# INTRODUCTION TO INFOSEC JOBS

BY EBRAHEM HEGAZY

# AGENDA

- Penetration tester
- Security analyst
  - Security operations center (SOC)
  - Triage team member
- Security consultant
  - Security consultant (Red teaming)
  - Security consultant (ThreatIntel)
  - Security consultant (Identity and Access Management)
- Security engineer
  - Security engineer (Applications)
  - Security engineer (Systems)
  - Security engineer (ICS)
- Incident handler
- Malware analyst
- CISO

# BEFORE WE START

- We will cover 13 different infosec job, but there is definitely more;
- Courses, and resources changes rapidly. However, the mentioned sources/courses are very good enough to get you up & running.
- We will have Q&A time at the end of the session.

# PENETRATION TESTER

What is it, and what would you do on a daily basis?

Background:

- Programing / Scripting
- Networking
- System administration
- Extensive knowledge of OWASP top 10 for web and mobile

Courses & Certifications:

- Web applications hackers handbook
- Network Pentesting (https://www.pentesteracademy.com/course?id=6)
- EWPT & EWPTXv2 (https://www.elearnsecurity.com/certification/)
- OSCP (https://www.offensive-security.com/pwk-oscp/)

# SECURITY ANALYST

## SECURITY OPERATIONS CENTER (SOC)

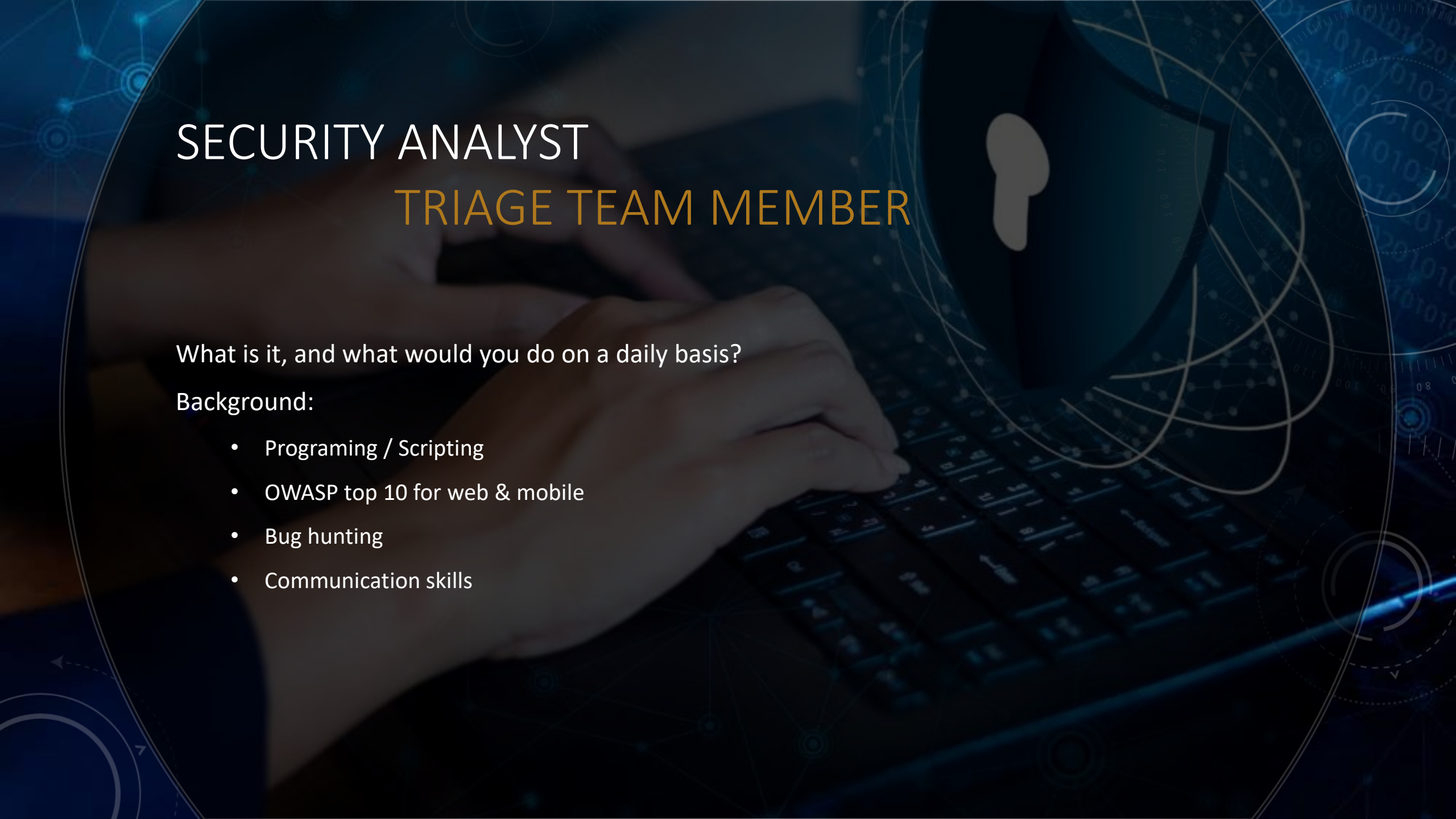
What is it, and what would you do on a daily basis?

