WorkED

# CYBERSECURITY VIRTUAL EXTERNSHIP

WorkED

# EXTERNSHIP OVERVIEW

## INSIGHTFUL INSTRUCTION

### WE WILL LEARN ABOUT:

- Threats to information security
- Motivations of hackers
- Effects of hacking and data security breaches
- Roles of industry professionals and law enforcement agencies
- Prevention and hardening techniques

## ENGAGING ACTIVITIES

### WE WILL PARTICIPATE IN:

- Knowledge practice games
- Team projects
- Peer discussion
- Simulated scenarios
- Competitive skills challenges

## INDUSTRY EXPOSURE

### WE WILL GAIN:

- Perspective from an industry professional
- Understanding of related careers and skills
- Public, private and personal vantage points
- Useful knowledge and skills that can be put into application

WorkED

# JOIN GOOGLE CLASSROOM
# CLASS CODE: yvbhyz5

Open a new tab in your web browser and navigate to **http://classroom.google.com**

**Log in** with your Google Account. If you don't have one, create one now.

Click the "**+**" icon near the top right-hand corner of the web page.

Click "**Join Class**", type the class code and click "**Join**".

WorkED

# EXTERNSHIP EXPECTATIONS

1. Arrive on time with camera enabled and microphone muted.
2. Participate from a quiet, comfortable place free of distractions.
3. Refrain from using electronic devices for non-relevant purposes.
4. Ask questions in text chat, or click the "raise hand" option to be called on.
5. Respond verbally when called upon communicating in complete sentences.
6. What to say instead of "I don't know":
    a. “Would you please repeat the question?”
    b. “May I have some more information?”
    c. “May I ask a friend?”
    d. “May I have some time to think?”
    e. “Where can I find more information?”

WorkED

# OPEN DAY-1 GUIDED NOTES

In our Google Classroom, click the “**Classwork**” tab at the top.

Click “**Day 1**” under “**Daily Materials**”.

Click “**View Assignment**”

Open the Day 1 Guided Notes Document

WorkED

# WHAT IS CYBERSECURITY?

It is the practice of **protecting** computer and their networks against **unwanted access** and the loss of data or theft.

Prevents **unwanted access to your information** in both personal and business use

Helps keep your files and data **secure and private**

Major **Job growth** over the next several years

Rapidly **evolving** industry

WorkED

# CHALLENGES OF CYBERSECURITY?

Technology is **always evolving**

You have **no idea when its coming** until you figure out its happening or it's already over

**Never** 100% secure

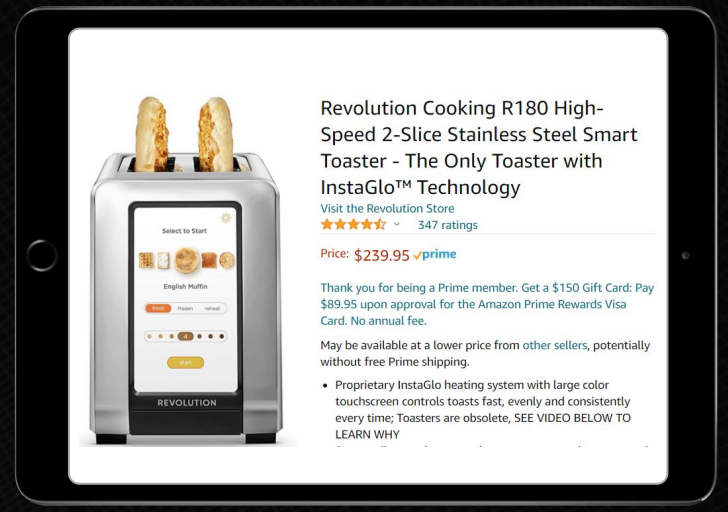
**Not enough people** to fill the jobs (estimated 3.5 million jobs)

