Reliable IT Healthcare

Doing IT Right!

Doing Security Right!

Security is No Longer an Option

Or Start Planning for Downtime

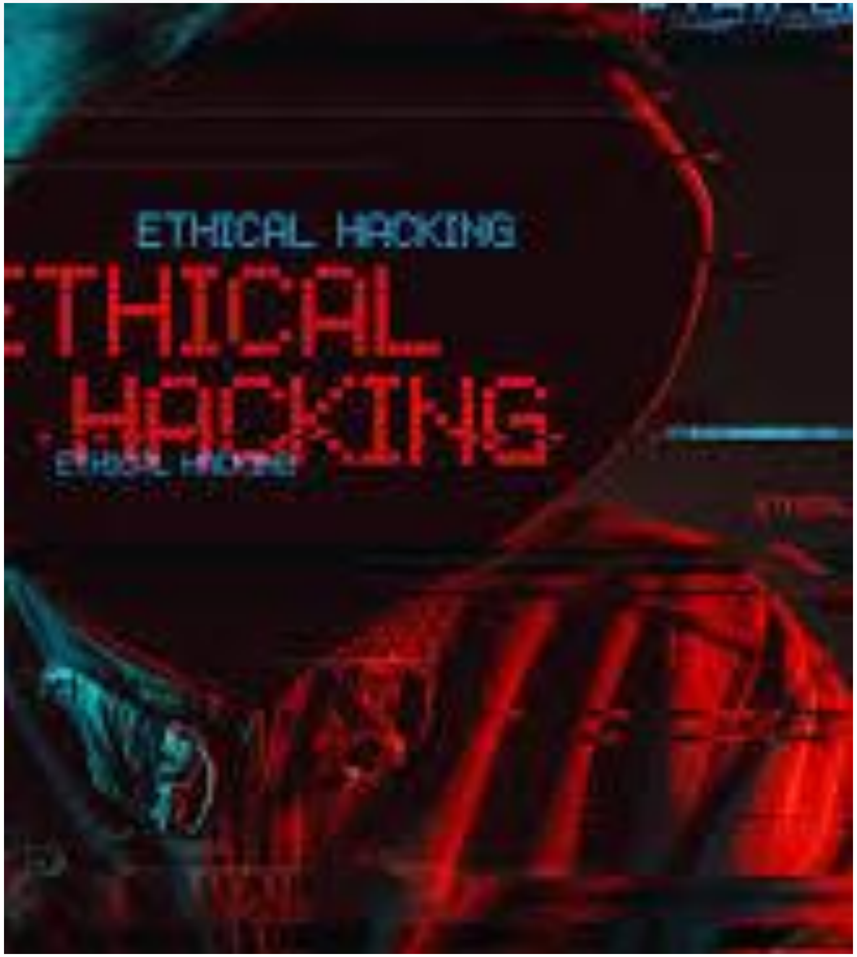
State of the Union

- Security Risk Assessments that work
- Defending against Ransomware Attacks
- Disaster Recovery and Business Continuity – the silent issue
- Logging and Identification Tools

Security Risk Assessments

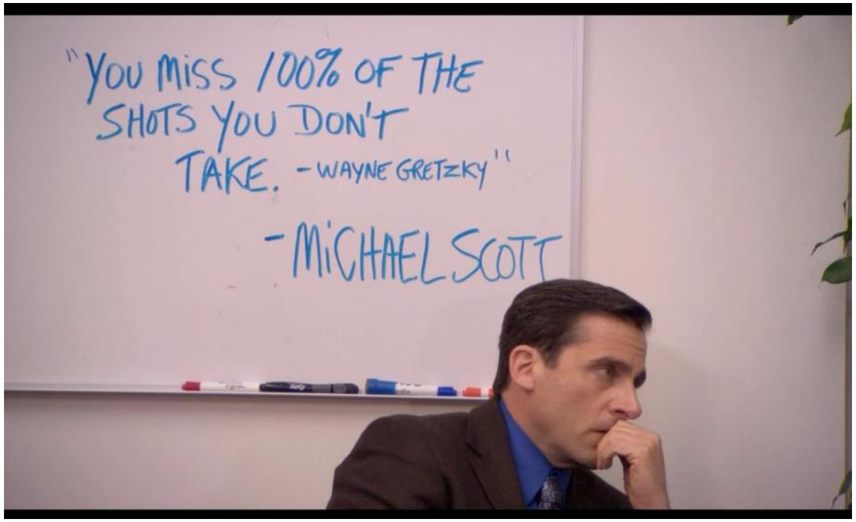
Security Risk Assessments

- Make sure you are doing them every year with an outside firm.
- Make sure your Assessment includes a Penetration Test. - Ethical Hacking
- Implement a Security Awareness Program and HIPAA Compliance Plan



