Networking › Other Computers & Networking

Share

USB Rubber Ducky Payload Deployer HID Emulator Hack Injector Metal(KEY + MOUSE!)

$16.31
+ $2.21 Shipping

ebay MONEY BACK GUARANTEE

Qty : 1

Buy It Now

Add to cart

or Best Offer

Make Offer

Watch

Get it by **Thu, Dec 5 - Tue, Dec 31** from Shanghai, China

- **New** condition
- 30 day returns - Buyer pays return shipping

"We recommand Dckuino.js by Seytonic. USB Rubber Ducky Tutorial. Normal Rubber Duckies can inject only Keyboard Strokes. Our model can inject Keyboard…"

Read full description

See details

Sold by
nicuo (256)
100.0% Positive feedback
Contact seller

Dangerous Toys

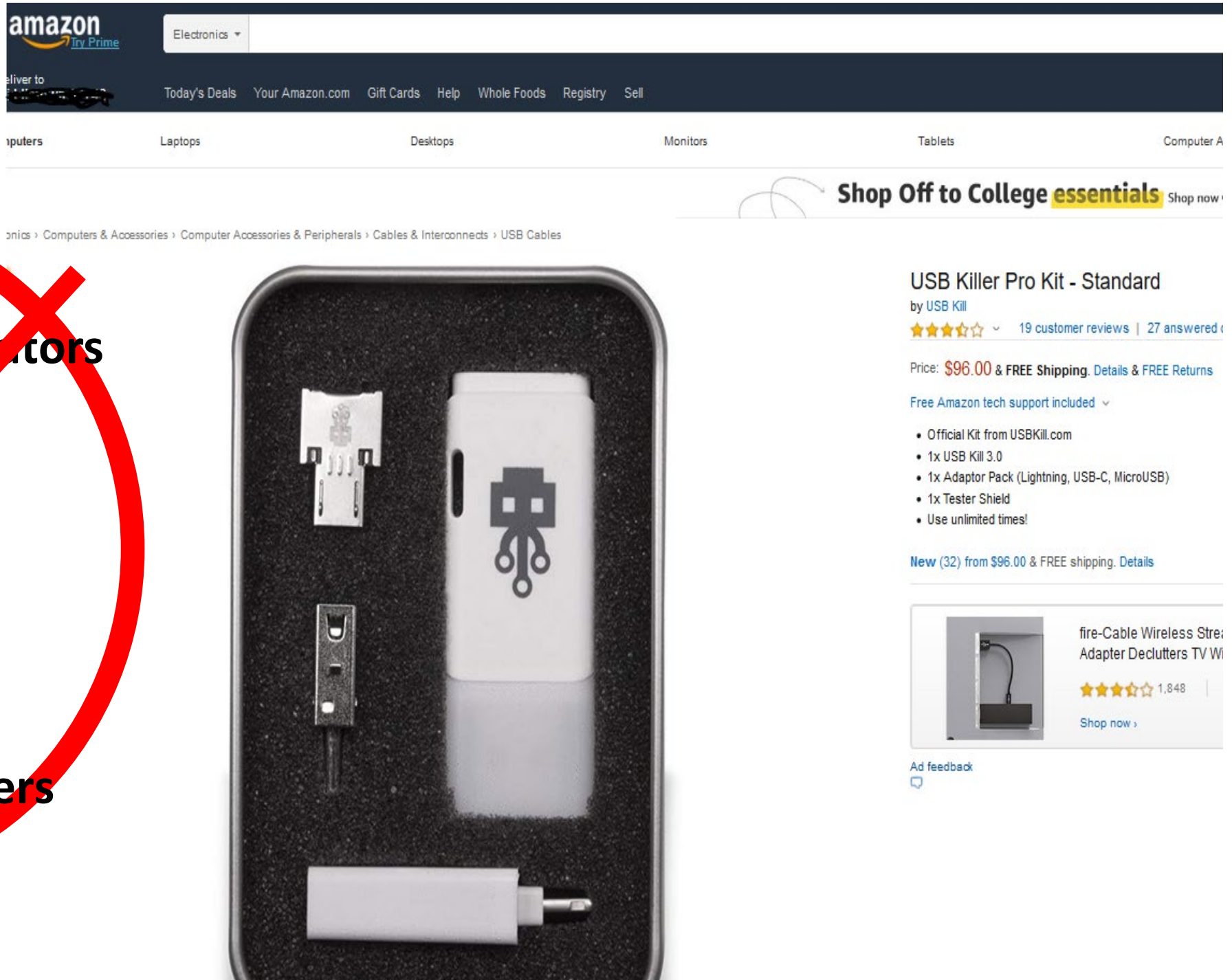
USB Device Impersonators

USB Killers

Man in the Middle Faceplates

Wireless Pineapples

Payload Phone Chargers



Dangerous Toys

- USB Device Impersonators
- USB Killers
- Man in the Middle Faceplates
- Wireless Pineapples
- Payload Phone Chargers

Wifi Pineapple Wireless Network Wifipineapple Wireless Security

$75.99 from eBay - chunyu1991_1

NOTE: The version of the **wireless** security auditing device wifipineapple sixth generation

Wifi Pineapple Wireless Network Wifipineapple Wireless Security

$75.09 from eBay

WiFi Pineapple Wireless Network wifipineapple **wireless** security auditing hak5 Descrip

Wireless · USB · Wi-Fi

Wifi Pineapple Wireless Network Security Audit Wireless Wifi Security

$62.69 from eBay - xiaof12

Please do not upgrade the new system firmware. If there is any problem, please brush bac

