workED

CYBERSECURITY INCIDENT RESPONSE TECHNOLOGIES

Presented by:

workED

INTRODUCTION

- Understand what an incident response is and who conducts it.
- Identify steps of an incident response.

workED

INCIDENT RESPONSE QUESTIONS

What is an incident response?

Who conducts an incident response?

What are the steps of an incident response?

workED

WHAT IS AN INCIDENT RESPONSE?

- Process an organization uses to handle a data breach or cyberattack
- Defines what constitutes an incident for the company
- Provides a clear, guided process to be followed when an incident occurs

workED

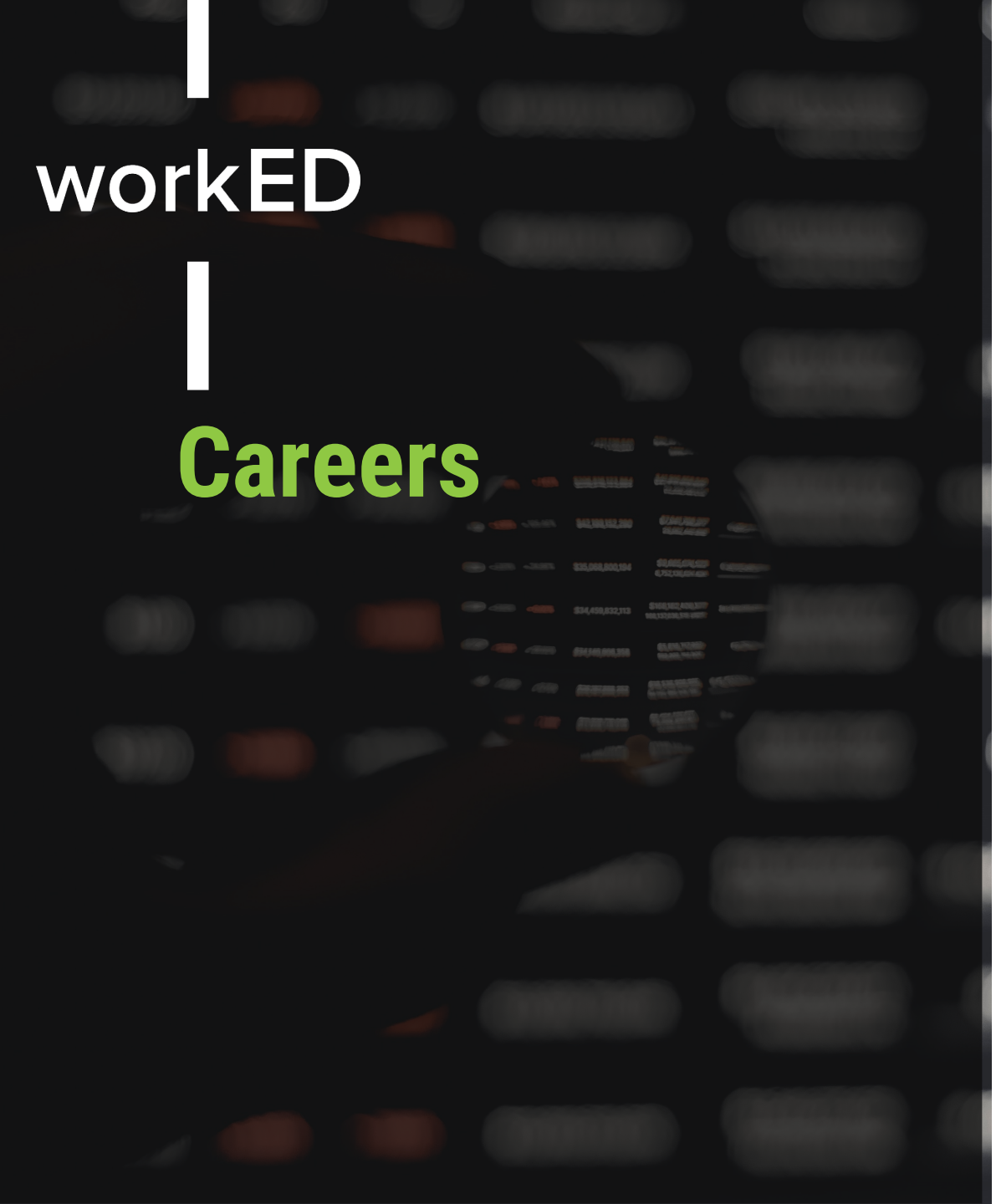
WHO CONDUCTS AN INCIDENT RESPONSE?

- Conducted by an organization's computer incident response team (CIRT) or cyber incident response team
  - Security and general IT staff
  - Members of the legal, human resources, and public relations departments
- Responsible for responding to security breaches, viruses, and other potentially catastrophic incidents

workED

WHAT ARE THE STEPS OF AN INCIDENT RESPONSE?

1. Preparation: Determine CIRT members, access control, tools, and training.
2. Identification: Detect and determine incidents and their scope.
3. Containment: Contain damage and prevent further damage.
4. Eradication: Remove threat and restore affected systems.
5. Recovery: Restore operations and test/verify compromised systems.
6. Lessons Learned: Review incident and improve/update incident response plans.



1. Network Security Specialist: Network and system specialist who is extremely familiar working and configuring routers, firewalls and intrusion detection systems.
2. Pentesters - ethical hackers
3. Incident Handlers: are people with thorough knowledge of attack methodology and incident response, performing analysis and response tasks for various sample incidents, applying critical thinking skills in responding to incidents. "They are the individuals who need to predict that problems are going to happen and what action will be needed to mitigate these issues," says Peter Allor, Steering Committee Member of the Forum for Incident Response and Security Teams (FIRST). He also is the program manager for cyber incident & vulnerability handling for IBM.

workED

Careers Cont'd

1. **Forensics Analyst:** - This role specifically focuses on the rigorous, scientific and thorough forensic analysis of computing systems for evidence and impact of system compromise and digital support of legal, HR, and ethics investigations.
2. **Research Analyst:** focus on learning new techniques, mitigation and protection strategies, staying abreast of technology to help in the incident response activities.
3. **Team Leader:** typically is in charge of leading the team through crises and is involved with people across business units communicating what is going on, what it means and cost to business.

workED

CONCLUSION

- Proper preparation and planning are the key to effective incident response.
- Without a clear-cut plan and course of action, it's often too late to coordinate effective response efforts after a breach or attack has occurred.
- Taking the time to create a comprehensive incident response plan can save your company substantial time and money by enabling you to regain control over your systems and data promptly when an inevitable breach occurs.

workED

CYBERSECURITY
INCIDENT RESPONSE TECHNOLOGIES

QUESTIONS?

THANK YOU