MalTrak

MalTrak Certified SOC Analyst

Go from a complete newbie to your first entry job in cybersecurity in 3 Months

Key Benefits

- Personalized guidance
- Real-world practical experience
- Professional Certification
- Resume & Job Hunting Advice

Are you ready to be part of the ever-growing field of cybersecurity?

Whether you are a lawyer, doctor, or even working in IT administration or network security, this MalTrak Certified SOC Analyst Program helps you to shift your career to cybersecurity and get all the necessary skills & certifications to land your first SOC job in cybersecurity

Key Benefits:

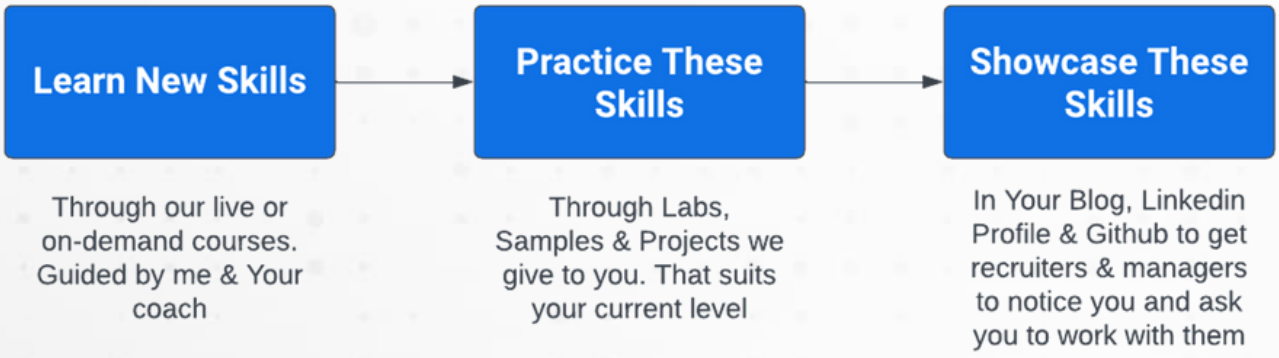
- **Get personalized guidance & Mentorship:** From monthly 1:1 calls to 3 times weekly group live zoom calls to our personalized roadmap, and the practical hands-on labs and exercises we provide you to learn the skills practically with dedicated time & effort to answer your questions.
- **From SOC to Threat Hunting Live Training:** 24-hour live hands-on training where you will gain the experience and expertise we have gained after working over 10 years in the industry. You will get our direct guidance and supervision throughout the live training. Don't reinvent the wheel or spend years relearning all these skills. Start from where others stopped through this live training program.
- **Get the real-world experience needed for the high-paid job you are applying for** through our practical labs. You will look over the shoulders of our engineers on how they analyze real attacks and as well in-depth case studies to shortcut the experience needed for a high-paid job in cybersecurity.
- **Get access to an intensive on-demand courses library,** you will get from complete foundational training like Linux & Networking Fundamentals to more advanced courses with easy-to-follow hands-on labs, copy-paste cheatsheets, workbooks and much more.
- **Get certified and build a compelling resume for the dream job you are applying for**. Our team will help you craft a compelling resume that showcases your skills, your experience and your creditability. And as well, get our MalTrak Certified SOC Analyst certification.

The Program Structure:

The program is mainly 3 months with 3 times weekly group zoom calls, 1:1 calls every month to track your progress and as well live training, and much more.

You will have access to our library of courses and as well the recording of the live training for one year. And as well for our community if you would like to ask questions and interact with the other students

Coaching, Guidance & Mentorship



Personalized guidance on all the required skills you will need to learn cybersecurity.

Throughout the whole program, we provide coaching, guidance and mentorship for you to help you laser focus on the goals you want to achieve, unclutter yourself and get through any obstacles you might face along the way.

The Process:

- **Step 01:** We will provide you with the necessary training and materials to learn a new skill. And we will be reviewing your progress in learning it
- **Step 02:** Once you learn this skills, we are going to provide you with efficient, close-to-real-world labs to practice more and gain the experience needed.
- **Sep 03:** You are going to document this experience you gained from the previous lab in a blog, GitHub project, and your LinkedIn profile to showcase that skill in front of hiring managers and recruiters to get them to reach out to you to hire you in their team. We will be reviewing your work to make sure it shows you in the most professional way possible.

Access & Support:

- Once you join, you will have a 1:1 assessment and onboarding call with your direct coach. He will assess your skills and build a roadmap for you. Also, you will have a monthly 1:1 calls to track your progress
- You will have a group zoom weekly meeting with me where I will guide you and review your weekly report. Your weekly report should consist of:

1. What have you done last week?
2. What are you going to do next week?
3. Did you face any obstacles learning, practicing or documenting your work?
4. Do you have any questions you want to ask? Resume to review or help in job hunting or interviews?