Wireless · 802.11n · 802.11g · 802.11b · USB · PC · Wi-Fi

Lusya WiFi Pineapple Wireless Network Security Audit Wireless WIFI

$83.44 from AliExpress.com

in from on AliExpress.com | Alibaba Group

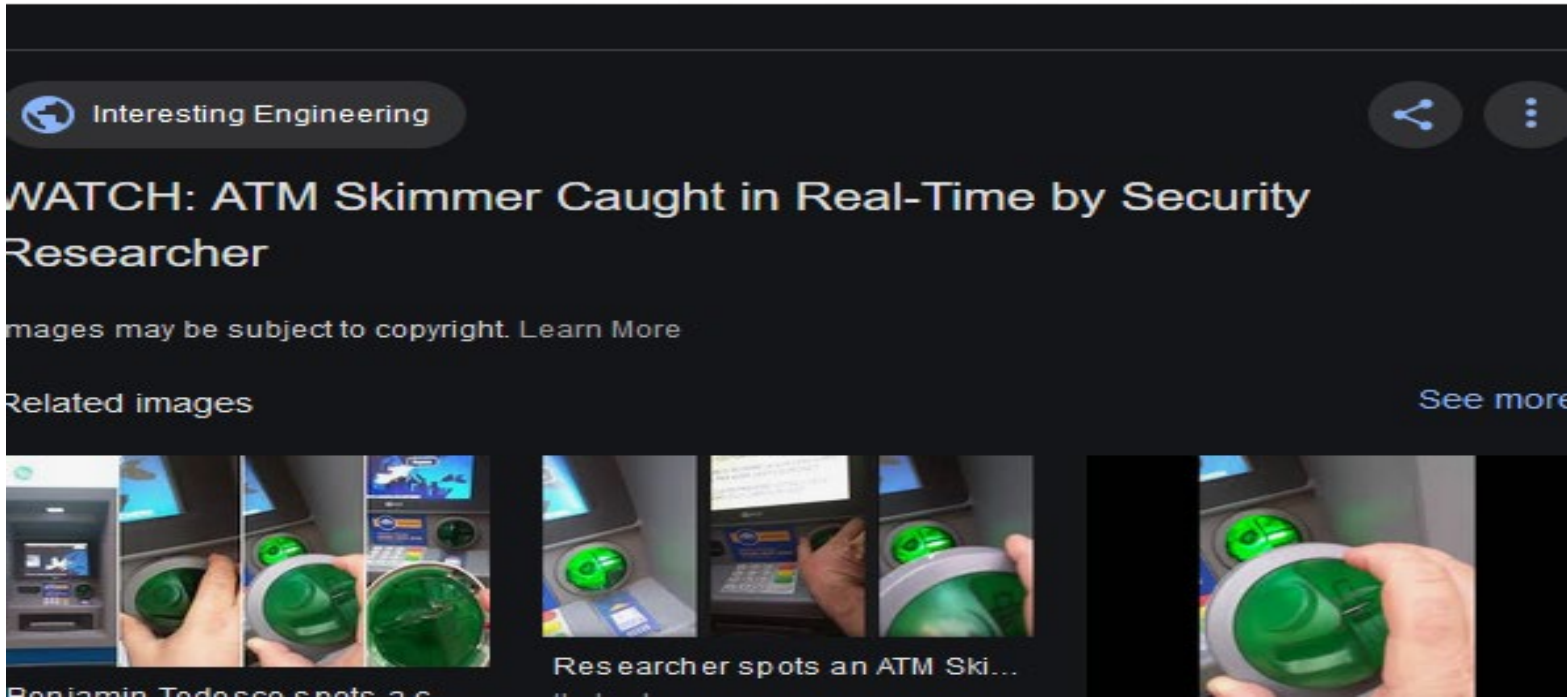
With Wi-Fi · Wireless

Dangerous Toys

- USB Device Impersonators
- USB Killers
- Man in the Middle Faceplates
- Wireless Pineapples
- Payload Phone Chargers

Dangerous Toys

- USB Device Impersonators
- USB Killers
- Man in the Middle Faceplates
- Wireless Pineapples
- Payload Phone Chargers



Airtag and GPS Trackers

Waterproof Apple AirTag Magnet...

Cube Bluetooth Smart Tracker

https://censys.io Internet of Things

FTP and Telnet Sites North Carolina US

66.207.227.71 (pode.intrstar.net)
STARWIRELESS-15153 - StarVision, Inc. (15153) Dunn, North Carolina, United States
21/ftp, 23/telnet
location.province: `North Carolina`

152.13.178.2 (CAM225DSJ1300.uncg.edu)
UNC-GREENSBORO - University of North Carolina at Greensboro (53785) Greensboro, North Carolina, United States
21/ftp, 23/telnet, 443/https, 80/http
HP Designjet 36B634A0
tags: `ftp`

198.85.198.4