Can be **expensive** and detailed

WorkED

# CHALLENGES CONT'D

# EMERGING TECHNOLOGIES




## DEVICES CONNECTED TO THE INTERNET - GIVING ACCESS TO THE NETWORK

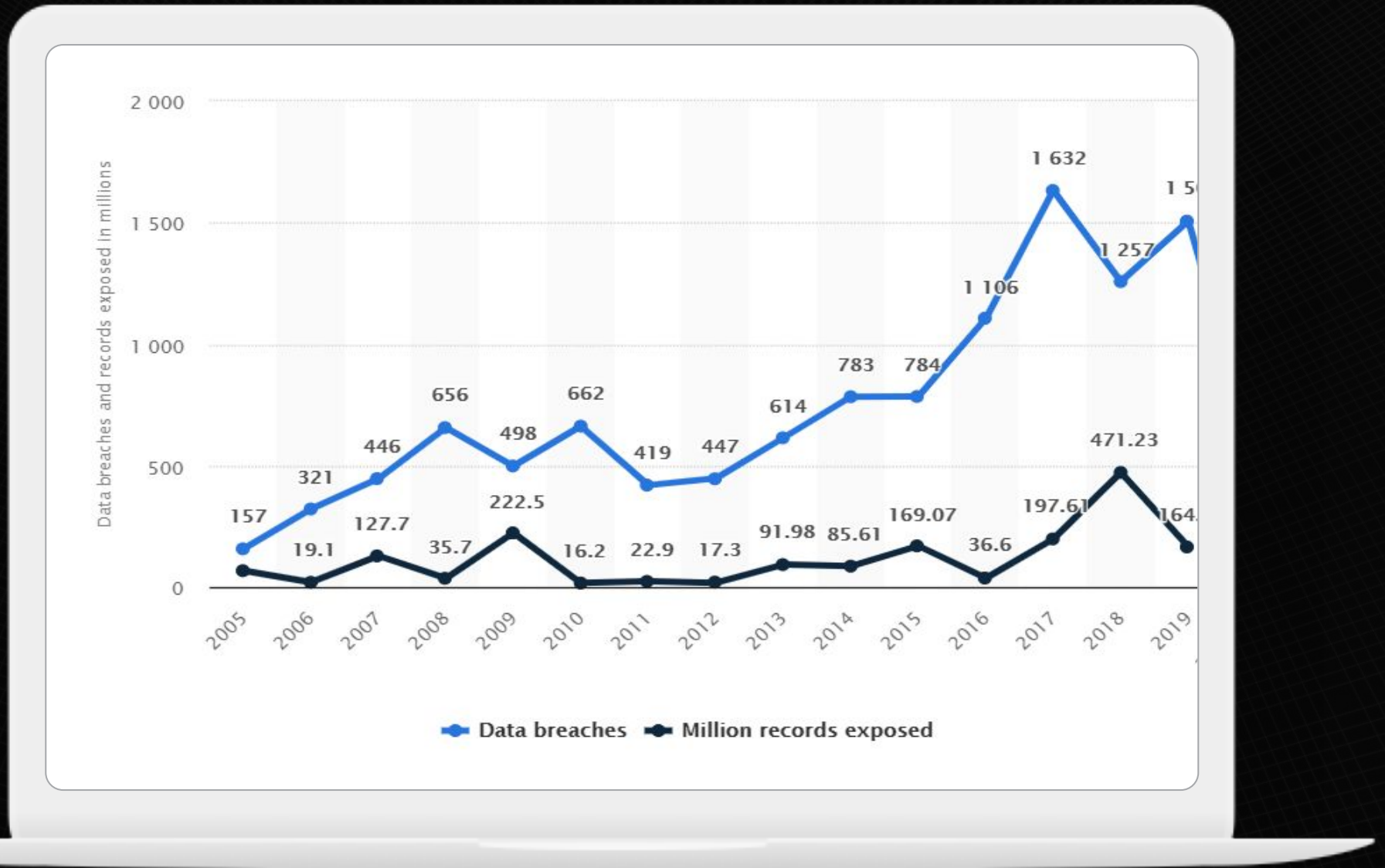
IOT - Internet of Things - Devices that are controlled from an app/Bluetooth or SmartThings

AI - Artificial Intelligence - wide-ranging branch of computer science concerned with building smart machines capable of performing tasks that typically require human intelligence

Cloud computing - the on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user. The term is generally used to describe data centers available to many users over the Internet

WorkED

# ATTACKS BY THE YEARS



WorkED

# EXPENSIVE CYBERSECURITY

**$500m**

2015- 1 bank **spent** over $500 million to fight cyber crime
(FORTUNE)

**$1t**

2017-2021 - An estimated $1 trillion **will be spent** on cybersecurity
(CYBERSECURITY VENTURES)