- You will also have two other weekly meeting with your dedicated coach (3 group calls in total in different time zones so you can attend at least one of them)
- You will have a dedicated hour every day to ask questions and get your direct coach to help you.
- You will have access to a community of +200 students and professionals in cybersecurity

Access To Our On-Demand Courses Library

On-demand Library of hands-on training

You will learn all foundational skills & prerequisties that prepares you to be the next SOC analysis

In this library of on-demand courses, we are going to provide you with all the needed fundamental skills to start learning cybersecurity. You will learn about IT administration, operating systems, and networking

You will also be introduced to cybersecurity key concepts in a practical and engaging way. We will cover the necessary skills that qualify you to work as a SOC Analyst.

You will learn how real attacks work, the basics of log analysis, incident response, forensics investigation, and malware analysis. As well, you will be introduced to advanced attacks such as Fileless attacks and ransomware attacks.

If you are completely new to IT or to cybersecurity, this library of courses will give you all the prerequisites you need to start your career in cybersecurity.

You will have access to this entire library of courses for one year and you will be guided through this training with our mentorship and guidance

Key Objectives:

- Learn the required IT administration skills for Windows and Linux
- Learn internet communication, network protocols, and packet analysis (TCP, UDP, IP, HTTP, DNS ... etc)
- Learn the key concepts of Cybersecurity
- Learn How real targeted attacks work
- Learn how to perform Log Analysis
- Learn the fundamentals of incident response and malware analysis

Our Students Testimonials

"Thank you Amr Thabet for the great effort in this training. You have covered many topics/techniques of the red team and the blue team that simulate the thinking of the attacker and how to deal with them in the most practical and realistic way "

- Andrew Essam, Network Security Engineer at Vantage Securities Brokage

"Thank you Amr Thabet for explaining some adversary simulation steps according to the MITRE ATT&CK framework with such clear examples. Don't miss this training from Amr Thabet "

- Ali Soban, Cisco Certified Specialist- Security

"This training from MalTrak is one of the best courses I have ever taken. The curriculum gives you an excellent starting point for a career in incident response and malware analysis. It provides a clear understanding of what modern cyberattacks look like in real-world and how to recognize the tools and the techniques used by any cybercriminal and how to analyze them. Totally recommended"

- Paul Gallovich, SOC Analyst at Coast Community College District

"The best training available to master incident response, digital forensics, and malware analysis. It helped me a lot in strengthing my skills. Totally recommended"

- Moutaz Elsheikh, Sr Forensic Intelligence Analyst

"Basically I have gone through many courses and boot camps order to learn "Real life CyberSecurity operations" but a significant amount of courses just showed old techniques or some better tools. However, the training delivered by Amr Thabet covered that gap and explained to me the reality of industry and methodology. I'm personally working in the industry and got really juicy and interesting knowledge. I highly recommend people to attend this."

- Shravan Kumar, Cyber Security Associate at FICO

In-Depth Investigation & Threat Hunting

Feb 19-22, 2024 (4 days, Live Through Zoom)

This training focuses on in-depth investigation through the logs, memory and digital forensics artifacts to detect, investigate and hunt for the targeted attacks, APT attacks and ransomware attacks

In the In-Depth Investigation & Threat Hunting live training, you will learn the most needed skills to become a SOC analyst, Incident Handler, or even a Threat Hunter.

You will learn **how real APT attacks and targeted attacks work**, how to **perform in-depth investigation** through collecting and analyzing digital artifacts, **performing live forensics, memory forensics**, and **how to automate this process across the whole enterprise in Powershell.**

As well, you will learn how to perform threat hunting based on the MITRE ATT&CK framework and powered by threat intelligence. Not just the Attackers' IoCs but their tactics, techniques, and procedures.

Key Objectives:

- An in-depth understanding of APT attacks, fileless malware, and targeted ransomware attacks from initial access until the lateral movement and domain overtake
- How to perform an in-depth digital investigation through live forensics, memory forensics, or analyzing key artifacts to detect malicious activities.
- How to build a threat hunting process that is powered by MITRE ATT&CK framework and threat intelligence information.