NCREN - MCNC (81) Albemarle, North Carolina, United States
21/ftp, 23/telnet
21.ftp.banner.banner: `220 Welcome to the Valere FTP server.`

152.20.39.207
NCREN - MCNC (81) Wilmington, North Carolina, United States
21/ftp, 23/telnet
21.ftp.banner.banner: `220 FTP print`

98.26.91.139 (cpe-98-26-91-139.nc.res.rr.com)
TWC-11426-CAROLINAS - Charter Communications Inc (11426) Durham, North Carolina, United States
21/ftp, 23/telnet

location.country_code: US and tags: scada

64.19.73.45 (45-73-19-64-wtn-ny.a-315.westelcom.com)
WFC-ASN - Westelcom Internet, Inc. (11722) Watertown, New York, United States
Schneider Electric BMX P34 2020 v2.0 502/modbus
tags: `scada` `gateway`
SCADA SCADA GATEWAY

66.44.215.170 (170.subnet-66-44-215.ellijay.com)
ELJY30540 - Ellijay Telephone Company (25853) Blue Ridge, Georgia, United States
Schneider Electric BMX NOE 0100 V2.80 502/modbus
tags: `scada` `gateway`
SCADA SCADA GATEWAY

162.155.7.242 (rrcs-162-155-7-242.central.biz.rr.com)
TWC-10796-MIDWEST - Charter Communications Inc (10796) Strongsville, Ohio, United States
Schneider Electric BMX P34 2020 v2.5 502/modbus
tags: `scada` `gateway`
SCADA SCADA GATEWAY

