CYBER74

CYBERSECRURITY AWARENESS FOR CONEGRATIONS

Agenda

- Meet the Speaker
- What is Cybersecurity?
- Cyber Threat Landscape
- What do we do?
- Wrap Up

Meet the Speaker

Tim Weber

- Certified as an Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH) and CMMC-AB Registered Practitioner.
- Over 30 years of IT and cybersecurity experience
- Contributor to regional and national publications, including New York Times and NPR
- Tim devotes time sharing his cybersecurity knowledge across the world, speaking at international industry events and conferences.

Tim Weber

VP of Channel Growth
Cyber74
Tweber@cyber74.com

What is cybersecurity?

Cybersecurity

Cybersecurity is the practice of deploying people, policies, processes and technologies to protect organizations, their critical systems and sensitive information from digital attacks.

Source: Gartner

Cybersecurity

~~Cybersecurity is the practice of deploying people, policies, processes and technologies to protect organizations, their critical systems and sensitive information from digital attacks.~~

Cybersecurity is the practice of managing risk. For most businesses, security is a cost center, so security only makes sense to the extent that it reduces business risk or saves money.

Cyber Threat Landscape

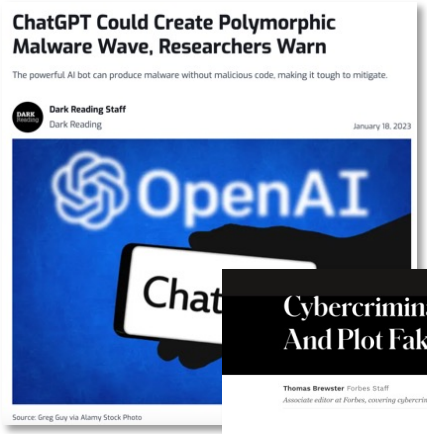
SMBs Are Targets

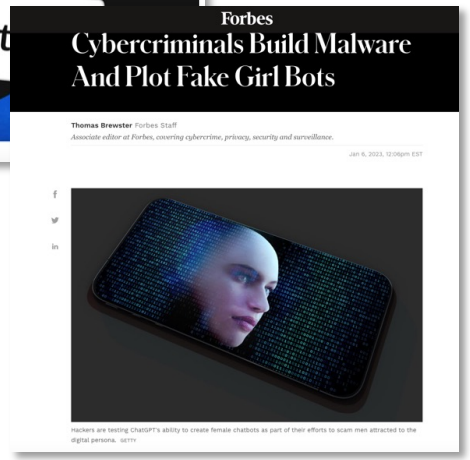
The gap between the number of breaches seen by small and large organizations has become much less pronounced over the past two years.

All organizations are being targeted by financially motivated organized crime actors !!

CYBER74

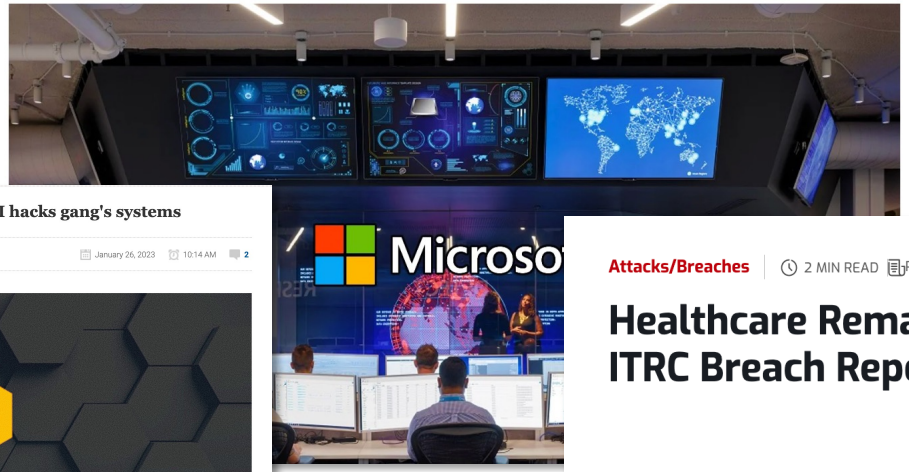
Current Landscape





Cybercrime Ecosystem Spawns Lucrative Underground Gig Economy Jan 30, 2023

The complex nature of cyberattacks has increased demand for software developers, reverse engineers, and offensive spe



Attacks/Breaches | 2 MIN READ | PRODUCTS & RELEASES

Healthcare Remains Top Target in 2022 ITRC Breach Report

January 25, 2023

NEW YORK, Jan. 25, 2023 /PRNewswire/ -- At least 344 organizations in the healthcare industry suffered data breaches in 2022, according to a just-released report from the Identity Theft Research Center® (ITRC). This is the third year in a row that healthcare organizations led all industries in the number of data compromises.

FBI Internet Crime Complaint Center (IC3)

FBI Internet Crime Report
https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf)

1. Business Email Compromise - Estimated at US $2.4 billion in losses
2. Cryptocurrency – Estimated at US $1.6 billion in losses
3. Ransomware - Estimated at US $49.2 million in losses

We Are Only Human

A person is involved at the center of most security events

- 82% of breaches result from human elements
- 66% of breaches involve phishing or stolen credentials
- 2.9% of employees may click on phishing emails

SMBs can significantly reduce their attack surface by focusing on controls to mitigate the likelihood of phishing techniques and stolen account credentials

- Adopt email filters and provide user training to combat phishing attacks
- Practice good password hygiene
- Use multi-factor authentication (MFA) everywhere

Source: Verizon 2022 Data Breach Investigations Report
https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf

What Do We Do?