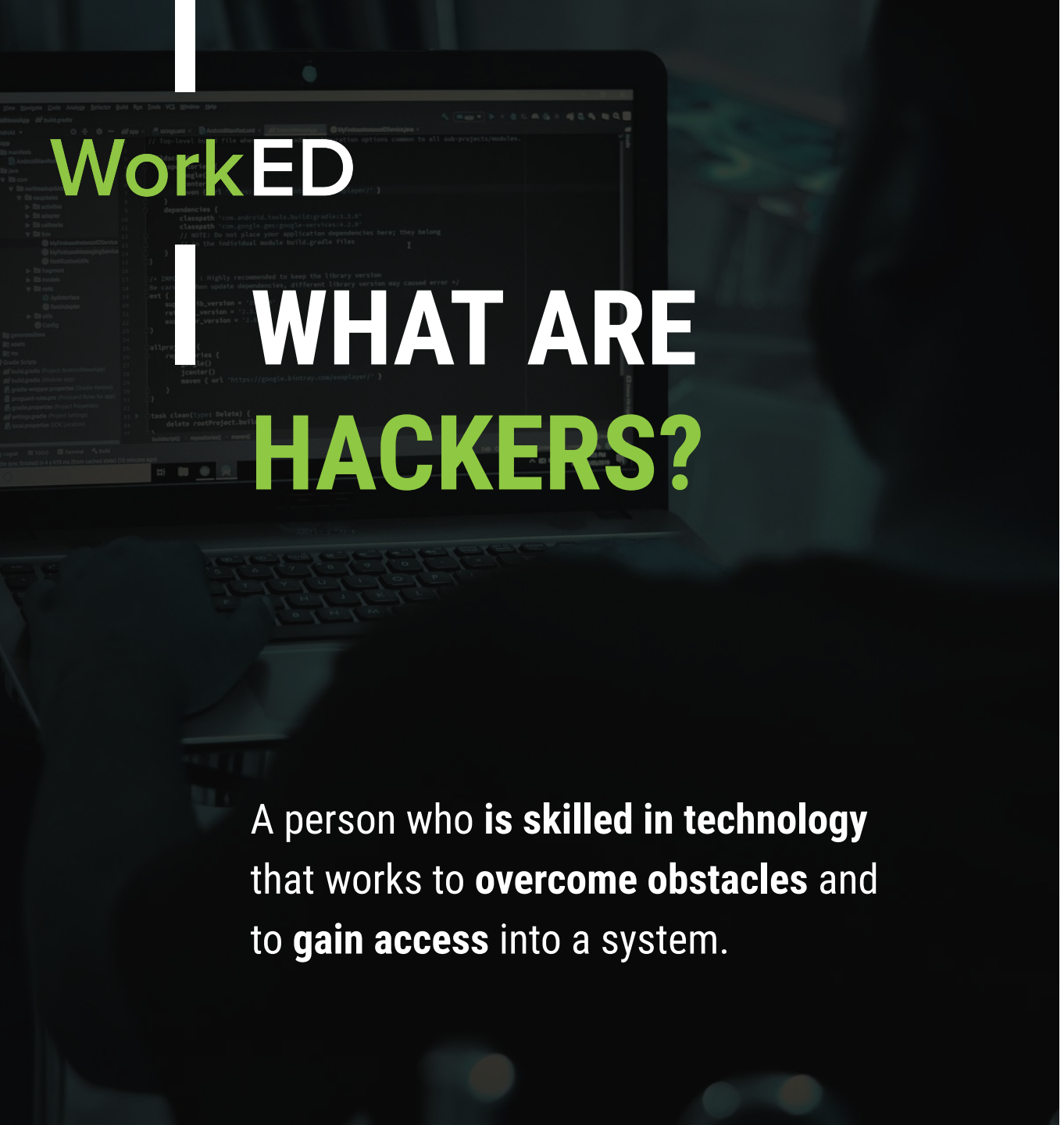
**$19b**

2017 - **Government will spend** a projected $19 billion on cybersecurity
(WHITE HOUSE)

**$217**

estimated **cost** per record per data breach in the US
(FORBES)