166.250.100.120 (120.sub-166-250-100.myvzw.com)
CELLCO - Cellco Partnership DBA Verizon Wireless (22394) United States
Schneider Electric BMX P34 2020 v2.6 502/modbus
tags: `scada` `gateway`
SCADA SCADA GATEWAY

https://shodan.io Internet of Things

Jo-ann Stores, LLC
Added on 2019-08-01 12:53:58 GMT
United States, Stow

166.215.52.198
mobile-166-215-52-198.mycingular.net
AT&T Wireless
Added on 2019-08-01 12:43:45 GMT
United States

```
Basic Hardware: 6ES7 212-1BE31-0XB0  v.0.2
Module: 6ES7 212-1BE31-0XB0  v.0.2
Basic Firmware: 6ES7 212-1BE31-0XB0  v.3.0.2
```

ics

209.201.40.202
209-201-40-202.dia.static.centurylink.net
CenturyLink
Added on 2019-08-01 12:44:05 GMT
United States, Logan

```
HTTP/1.1 400 Bad Request\r\nContent-Type: text/html; charset=us-ascii\r\nServer: Microsoft-HTTPAPI/2.0\r\nDate: Tl
\n<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">\r\n<HTML><HEAD...
```

67.141.196.22
h22.196.141.67.static.ip.windstream.net
Windstream Communications
Added on 2019-08-01 12:50:53 GMT
United States, Cornelius

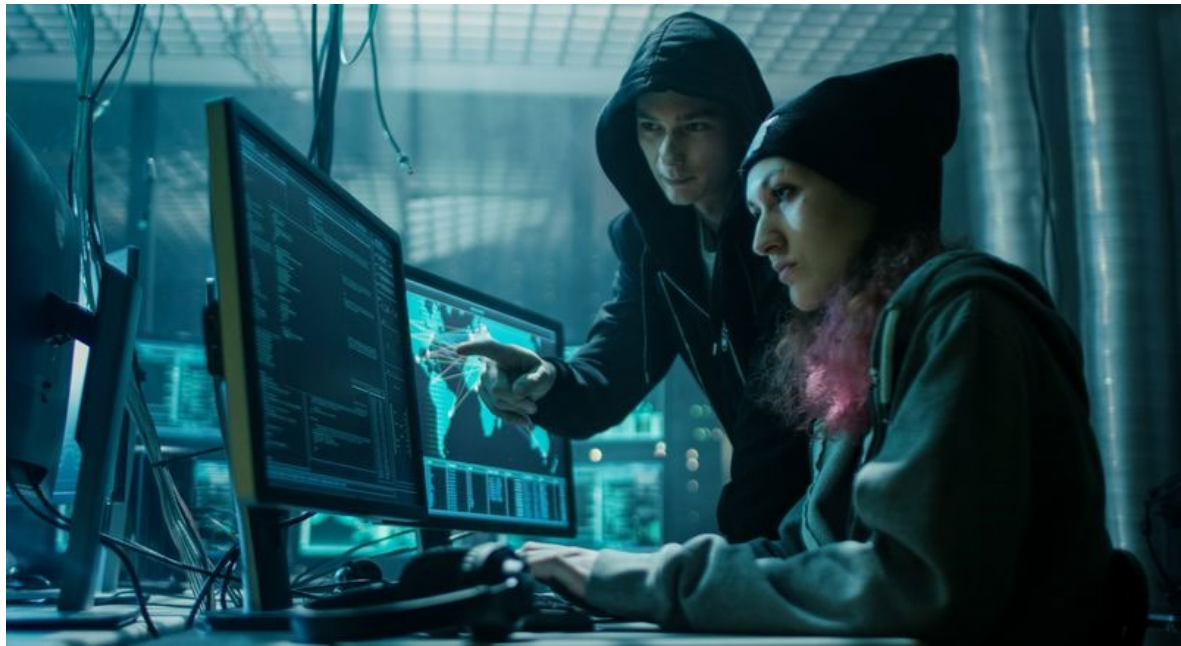
```
Basic Hardware: 6ES7 215-1HG31-0XB0  v.0.1
Module: 6ES7 215-1HG31-0XB0  v.0.1
Basic Firmware: 6ES7 215-1HG31-0XB0  v.3.0.2
```