Background:

- System administration
- Networking
- Scripting (Python / Bash)
- Basic knowledge of Incident handling process
- Basic malware analysis knowledge

Courses & Certifications:

- MCSE (Windows), and RHCE (Linux)
- Intro to Malware Analysis and Reverse Engineering (https://www.cybrary.it/course/malware-analysis/)
- iTi SOC track (http://www.iti.gov.eg/Admission/ITPprogram/intake38/SOCtrack)



# SECURITY ANALYST

## TRIAGE TEAM MEMBER

What is it, and what would you do on a daily basis?

Background:

- Programing / Scripting
- OWASP top 10 for web & mobile
- Bug hunting
- Communication skills

# SECURITY CONSULTANT

# SECURITY CONSULTANT (RED TEAMING)

What is it, and what would you do on a daily basis?

Background:

- Good knowledge of system administration, specially in Windows environments.
- Networking
- Programing, or scripting (Python / Bash)
- Social engineering
- OWASP top 10
- Solid knowledge of Active directory, and its common attacks
- Solid knowledge of command-and-control (C2/C&C) concepts, and tools.

Courses & Certifications:

- MCSE (Windows)
- OSCP (OSCE for advanced level)
- Rtfm: Red Team Field Manual (https://www.amazon.com/Rtfm-Red-Team-Field-Manual/dp/1494295504)
- Attacking and Defending Active Directory (https://www.pentesteracademy.com/course?id=47)
- Adversary Tactics: Red Team Operations (https://specterops.io/how-we-help/training-offerings/adversary-tactics-red-team-operations)

# SECURITY CONSULTANT (THREATINTEL)

What is it, and what would you do on a daily basis?

Background:

- Extensive recon & information gathering knowledge
- Access to, and contentious monitoring of hacking forums
- Scripting knowledge (i.e. Python)

Courses & Certifications:

- OSINT: Fun with Open Source Intelligence (https://www.pentesteracademy.com/course?id=29)
- eCTHPv2 (https://www.elearnsecurity.com/certification/ecthp_v2/)
- Certified Threat Intelligence Analyst (C|TIA) - https://www.eccouncil.org/programs/certified-threat-intelligence-analyst-ctia/

Notes:
TIBER

Let's check a real job: https://www.glassdoor.com/Job/remote-threat-intelligence-analyst-jobs-SRCH_KO0,34.htm?jl=3581549478

# SECURITY CONSULTANT (IDENTITY AND ACCESS MANAGEMENT))

What is it, and what would you do on a daily basis?

Background:

- System administration (Windows, and Linux)
- Good knowledge of Active directory, and Database management
- Networking

Courses & Certifications:

- MCSE (Windows), RHCE (Linux)
- CISSP (IAM chapter)
- Product/tool based training. For example:
  - AWS IAM (Identity and Access Management) – Deep Dive (https://linuxacademy.com/course/aws-iam-identity-and-access-management-deep-dive/)
  - Managing Identities in Microsoft Azure Active Directory (https://www.pluralsight.com/courses/microsoft-azure-active-directory-managing-identities)

Notes:
Automation
Joiner, Mover, and Leaver

# SECURITY ENGINEER

# SECURITY ENGINEER (APPLICATIONS)

What is it, and what would you do on a daily basis?