## JOB GROWTH



WorkED

# WHAT ARE HACKERS?

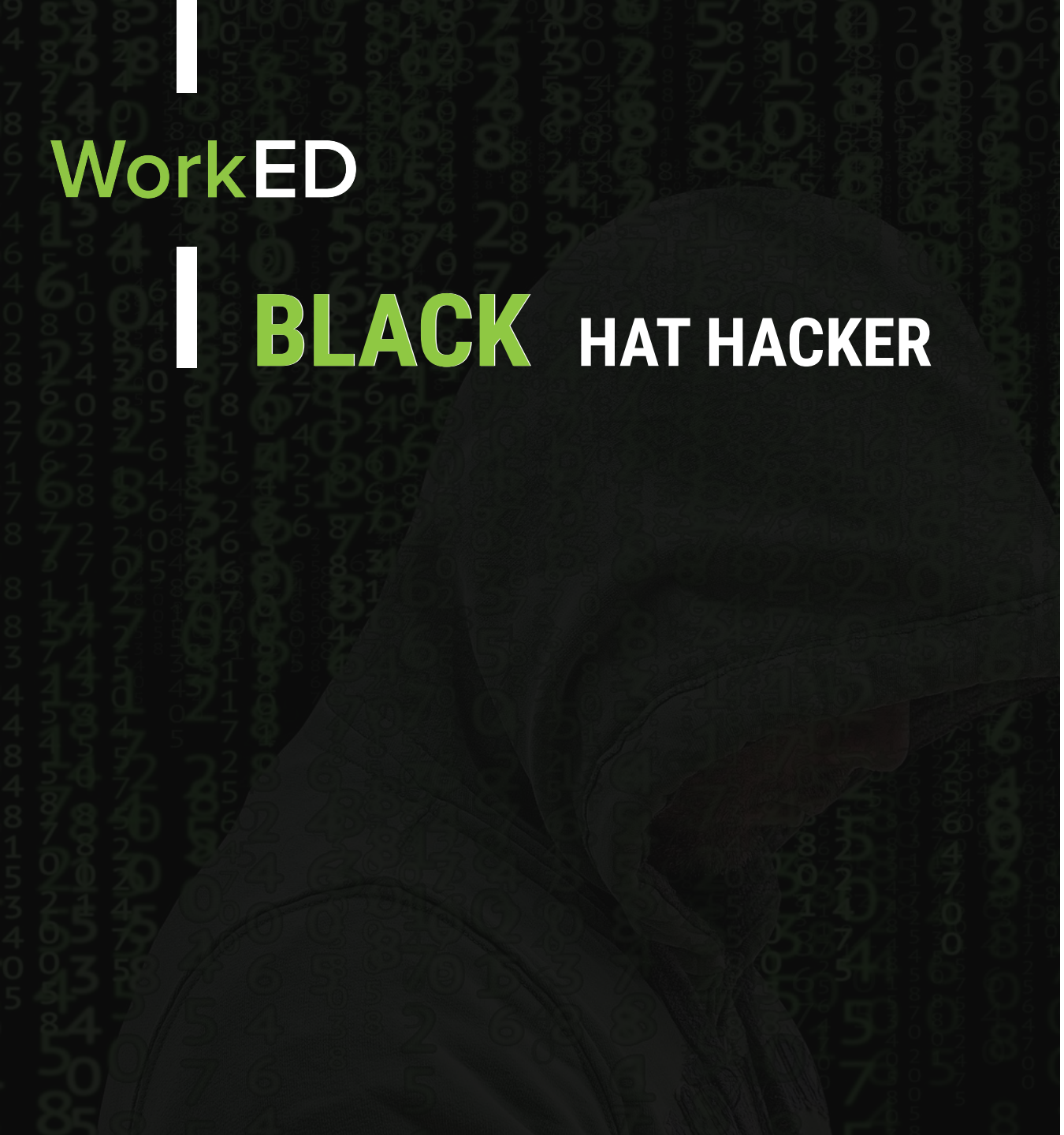
A person who **is skilled in technology** that works to **overcome obstacles** and to **gain access** into a system.