Security Risk Assessments

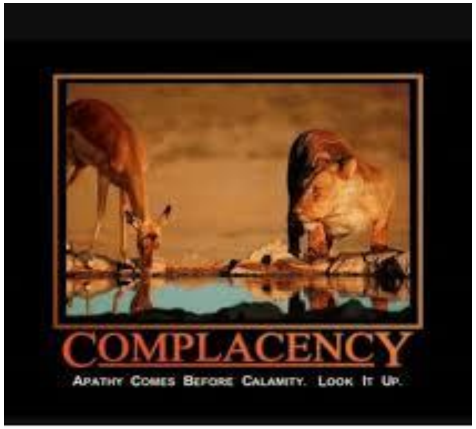
- Biggest Issue we see with Assessments
  - Compliancy and Non-Action


"YOU MISS 100% OF THE SHOTS YOU DON'T TAKE. - WAYNE GRETZKY"
- MICHAEL SCOTT

Security Risk Assessments

- Biggest Issue we see with Assessments
  - We have been able to breach 50% of the clients that we have done Risk Assessments for in 2019

OVERCONFIDENCE
This is going to end in disaster, and you have no one to blame but yourself.

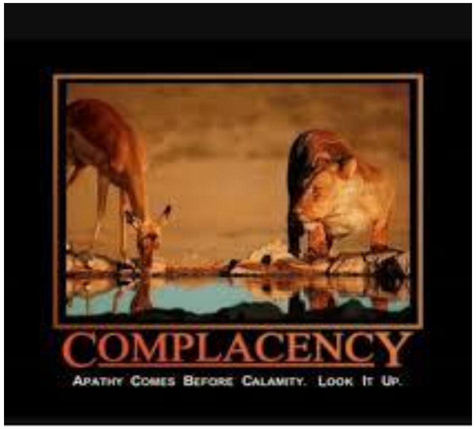


Complacency vs Contentment

Security Risk Assessments

- Biggest Issue we see with Assessments
  - We have been able to breach 80% of the clients that we have done Risk Assessments for in 2020

OVERCONFIDENCE
This is going to end in disaster, and you have no one to blame but yourself.



