



CybersCool Defcon Inc.

Syllabus - The OSINT Analyst

Course Outline:

1. OSINT

2. ANALYTICAL PRACTICES

Topic Covered:

- Cognitive Biases Direction
- Collection Planning Analysis
- Evaluation Reporting
- Dissemination

3. OPERATIONAL SECURITY

Topic Covered:

- Risk Modeling
- Thought Processes
- Device Hardening
- Browser Hardening
- Account Creation
- Best Practices

4. INDEPENDENT STUDY

Topic Covered:

- Practical Creation of Accounts
- Browser Hardening

5. SEARCH ENGINE

Topic Covered:

- Boolean Logic
- Keyword Generation
- Search Engines



CybersCool Defcon Inc.

6. SEARCH BEST PRACTICES

Topic Covered:

- Dorks and Operations
- Image Searching
- Caches and Archives
- Best Practices
- Searching Self Study and Practice

7. PARTICIPANT FREE TIME – IMPLEMENTATION

Topic Covered:

- Searching
- Account Creation
- Operational Security
- Guided Exercises
- Content Enrichment
- Weekly Review & Quiz

8. NETWORK ANALYSIS

Topic Covered:

- Network Types
- Nodes & Edges
- Utility of Visualization

9. SOCIAL MEDIA

Topic Covered:

- Platforms
- Foundations of online assets

10. PLATFORM INVESTIGATION

Topic Covered:

- Twitter, Facebook, Reddit, YouTube, Others
- Practical Exercises



CybersCool Defcon Inc.

11. DARK WEB

Topic Covered:

- Background & History
- Markets
- Browsers
- Best Practices

12. DEEP WEB & MESSAGING PLATFORM

Topic Covered:

- Background
- Platforms
- Tools & Best Practices

13. VIRTUAL HUMINT

Topic Covered:

- OpSec Practices
- Cognitive Biases
- Best Practices

14. SELF STUDY

Topic Covered:

- Deep
- Dark Web & Exercises

15. ENRICHMENT LESSON – WORKING MULTILINGUALLY

Topic Covered:

- Machine Translation
- Tools
- Audio/Video
- Transcribing
- Best Practices
- Self-Study
- Weekly Review & Quiz



CybersCool Defcon Inc.

16. PEOPLE INVESTIGATIONS

Topic Covered:

- Theory & Approaches
- Username & Names
- Email Addresses
- Phone Numbers
- Breached Data
- Facial Recognition
- Exercise

17. COMPANY INVESTIGATIONS

Topic Covered:

- Background
- Sign of Illicit
- Behavior
- Practical Tools
- Corporate Registries
- Financial Documents
- Customs Statements
- Exercises

18. MONITORING

Topic Covered:

- Best Practices
- Platforms
- Tools
- Geo-Tools
- Advanced Monitoring
- Cyber Monitoring
- Automation
- Monitoring Array Exercise

19. IMAGE & VIDEO VERIFICATION

Topic Covered:

- Digital Forensics
- Reverse Searching
- Digital Touchups/Metadata



CybersCool Defcon Inc.

20. ENRICHMENT SESSION

Topic Covered:

- Disinformation and Influence Operations
- Weekly Quiz

21. DOMAIN ANALYSIS

Topic Covered:

- Background
- Technological
- Overview
- DNS/IP
- Infrastructure
- Mapping
- VPS
- WHOIS
- Reverse IP. Name
- Server, Mail Server
- Exercises
- Tracker Mapping
- WordPress
- Investigation and Exploitation
- Marketing Tools
- Advances techniques
- Qualitative Investigation
- Traffic Measuring
- Concluding Exercises

22. ENRICHMENT LESSON

Topic Covered:

- Cryptocurrency
- Cryptocurrency Investigation, Methods, Exercises
- Blockchain Theory & History
- Utility in Cybercrime
- Concluding Investigation, Reporting and Presentation Exercises
- Comprehensive Review Session



CybersCool Defcon Inc.

23. ANALYST PLATFORM

Topic Covered:

- Tools
- Q&A
- Hands-On
- Reporting and Dissemination Exercises
- Collaboration Exercises

24. FINAL EXERCISE

Here's are the of component needed in hosting cybersecurity learning platform via Cloud Services.

1. Server Infrastructure:

- Webservers: Apache Nginx for hosting the platform
- Database Servers: MySQL, PostgreSQL, MongoDB for storing user data, courses, and progress.

2. Networking Equipment:

- Routers switched and firewalls to manage network security.
- Load balancers for distributing incoming traffic across multiple servers.

3. Security Software:

- Intrusion Detection Systems (IDS) and Intrusion Prevention System (IPS) to monitor and protect against cyber threats.
- Anti-malware and antivirus software to scan for and remove malicious software.
- Security information and event management (SIEM) software for aggregating and analyzing security logs.

4. Authentication and Authorization Systems:

- Single Sign-On (SSO) solutions for seamless login across multiple services.
- Role-based access control (RBAC) for managing user permissions within the platform.

5. Encryption Tools:

- SSL/TLS certificates for encrypting data transmitted between servers and clients.
- Encryption protocols (e.g., AES) for securing stored data.

6. Monitoring and Logging Tools:

- Monitoring tools for tracking system performance, uptime, and resource usage.
- Logging tools for recording user activity system events, and security incidents.



CybersCool Defcon Inc.

7. Content Delivery Systems:

- Content Delivery Network (CDNs) for delivering course materials and multimedia content quickly and reliably.

8. Virtualization and Containerization Platforms:

- Virtual machines (VMs) or containers for isolating and running application services.
- Orchestration tools like Kubernetes or Dockers Swarm for managing containerized applications.

9. Backup and Disaster Recovery Solutions:

- Regular backups of data to prevent data loss in case of system failure or cyber-attacks.
- Disaster recovery plans and procedures to restore services quickly in the event of a major outage.

10. Development and testing Environments:

- Development frameworks and tools for building and testing new features.
- Continuous Integration/Continuous Deployment (CI/DC) pipelines for automating software deployment.

11. User Interface and Experience Tools:

- Fronted frameworks like React.js or Angular for building responsive and interactive user interfaces.
- Design tools for creating visually appealing and intuitive user experiences.

12. Compliance and Regulatory Tools:

- Tools for ensuring compliance with data protection regulations (e.g., GDPR, HIPAA).
- Vulnerability scanning tools for identifying and addressing security weaknesses.

13. Customer Support and Communication Tools:

- Helpdesk software for managing user inquiries and support tickets.
- Communication tools like email, chat, and collaboration.

14. Education Content Creation Tools:

- Authoring tools for creating and editing educational materials, such as videos, presentations, and quizzes.
- Learning management system (LMS) for organizing and delivering course content to users.



CybersCool Defcon Inc.

15. User Analytics and Feedback Systems:

- Analytics tools for tracking user engagement, course completion rates, and other key metrics.
- Feedback mechanics for collecting user opinions and suggestions for improving the platform.

16. Legal and Compliance Support:

- Legal consultation for ensuring compliance with intellectual property laws, terms of service, and privacy policies.
- Cyber insurance to protect against potential legal liabilities and financial losses from security incidents.

17. Training and Support for Staff:

- Training programs for platform administrators, instructors, and support staff on cybersecurity best practices and platform usage.
- Technical support for troubleshooting issues and resolving user concerns.

18. Internet Bandwidth:

- The required amount will depend on factors such as the numbers of users accessing the platform simultaneously, the type of content being served (e.g., text, images, videos), and any streaming of interactive features.