DAY #1:

INTRODUCTION TO APT ATTACKS & MITRE ATT&CK

- What is an APT Attack?
- What are the Attack Stages? And what's MITTRE ATTACK?
- APT attack lifecycle
- Examples of real-world APT attacks
- Red Team Tools & Frameworks (PowerSploit, Powershell EMPIRE, Cobalt Strike, Metasploit, Kali Linux)

INTRO TO OUR PURPLE TEAM CLOUD LAB

- Intro to Purple Teaming & Why Purple Teaming?
- The Design of your lab
- Hands-on Attack Simulation using Atomic Red Team
- Hands-on Attack Simulation using Caldera
- Investigating Sysmon Logs using Elasticsearch
- Perform deeper investigation using Powershell Remoting
- Learn how to build this lab for yourself using AWS & Terraform

INTRO TO INCIDENT RESPONSE & THREAT HUNTING

- The Incident Response Lifecycle
- how attacks are being discovered (SOC, 3rd party & threat hunting)
- Security Controls and types of logs in an organization
- What's Threat hunting & why threat hunting?
- Types of Threat hunting
- The threat hunting process step by step
- Intelligence-based Threat hunting

INITIAL ACCESS & LOG ANALYSIS

- Spearphishing Attacks with a malicious attachment
- Spearphishing attacks with links
- Spearphishing attacks using social media
- Hands-on Simulating & Detecting Spearphishing using Sysmon Logs
- Advanced execution techniques
- Hands-on Analyze attacks using Sysmon & Splunk

DAY #2:

PACKET ANALYSIS & MALWARE EXFILTRATION

- Hunting the evil in packets
- Detecting Malware Exfiltration methods
- Detecting Downloaders, malicious documents, exploits and others
- Detecting IP Flux, DNS Flux, DNS over HTTPS
- Malicious bits transfer, malware communicating through legitimate websites
- Detecting peer-to-peer communication, Remote COM Objects and unknown RDP Communications
- Hands-on analysis using Wireshark & Microsoft Network Monitor
- Hunting the evil in zeek logs
- Hands-on analysis using zeek logs & Elasticsearch

IN-DEPTH INVESTIGATION & FORENSICS

- Why in-depth investigation?
- Detecting malware persistence: Autoruns registry keys and options
- Detecting malware persistence: Scheduled tasks and jobs
- Detecting malware persistence: BITs jobs
- Detecting malware persistence: Image File Execution Options & File Association
- Detecting Malware & Malicious Documents Execution (Prefetch, MRU, Shims, Outlook Attachments)
- $MFT structure and cavity searching
- How to perform Live Forensics (Hands-on)

MALWARE IN-DEPTH & MALWARE FUNCTIONALITIES

- Types of Malware
- Malware Functionalities in-depth (APIs, Code Functionalities & Detection Techniques)
- Malware Encryption & Obfuscation (packing, strings encryption, API encryption .. etc)
- Strings and API Encryption & Obfuscation
- Network communication Encryption & Obfuscation
- Virtual machine & Malware analysis tools bypass techniques
- Write your own YARA rule

DAY #3:

MALWARE DEFENCE EVASION TECHNIQUES

- Process Injection (DLL & Shellcode Injection)
- Advanced Process Injection (APC Queue Injection)
- Advanced Injections: Using NTFS NxF Feature
- Detecting Process injection using Sysmon logs
- Detecting Process injection using Live Forensics
- Use of legitimate applications for Applocker bypass
- Disguise malware using COM Objects
- Detecting & preventing the abuse of the legitimate applications
- Sysmon & EDR Bypass Techniques
- Detecting EDR bypass techniques with Live forensics

MEMORY FORENSICS

- Intro to Memory Forensics & Volatility
- Capture a full memory dump
- Extract suspicious & hidden processes
- Detecting memory injection, process hollowing & API hooking
- Detect injected threads using call stack backtracing
- Detect suspicious network communication & extract network packets
- Detect malware persistence Functionalities using registry hives
- Detect the initial access using Prefetch files & MFT extraction
- Extract windows event logs from memory
- Automate memory processing using python

DAY #4:

MALWARE PRIVILEGE ESCALATION TECHNIQUES

- UAC bypasses using legitimate apps
- UAC bypasses using COM objects
- UAC bypasses using Shimming
- Abusing Services for privilege escalation
- DLL Order Hijacking
- Privilege escalation to SYSTEM
- Best practices for detecting & preventing privilege escalation
- Mac OSX & Linux privilege escalation

INCIDENT RESPONSE IN AN ENTERPRISE: POWERSHELL INTRO

- Intro to Powershell
- Powershell Remoting
- Logon Types and Powershell vs RDP
- Collect & Analyze Malicious Artifacts using Kansa
- Collect Minidumps using Powershell
- Detect suspicious processes using Powershell
- Automating Artifacts collection & analysis for threat intelligence
- Convert your threat hunting hypothesis into an alert
- Write your own SIGMA rules

CREDENTIAL THEFT DETECTION & PREVENTION

- Detecting & Preventing Lsass Memory dump
- Detecting & Preventing Token Impersonation
- Find attack paths & weak links using Bloodhound

THIS TRAINING QUALIFIES YOU FOR:

- Cybersecurity Analyst
- SOC Tier 1
- Incident Handler (SOC Tier 2)
- Threat Hunter

Complete Resume Makeover & Job Hunting

LIMITED TIME

The registration is open only for a very short time as we are starting in less than a week.

