Demystifying the Digital Detective

Life of a DFIR Consultant

WAKE UP EXCERCISE

- NBA
- Comics
- Anime
- Human-Centric Design
- Drawing/Digital Art
- Paleontology/Dinosaurs
- CYBERSECURITY

Terryn Valikodath

DFIR Consultant

@ChocolateCoat

@CyberCoat

Kalamazoo, MI -> Grand Rapids, MI

- Jailbreaking iPhones
- Helpdesk
- System Administrator
- Cybersecurity Analyst
- DFIR

What is DFIR?

Digital Forensics

Detective

Collecting, preserving, analyzing, and presenting digital evidence.

DFIR

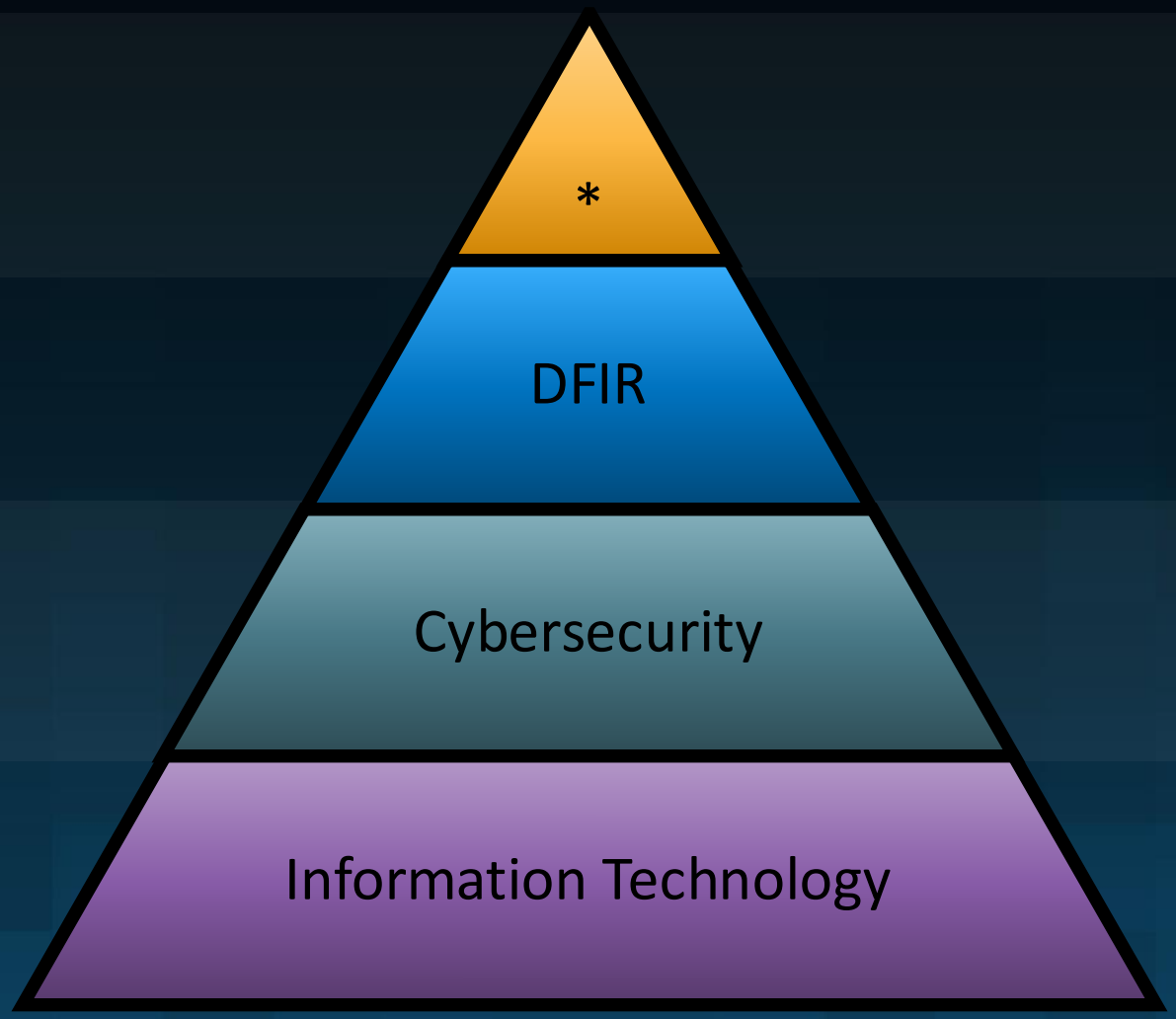
Responding to significant cybersecurity events through analysis and planning.