Background:

- Experience in applications development
- Deep technical understanding of applications vulnerabilities (i.e. OWASP Top 10)
- Experience in code reviews, vulnerability detection, and root cause analysis
- Pentesting / Bug hunting

Courses & Certifications:

- EWPT & EWPTXv2 (https://www.elearnsecurity.com/certification/)
- OSWE (https://www.offensive-security.com/awae-oswe/)

# SECURITY ENGINEER (SYSTEMS)

What is it, and what would you do on a daily basis?

Background:

- System administration
- Extensive Networking, and network security knowledge
- Scripting
- Good knowledge of corporate security concepts, and tools (i.e. Firewall, IDS/IPS, DLP, VPN)
- Knowledge of incident response, and malware behavior analysis

Courses & Certifications:

- CCNA / CCNP Security
- You usually start with a security solution, untill you become an SME (i.e. Cisco ASA, FireEye NX, McAfee DLP)

# SECURITY ENGINEER (ICS)

What is it, and what would you do on a daily basis?

Background:

- System administration (Windows)
- Extensive IT & OT Network protocols experience
- Good knowledge of corporate security concepts, and tools (i.e. Firewall, IDS/IPS, DLP, VPN, Data Dayood)
- Good understanding of OT environment factors (safety, hazards, policies, how machines works)
- Knowledge of PLC's, DCS, and SCADA systems

Courses & Certifications:

- Industrial Network Security - Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems (Book)
- ICS CERT courses (https://ics-cert-training.inl.gov/learn)
- Global Industrial Cyber Security Professional (GICSP) - https://www.giac.org/certification/global-industrial-cyber-security-professional-gicsp

# INCIDENT HANDLER

# INCIDENT HANDLER

What is it, and what would you do on a daily basis?

Background:

- System administration (Windows), and Linux
- Networking
- Knowledge of various logs (i.e. network logs, webservers logs, and system logs)
- Knowledge of Digital forensics, and malware behavior analysis
- Knowledge of red teams techniques, tactics, and procedures (TTP)

Courses & Certifications:

- GIAC Certified Incident Handler (GCIH) - https://www.giac.org/certification/certified-incident-handler-gcih
- Windows forensics (https://www.pentesteracademy.com/course?id=23)

# MALWARE ANALYST

What is it, and what would you do on a daily basis?

Background:

- Good knowledge of low level programing languages (i.e. C, C++, and Assembly)
- Hands on knowledge of debuggers (i.e. IDA, OllyDbg)
- Good knowledge of binary reverse engineering
- Good understanding of windows internals

Courses & Certifications:

- Secrets of reverse engineering (https://www.amazon.com/Reversing-Secrets-Engineering-Eldad-Eilam/dp/0764574817)
- Practical malware analysis (https://www.amazon.com/Practical-Malware-Analysis-Hands-Dissecting/dp/1593272901)
- eCRE - https://www.elearnsecurity.com/certification/ecre/
- FireEye Malware Analysis Crash Course - https://www.fireeye.com/services/training/courses/malware-analysis-crash-course.html
- SANS 610 (Reverse-Engineering Malware: Malware Analysis Tools and Techniques) - https://www.sans.org/course/reverse-engineering-malware-malware-analysis-tools-techniques

# CHIEF INFORMATION SECURITY OFFICER (CISO)

What is it, and what would you do on a daily basis?

Background:

- System administration
- Networking experience
- Basic knowledge of all infosec jobs

Courses & Certifications:

- SANS 504
- CISSP
- CISA
- ISO 27001
- c|CISO - https://www.udemy.com/course/ec-council-certified-ciso-cciso-certification-practice-test/

# THANKS TO

- Osama Kamal (Sr. Consultant SOC @IBM)
- Ahmed Mashaly (Incident handling team @EG-CERT
- Bassem Ehab (IAM architect @Deutsche bank)
- Hesham Aly (CISO @Emirates NBD)
- Mohamed Abd El Latief (Senior incident response specialist @Kaspersky)
- Mohamed Fathi