## GOOD OR BAD

WorkED

# THE THREE HATS OF HACKERS

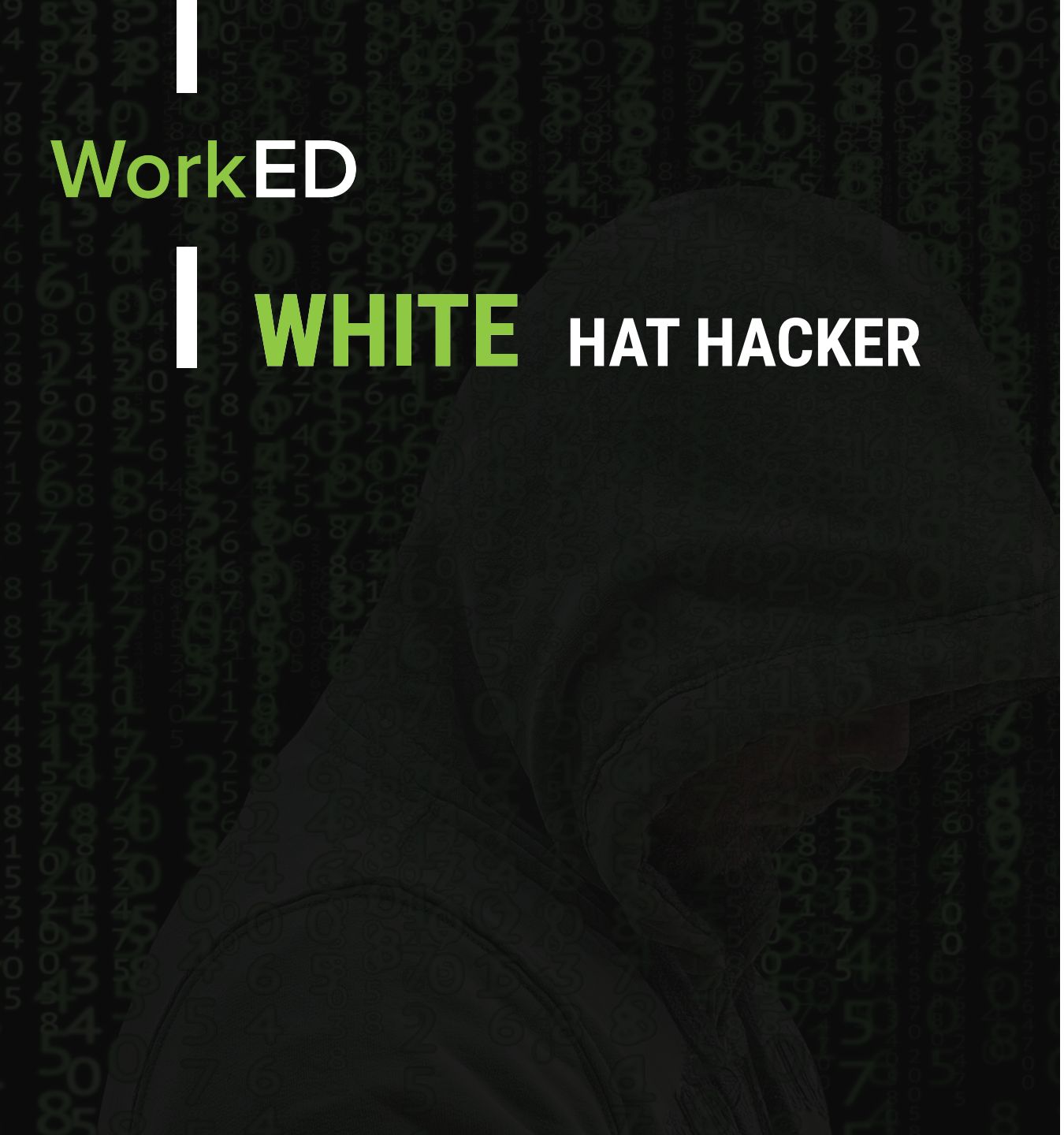
| BLACK HAT HACKER | WHITE HAT HACKER | GREY HAT HACKER |
| --- | --- | --- |
| BAD | GOOD | BOTH |



WorkED

# BLACK HAT HACKER

- Very Skilled with technology
- Someone who tries to access a system with criminal intent and without proper authorization
- They do not always have to access a system but can also place a “bug” that gives harmful intent