ics

165.227.224.226
Digital Ocean
Added on 2019-08-01 12:45:03 GMT
United States, New York

honeypot cloud

```
Location designation of a module:
Copyright: Operation
Module type: IM151-8 PN/DP CPU
PLC name: Technodrome
Module: v.0.0
Plant identification: Mouser Factory
OEM ID of a module:
Module name: Operation
Serial number of module: 88111222
```



Cost of a Data Breach 2022 Report

$9.44M

US average cost of a data breach (global $4.35M)

Top 3 cost amplifying factors

1. Compliance failures
2. System complexity
3. Cloud migration

Top 3 cost mitigating factors

1. AI platforms
2. Encryption
3. Analytics

45%
Breaches Cloud-based

$1M
Cost increase where remote work was a factor in the breach

$387 million
Average total cost of a breach of >50M records

$3.05 million
Cost savings due to security AI and automation

$180
Cost per record for compromised customer PII

19%
Share of breaches caused by compromised credentials

Time to identify and contain

Global average: 277 days ($1.1M savings under 200 Days)

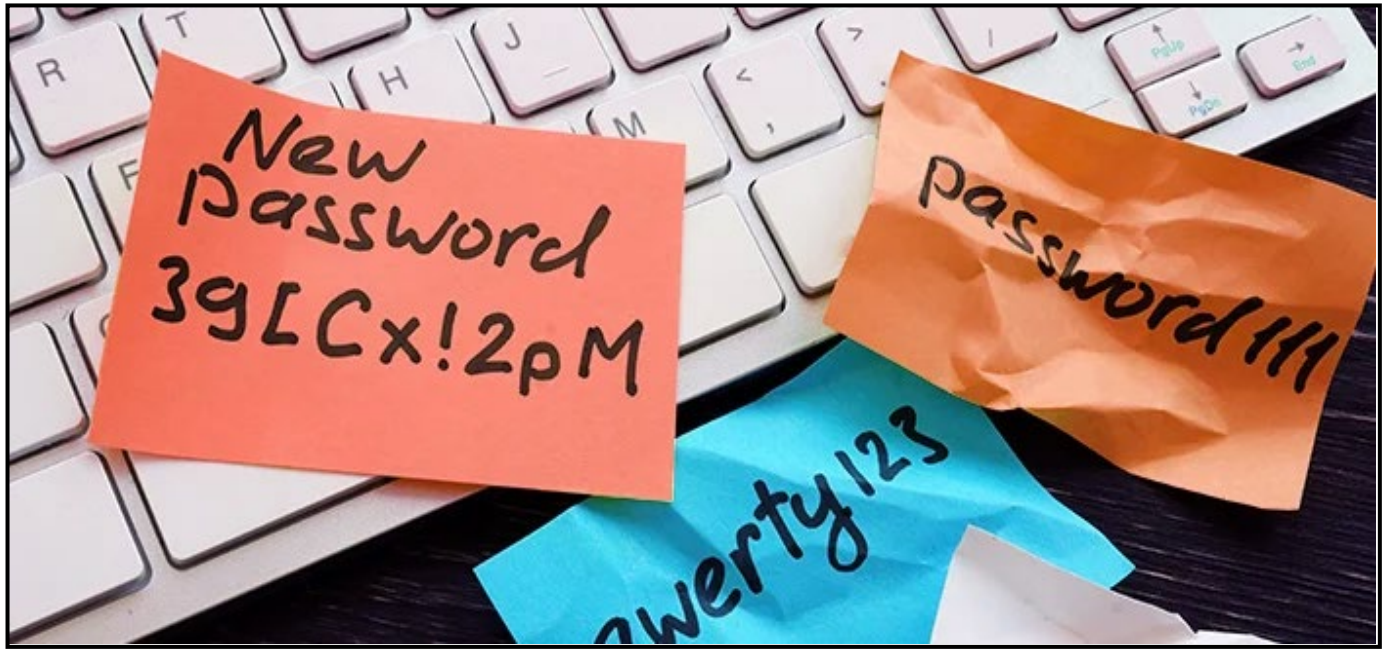
74 Days Less with Security AI and Automation