Complacency vs Contentment

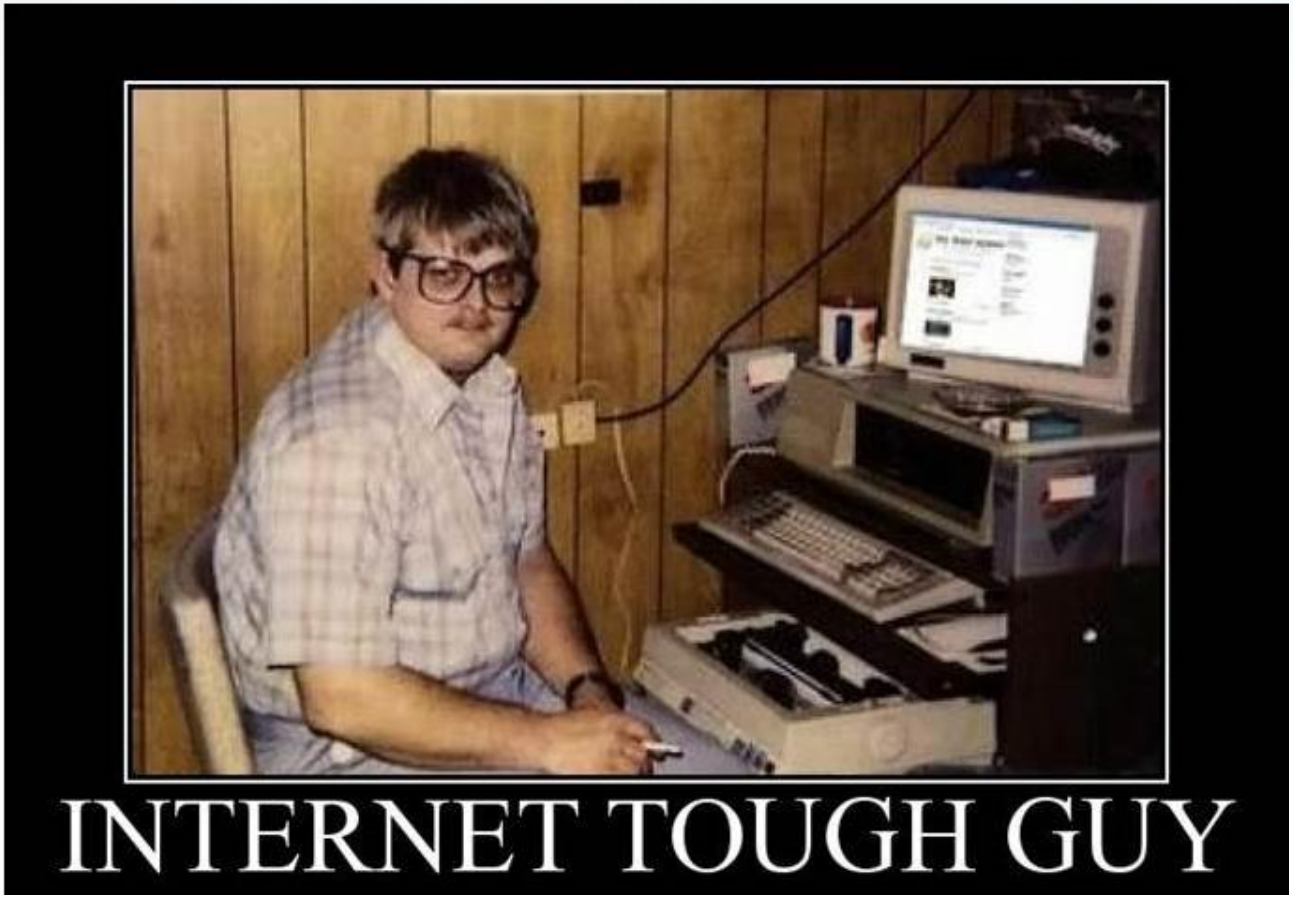
Ransomware

Ransomware

YOUR FILES HAVE BEEN ENCRYPTED!!
READ THE README FILE ON YOUR DESKTOP

Ransomware and its changing strategies

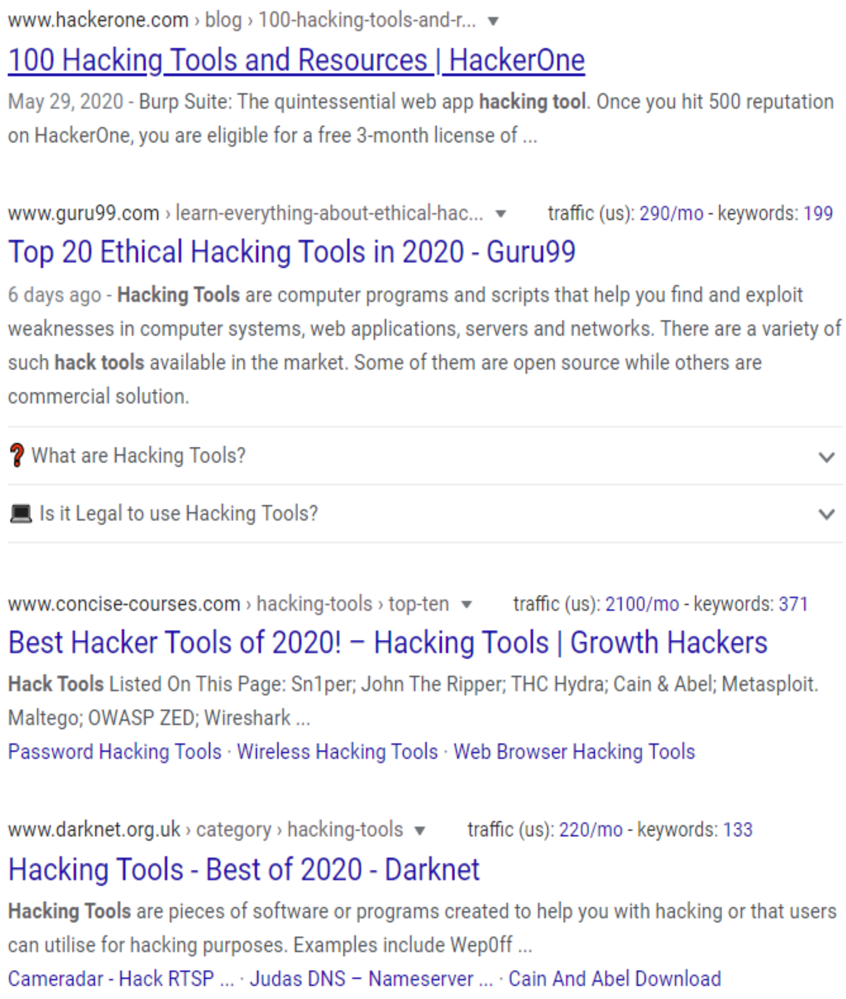
- Exfiltrate data, then encrypt (using better encryption than in the past):
  - Maze–adds ransoming to prevent leaking private data (Xerox).
  - ProLock –ransom to prevent leaking private data.
- RDoS (Ransom Denial of Service):
  - Claiming to be Fancy Bear, demanding payment in bitcoin.
- Other industries' attacks – attacking Availability of systems:
  - Garmin – Pilot and InReach services taken down, life-threatening.
  - Honda – forced to shut down factories in several countries.
- Attacks are on the rise, are more targeted, recovery costs increasing.


INTERNET TOUGH GUY

Ransomware

YOU KNOW WHAT THEY SAY. "FOOL ME ONCE,
STRIKE ONE, BUT FOOL ME TWICE... STRIKE THREE."

Google Search



www.hackerone.com › blog › 100-hacking-tools-and-r... ▾

100 Hacking Tools and Resources | HackerOne

May 29, 2020 - Burp Suite: The quintessential web app **hacking tool**. Once you hit 500 reputation on HackerOne, you are eligible for a free 3-month license of ...

www.guru99.com › learn-everything-about-ethical-hac... ▾ traffic (us): 290/mo - keywords: 199

Top 20 Ethical Hacking Tools in 2020 - Guru99

6 days ago - **Hacking Tools** are computer programs and scripts that help you find and exploit weaknesses in computer systems, web applications, servers and networks. There are a variety of such **hack tools** available in the market. Some of them are open source while others are commercial solution.

❓ What are Hacking Tools? ⌄

💻 Is it Legal to use Hacking Tools? ⌄

www.concise-courses.com › hacking-tools › top-ten ▾ traffic (us): 2100/mo - keywords: 371

Best Hacker Tools of 2020! – Hacking Tools | Growth Hackers

Hack Tools Listed On This Page: Sn1per; John The Ripper; THC Hydra; Cain & Abel; Metasploit. Maltego; OWASP ZED; Wireshark ...