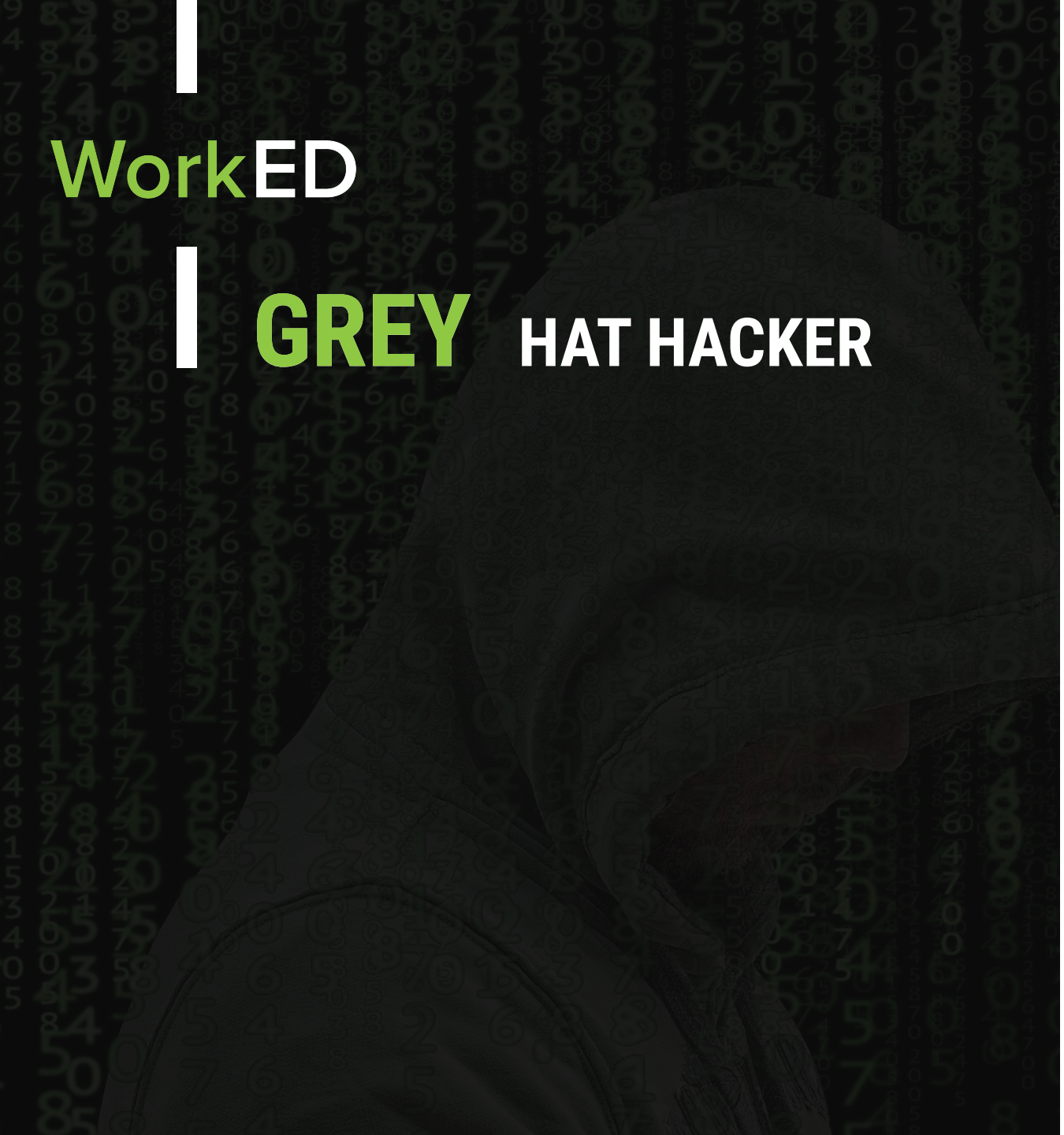
# WorkED

# WHITE HAT HACKER

- Someone who has permission to access a system using methods a black hat hacker might try in order to look for vulnerabilities
- Hired to do so or it is their job to hack for beneficial reasons

WorkED

# GREY HAT HACKER



- A mix between both Black and White hat hackers
- Is not given permission or authorization but will still hack and advise a company of its vulnerabilities. Expecting fees or money to help fix the vulnerability.

WorkED

# NIST

# National Institute of Standards and Technology

In order to **effectively protect our infrastructure**, the NIST created a guideline (framework) to help everyone stay on the same page and keep the 16 sectors secure. This includes:

- **Align cybersecurity decisions** to mission objectives;
- **Organize security requirements** originating from legislation, regulation, policy, and industry best practices;
- **Communicate cybersecurity requirements** with stakeholders, including partners and suppliers;
- **Integrate privacy and civil liberties** risk management into cybersecurity activities;
- **Measure current state** and express desired state;
- **Prioritize cybersecurity resources and activities**; and
- **Analyze trade-offs** between expenditure and risk.