29 Days Less withExtended Detection and Response (XDR)

$2.66 million ⬇
Average cost savings with incident response teams and IR testing vs. no IR teams or testing

Passwords like Promises

Never meant to be broken



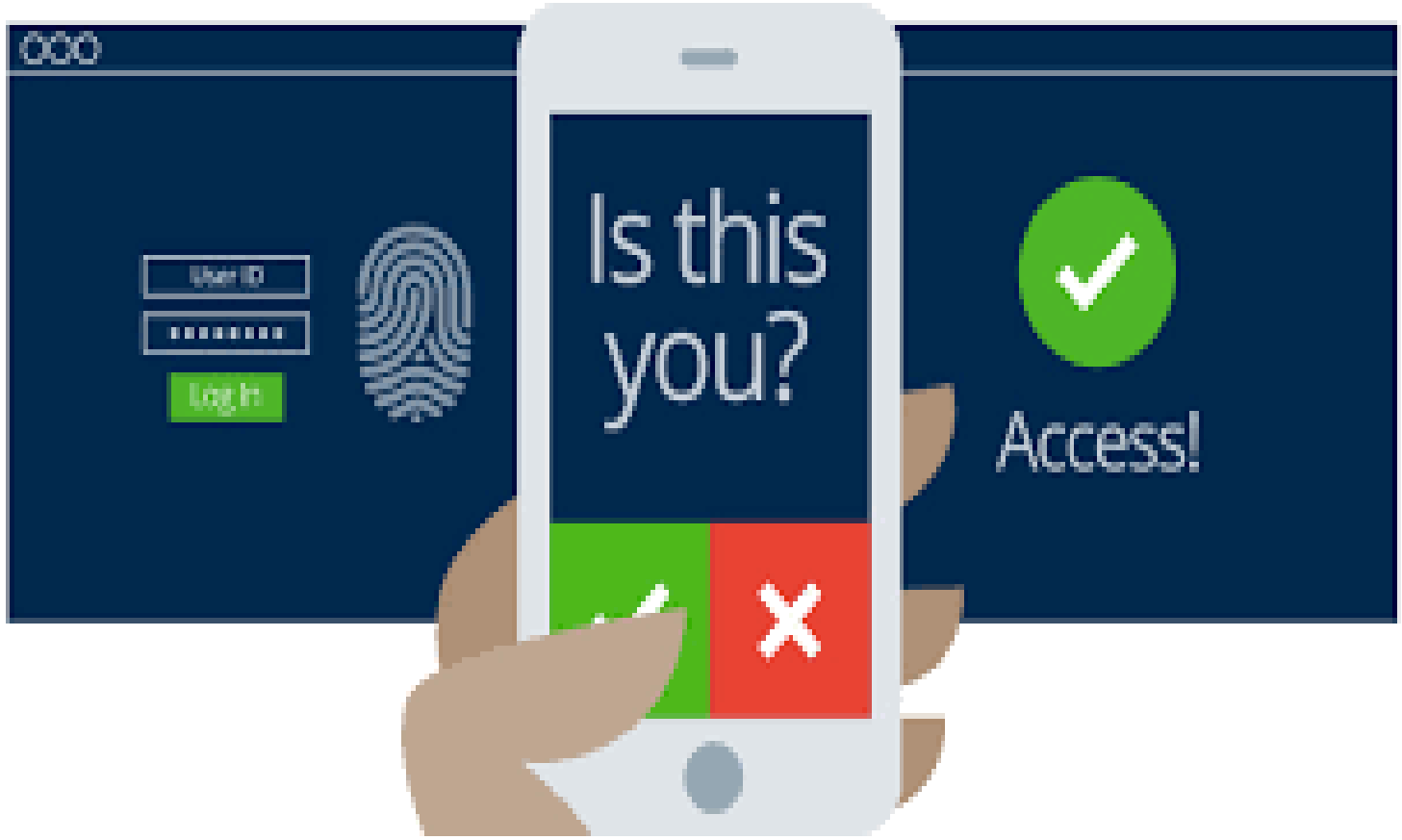
Password = Something I know?