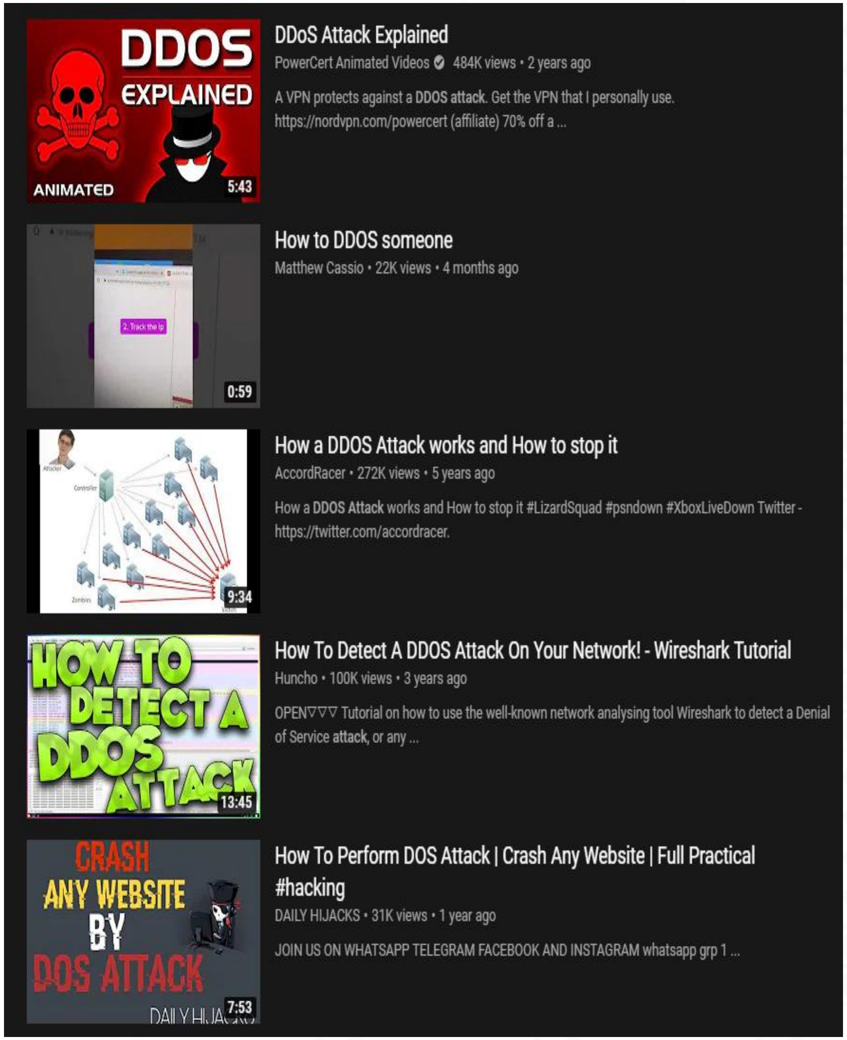
Password Hacking Tools · Wireless Hacking Tools · Web Browser Hacking Tools

www.darknet.org.uk › category › hacking-tools ▾ traffic (us): 220/mo - keywords: 133

Hacking Tools - Best of 2020 - Darknet

Hacking Tools are pieces of software or programs created to help you with hacking or that users can utilise for hacking purposes. Examples include Wep0ff ...

Cameradar - Hack RTSP ... · Judas DNS – Nameserver ... · Cain And Abel Download



DDoS Attack Explained

PowerCert Animated Videos ✓ 484K views • 2 years ago

A VPN protects against a **DDOS attack**. Get the VPN that I personally use. https://nordvpn.com/powercert (affiliate) 70% off a ...

How to DDOS someone

Matthew Cassio • 22K views • 4 months ago

How a DDOS Attack works and How to stop it

AccordRacer • 272K views • 5 years ago

How a **DDOS Attack** works and How to stop it #LizardSquad #psndown #XboxLiveDown Twitter - https://twitter.com/accordracer.

How To Detect A DDOS Attack On Your Network! - Wireshark Tutorial

Huncho • 100K views • 3 years ago

OPEN▽▽▽ Tutorial on how to use the well-known network analysing tool Wireshark to detect a Denial of Service **attack**, or any ...