So, make sure to sign up now before it's closed

This will be an ongoing process you will go through in the whole 3 months. We will help you showcase your work which will include building a technical blog where you are weekly sharing your technical analysis.

As well, it will include how to build a professional image on LinkedIn, reach out to recruiters and hiring managers, and write a compelling resume and cover letter.

Key Objectives:

- Build a technical blog to showcase your technical skills
- Build a professional world-class image on LinkedIn
- Build a professional clean resume and cover letter
- Reach out to recruiters and hiring managers to land the job you are looking for

Earn Our MalTrak Certified SOC Analyst Certification

By completing this 3-month program, you will gain our creditable certificate: MalTrak Certified SOC Analyst (MCSA) certification.

You will receive your certification in accredible.com so your future employer can verify your certificate. As well, you will be eligible for CPE points.

Registration Process

The program is open for a very short period as we are starting in a week or two, So, complete the registration now from here and apply Coupon: NEWYEAR to gain an extra discount (available until Jan 12)

Registration Link: https://maltrak.com/soc-registration
Coupon Code: NEWYEAR

Frequently Asked Questions (FAQ)

Q1: When does the program start?

The program is starting on January 22nd, 2024. The registration will be closing shortly beforehand and as well the early-bird price is closing on Jan 12.

Q2: What makes this program different from others?

This program is focused on coaching, mentorship and practical experience. A lot of programs are full of theory or general cybersecurity content but very few programs that are specific, practical and laser-focused on the necessary skills & tools you need to learn to land your first job in the industry.

This program prepares you for the roles:

- SOC Analyst (Tier 1)
- Incident Handler (Tier 2)
- Threat hunter
- Security Analyst

Q3: Is this certification credible?

Yes, through the last few years, MalTrak established a credible name through its hands-on training and the skilled participants who graduated through our programs.

MalTrak Certified SOC Analyst certification will help get through the resume filtration process and get to the interviews and the job offers with ease

Q4: What happens if I can't attend any live training?

You will have 1-year access to the recordings. You can watch it at any time.

Q5: How long is the Master's Program?

3 Months. With access to the library of training & our community for one year

Q6: How much time should I allocate per week?

Only 2 hours/working day. If you can add 4 hours on Sunday as well, that would be great

About MalTrak

If you are ready to shift your career to the ever-growing field of cybersecurity, you are ready for MalTrak

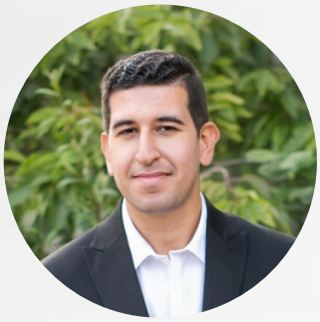
MalTrak is a cybersecurity organization **specialized in the detection, response, and hunting of current threats companies are facing right now** such as targeted attacks, ransomware attacks, and cloud attacks.

MalTrak's mission is to equip cybersecurity professionals and companies with the training, tools, and processes to help them respond to such attacks and better protect their assets

MalTrak has helped over 200 professionals from all over the world build their skills in cybersecurity with live training, recorded training, and personalized coaching.

Now MalTrak is continuing its mission through this dedicated Masters program to ensure that the new generation of cybersecurity professionals are equipped with the practical skills and tools to protect

About Amr Thabet



Amr Thabet, Founder of MalTrak

Amr Thabet is a malware researcher and an incident handler with **over 10 years of experience**, he worked in some of the **Fortune 500 companies, including Symantec, Tenable, and others**.

He is the founder of MalTrak and the **author of "Mastering Malware Analysis, 2nd Edition" book** published by Packt Publishing.

Amr has spoken at **top security conferences all around the world**, including **Blackhat, DEFCON**, **Hack In Paris**, and **VB Conference**. He was also featured in Christian Science Monitor for his work on Stuxnet.

His mission is to help security professionals worldwide build their expertise in malware analysis, threat hunting, red teaming, and, most importantly, protect their organization's infrastructure from targeted attacks, ransomware attacks, and APT attacks.