Password Vault

Multi-Factor Authentication:

Great unless you're already compromised

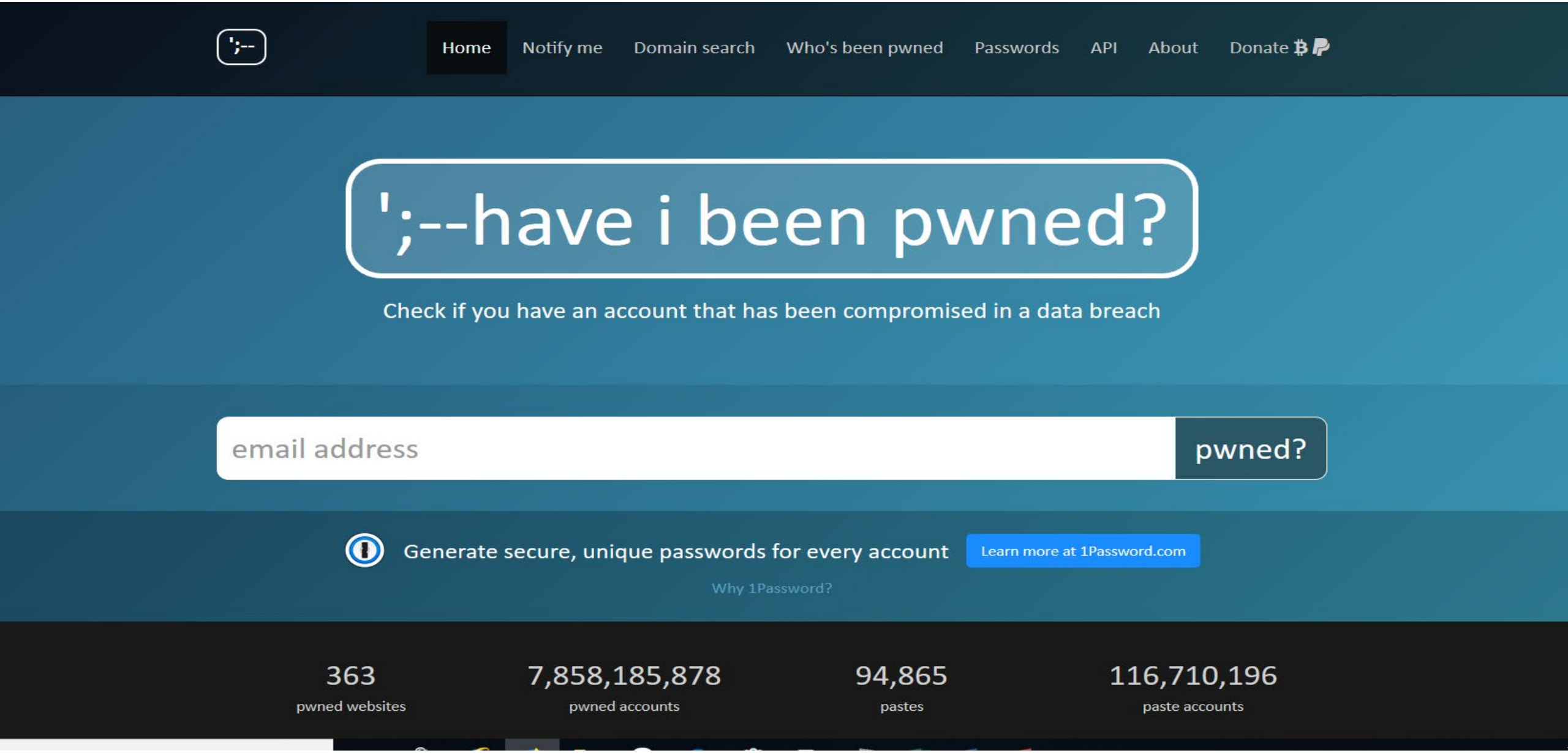
- **Something I know, Something I am, Something I have**