How To Perform DOS Attack | Crash Any Website | Full Practical #hacking

DAILY HIJACKS • 31K views • 1 year ago

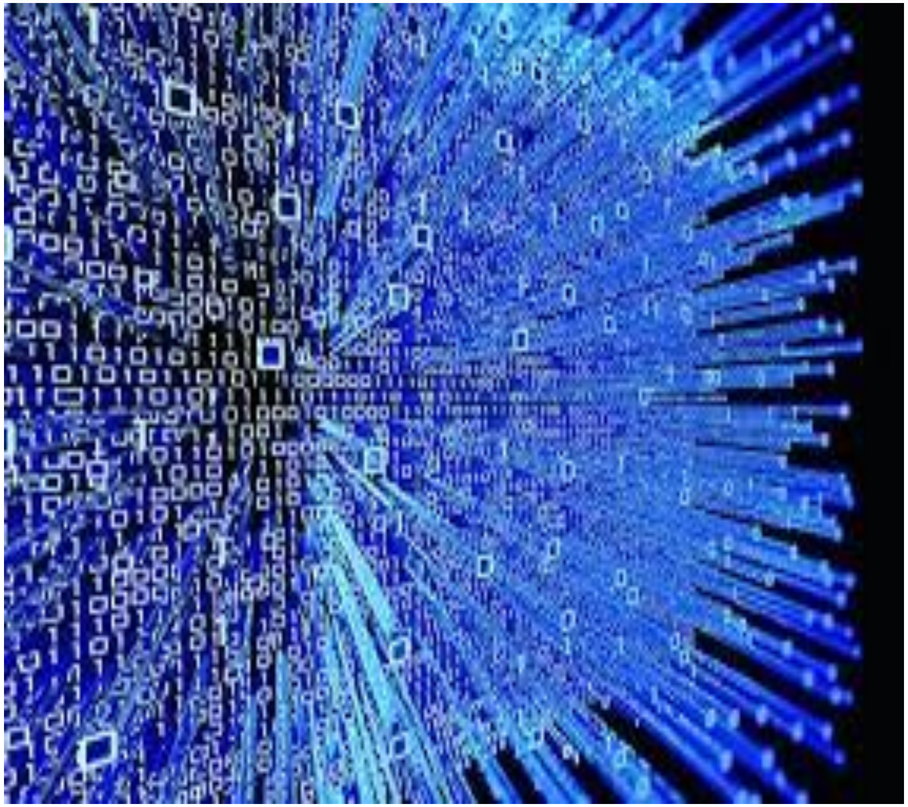
JOIN US ON WHATSAPP TELEGRAM FACEBOOK AND INSTAGRAM whatsapp grp 1 ...

Disaster Recovery and Business Continuity – the silent issue

Disaster Recovery and Business Continuity – the silent issue

WE LOST ALL OF OUR COMPANY DATA AND OUR BACKUPS, TOO.
Dilbert.com DilbertCartoonist@gmail.com
SO I HACKED INTO OUR GOVERNMENT'S SECRET DATABASE WHERE THEY KEEP RECORDS OF EVERYTHING WE SAY OR DO AND GOT IT ALL BACK.
©2013 Scott Adams, Inc.
I FEEL AS IF I SHOULD BE DOING SOMETHING NOW.
NAH. EVERYTHING IS WORKING FINE.

Disaster Recovery and Business Continuity – the silent issue



Security in Medical Practices

Data Centers

Data Centers

I CHANGED ALL MY PASSWORDS TO "INCORRECT".
SO WHENEVER I FORGET, IT WILL TELL ME "YOUR PASSWORD IS INCORRECT."
quickmeme.com

I WON'T BE IMPRESSED WITH TECHNOLOGY
UNTIL I CAN DOWNLOAD A BEER

Medical Practice

- Issues: Physician group was concerned with the amount of Phishing attacks they been getting and wonder if they have been compromised?
- Issues: How do they know for sure?

Requirements

- Restrict Access to PHI
- Monitor how PHI is communicated
- Ensure the integrity of PHI in Transit
- Ensure the integrity of PHI at rest
- Ensure 100% message accountability
- Two Factor
- Encryption