Incident Response

Firefighter

Identifying, managing, and mitigating security breaches or attacks.

Where does it fit in IT?



DFIR Specialization

Focused skillsets around unique situations.

DFIR

Specialized investigation and analysis.

Cybersecurity

Protection of an organization’s IT assets.

Information Technology

Utilizing and managing technology within organizations.

Job Description

Forensic Investigator

Digital Evidence Examiner

Cyber Analyst

Threat Detection Analyst

IT Helpdesk

Incident Commander

Detection Engineer

Incident Responder

Threat Hunter

System Administrator

Forensic Examiner

DFIR Specialist

Incident Response Engineer

DFIR Consultant

SOC Analyst

DFIR Analyst

The Job on Paper

SPOILERS: Don't worry too much about the specifics

DFIR Job

Experience

- 1-3 years of DFIR experience
- 3-6 years of IT/Cyber experience

Education

- Relevant Cybersecurity Bachelor's or Master's

Certifications

- GCIH, GCFA
- Security+

Skills & Knowledge

- Multiple cybersecurity tools
- Programming language(s)
- All operating systems

Day-to-Day

Realities of the Job

No day is ever the same

On-Call rotations

Volatile workload

Volatile emotional state

No clear schedule

Flexibility and adaptation

Type of Work

Not everyday is an incident

Reactive	Proactive
Emergency Response	IR Plans & Playbooks
Threat Intelligence	Tabletop Exercises
Consultancy	Threat Hunting

The Team

Incident Team

Incident Commander

Leads the team and makes decisions

Incident Analyst/Consultant

Technical analysis and recommendations

Threat Intelligence

Supportive analysis and contextual research

Who you work with

The incident team aren’t the only ones

C-Level

Managers

Project Team

IT Engineering

IT Support

Legal

Partners

Customers

Skillset

Technical Skills

Acquisition

- Disk Imaging
- Memory
- Network
- Cloud
- Triage

Analysis

- Forensic Artifacts
- Logs
- Malware
- Reputation Lookup
- Timeline Creation

IT Operations

- What does an enterprise IT network look like?
- What does an enterprise IT network contain?

Research

- Keeping up with the bad guys
- What do adversaries want?
- How do they “hack”?

Soft Skills

Communication

- High pressure situations and calming presence
- Simplify advanced security/IT concepts
- Explaining what needs to be done and why

Note Taking

- Sharing information with your team and customers
- Explain your brain
- Repeatable processes, scientific method

Reporting

- Explain what happened
- Influence the correct decisions
- Speak to your work

Job Opportunities

Where can you work?

DFIR/Consultancy Organizations

Law Enforcement

Auditing

Managed Service Provider (MSP)

Internal

Tips to get you in the field

- Experience doesn’t just have to be work-related (education, personal projects, research)
- Time is relative, don’t stress too much about the years listed

- Can you explain DFIR concepts
- Incident Response Lifecycle
- What you actually do at each stage

- Explain what a tool does, even if you don’t have direct experience
- Adjacent tools is often enough

Who is this job for?

Do you revel in the chaos of change?

Do you want to help people on their worst days?

Do you like learning how technology works and how it breaks?

THANK YOU!

Questions?

Twitter: @CyberCoat

Everywhere else: @ChocolateCoat

Blog: chocolatecoat4n6.com

thank you!


blog.talosintelligence.com


@talossecurity

TALOSINTELLIGENCE.COM/IR