WorkED

# 16 MAJOR CRITICAL INFRASTRUCTURE SECTORS

CHEMICAL

COMMERCIAL FACILITIES

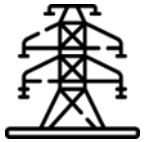
COMMUNICATIONS

CRITICAL MANUFACTURING

DAMS

DEFENSE INDUSTRIAL BASE

EMERGENCY SERVICES



ENERGY

FINANCIAL SERVICES

FOOD AND AGRICULTURE

GOVERNMENT FACILITIES

HEALTH CARE AND PUBLIC HEALTH

INFORMATION TECHNOLOGY

NUCLEAR REACTORS, MATERIALS AND WASTE

TRANSPORTATION SYSTEMS

WATER AND WASTEWATER SYSTEMS

WorkED

# WHY IS INFRASTRUCTURE IMPORTANT?

- The essential services that **our country depend on**. These are the **backbone** and what America depends on to function.
- These are **highly sensitive** as they receive the most types of cybersecurity threats or attacks.
- CIP or Critical Infrastructure Protection - the need and priority **to protect** the most important items to run a country.
- Government is **heavily involved** in protecting these 16 sectors.

# WorkED

## CHEMICAL

Nuclear power plants, energy resources

## COMMERCIAL FACILITIES

Places of business with large gatherings such as malls

## COMMUNICATIONS

Satellite and wireless communications

# WorkED

## CRITICAL MANUFACTURING

Producing products in bulk such as companies that make cars

## DAMS

Helps contain and control large bodies of water

## DEFENSE INDUSTRIAL BASE

Research and development, as well as design, production, delivery, and maintenance of military weapons systems

# WorkED

## EMERGENCY SERVICES

Police departments and fire stations, county sheriff's offices, Department of Defense police and fire departments, and town public works departments

## ENERGY

Oil, Electricity, Natural Gas - supplying fuels to the transportation industry, electricity to house and businesses, and other sources of energy that are important to growth and production across the nation

## FINANCIAL SERVICES

Banks, Credit Card Companies, Insurance companies

# WorkED

## FOOD AND AGRICULTURAL

2.1 million farms, 935,000 restaurants, and more than 200,000 registered food manufacturing, processing, and storage facilities

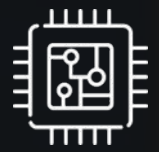
## GOVERNMENT FACILITIES

Educational buildings, museums, national monuments and several buildings owned by the local state and federal government.

## HEALTHCARE AND PUBLIC HEALTH

Protects all sectors of the economy from hazards such as terrorism, infectious disease outbreaks, and natural disasters

WorkED



## INFORMATION TECHNOLOGY

Software and services, technology hardware and equipment and semiconductors and semiconductor equipment

## NUCLEAR REACTORS, MATERIALS, AND WASTE

Covers most aspects of America's civilian nuclear infrastructure

# WorkED

## TRANSPORTATION SYSTEM

Quickly, safely, and securely moves people and goods through the country and overseas - Highways, Boats, Airplanes, Trains

## WATER AND WASTE

Ensuring the supply of safe drinking water and waste treatment and service is essential to modern life and the Nation’s economy

WorkED

# EXAMPLES OF CYBER THREATS TO CRITICAL INFRASTRUCTURE

## HUMAN DEFICIENCIES

- Insider Threats
- Social Engineering
- Phishing Attacks
- Election Hacking

## SYSTEM DEFICIENCIES

- Legacy Software
- Default Configurations
- Encryption
- Unsegmented Networks
- Denial of Service (DDoS)
- Malware
- Ransomware
- Parameter Manipulation

WorkED

# NIST CYBER SECURITY FRAMEWORK

## IDENTIFY

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

## PROTECT

- Access Control
- Awareness and Training
- Data Security
- Info Protection Processes and Procedures
- Maintenance
- Protective Technology

## DETECT

- Anomalies and Events
- Security Continuous Monitoring
- Detection Processes

## RESPOND

- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

## RECOVER

- Recovery Planning
- Improvements
- Communications

WorkED

# OTHER STANDARDS

## ISO

### International Organization for Standardization

- While NIST is more security control driven with a wide variety of groups to encourage best practices related to federal information systems, ISO less technical and more risk focused for organizations of all shapes and sizes.
- Both NIST and ISO can be used together using the best areas to fight against unwanted intrusions but NIST is the only mandatory framework.

## COBIT

### Control Objectives for Information and Related Technology

- Created by ISACA - Informations Systems Audit and Control Association
- Ensures quality, control, and reliability of information systems in an organization, which is also the most important aspect of every modern business.

WorkED

# THANK YOU

Contact us at
hello@workededu.com
800-410-6088