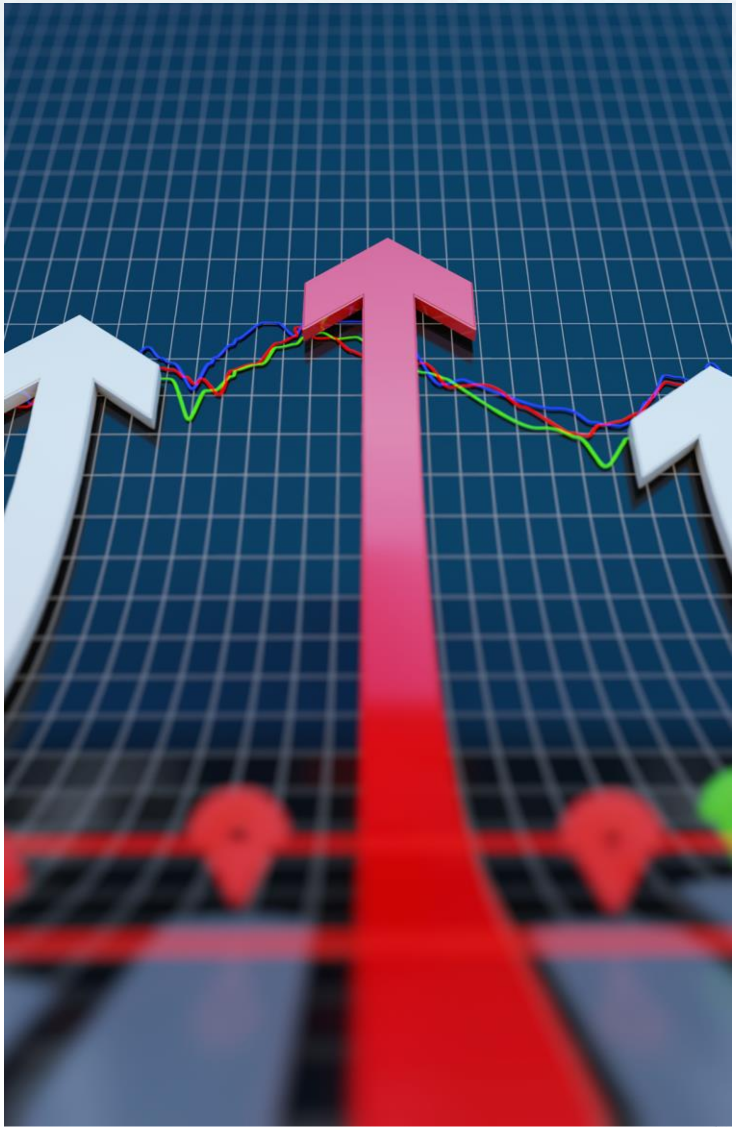
Microsoft365

Logging and Identification

5 Layers of Defense

- ✓ Using Microsoft Security Tools

- ✓ Microsoft Security Tools
- ✓ Microsoft Secure Score
- ✓ Microsoft Security Center
- ✓ Microsoft SIEM and XDR
- ✓ Microsoft Compliance



5 Layers of Defense

- 1st Layer of Defense
  - Spam Filtering w/AV
  - Antivirus
  - Security Awareness Training, Dark Web Scan, Phishing
  - Identity Management - 2FA
  - Onsite Backup
- 2nd Layer of Defense –BAMP
  - Backup (Ransomware Proof)
  - Antivirus (Artificial Intelligence AV Driven Tool – Ransomware Proof)
  - Monitoring
  - Patch Management
- 3rd Layer of Defense –SIEM
  - Security Information Event Management (SIEM) and/or Threat Detector
  - Managed FW with IDS/IPS and Web Filtering
- 4th Layer of Defense – Test and Assess
  - Yearly Security Risk Assessment w/ PEN Test
- 5th Layer of Defense
  - Business Continuity and Disaster Recovery Solution

5 Layers of Defense

- 1st Layer of Defense
  - Spam Filtering w/AV – Microsoft365
  - Antivirus - Webroot
  - Security Awareness Training, Dark Web Scan, Phishing - BreachSecureNow
  - Identity Management - 2FA – Microsoft365
  - Onsite Backup – Veeam or Kaseya
  - Security Policy’s -
- 2nd Line of Defense –BAMP
  - Backup (Ransomware Proof) - Kaseya
  - Antivirus (Artificial Intelligence AV Driven Tool) – Cylance or Deep Instinct
  - Monitoring – Kaseya, Lionguard, Auvik
  - Patch Management – Kaseya
- 3rd Line of Defense –SIEM
  - Security Information Event Management (SIEM) and/or Threat Detector – Netsurian and Microsoft365
  - Managed FW with IDS/IPS and Web Filtering - Fortinet
- 4th Line of Defense – Test and Assess
  - Yearly Security Risk Assessment w/ PEN Test – Security MSP
- 5th Line of Defense
  - Business Continuity and Disaster Recovery Solution – Microsoft Azure

Welcome to SKYNET

Q&A