Components of a Well-Designed Cybersecurity Solution for Your Business

Security Assessment

Security Awareness

Passwords

DNS Protection

Mobile Device Security

Advanced Endpoint Detection & Response

SIEM / Log Management

Dark Web Research

Backup

Computer Updates

Spam Email

Multi-Factor Authentication

Encryption

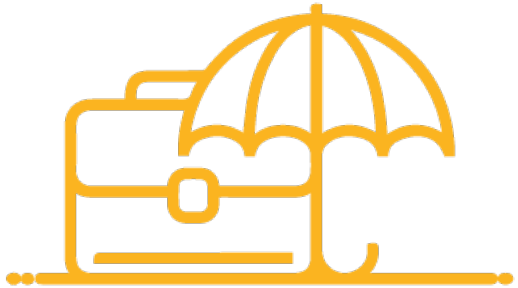
Firewall

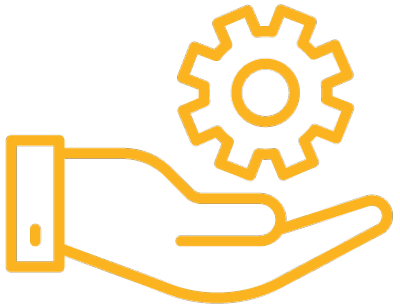
Cyber Insurance

Minimum Acceptable Technology

1. Incident response plan (Policy)
2. Multi-factor authentication
3. Endpoint Detection & Response (EDR -> MDR)
4. Security Incident & Event Mgmt. (SIEM)
5. Backups

- Cyber Security Assessment





An EDR is…*Endpoint Detection & Response*

How it works

- A EDR works by gathering and analyzing security related threat information on a workstation (an endpoint) to find security issues as they occur.
- When the EDR detects a threat, it can act quickly and isolate or even rollback to a known good state.

Why you need it

- Detects events on endpoints (file written, file executed, etc.)
- Responds to threats either automatically or with security team intervention
- Features built-in machine learning and behavioral analysis capabilities
- Allows cybersecurity experts to proactively threat hunt across endpoint devices
- Protects endpoints even if they are not on the network.

A SIEM is…
Security Information and Event Management

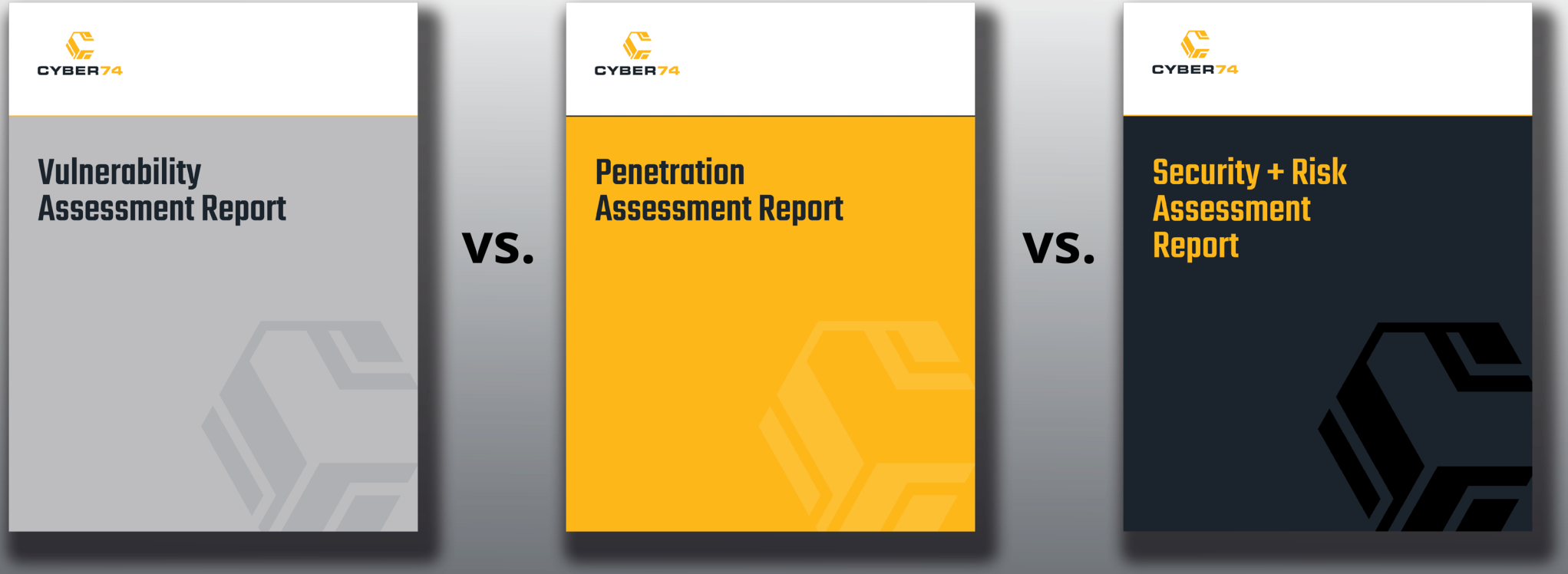
How it works

- A SIEM works by collecting log and event data generated by an organization's systems, devices, and applications and brings them into the centralized platform for analysis and reporting.
- When the SIEM identifies a threat through a set of predetermined rules, an alert is generated for human review.

Why you need it

- Full Visibility of Everything Happening within the network (including WFH)
- Dramatically Decreases the Time it Takes to Identify Threats
- Detailed Forensic Analysis in the Event of a Security Incident
- Auditing and Compliance Requirements

TYPES OF ASSESSMENTS



Q&A

GET IN TOUCH

If you have any questions or would like to discuss insights from this webinar in more detail, contact us below!

TWEBER@CYBER74.COM

CYBER74.COM

@CYBER74

@CYBER74TEAM

Thank You!