Share, Share, That's Fair!

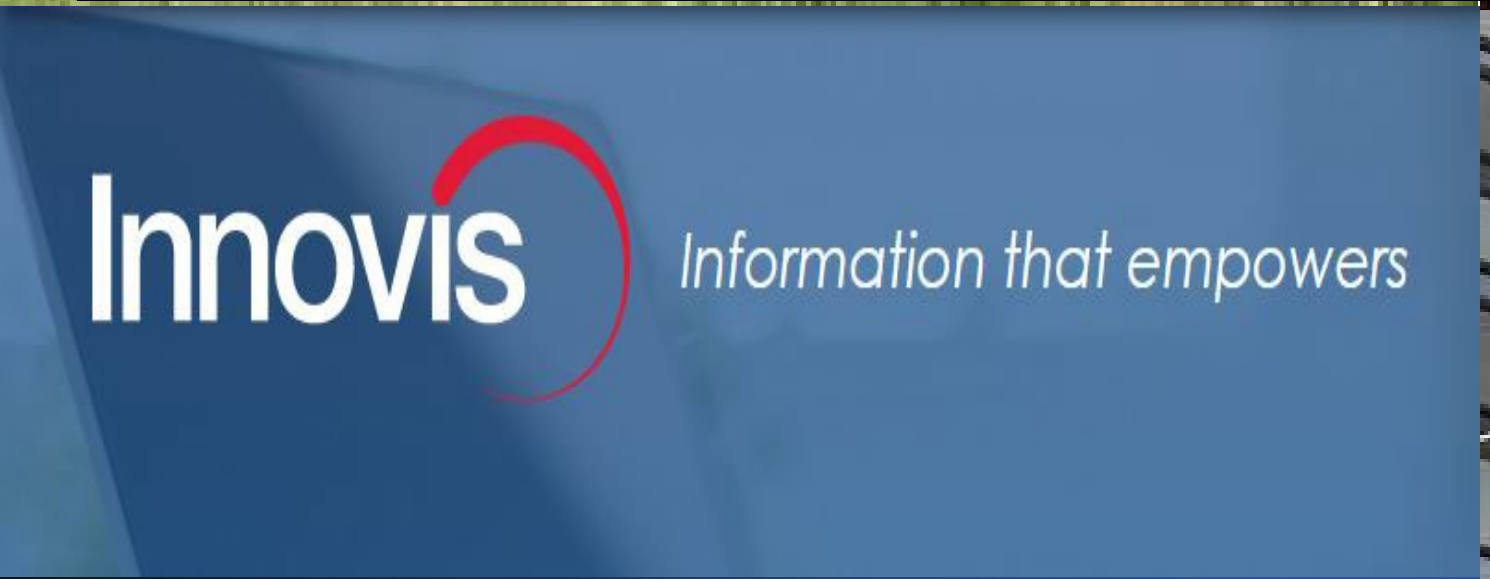
hmm?

https://haveibeenpwned.com



Adaptive Authentication/Access

Nationwide Credit Reporting Agencies



Lockdown Your Credit Reporting

- https://www.equifax.com/
- https://www.experian.com/
- https://www.transunion.com/
- https://Innovis.com/

Social <engineering> Dilemma

Michael Melore, CISSP
IBM Public Sector Cybersecurity Ambassador
& Senior Cybersecurity Advisor
Co-Founder SecRT (Security <Leaders> Round Table)
www.SecRT.us