08

Recorded · Course 08 of 08

SOC Analyst

Get job-ready for a Security Operations Centre: SIEM and Splunk log investigation, phishing email analysis, digital forensics and incident response. Pre-recorded, so you learn at your own pace, with a certificate when you finish.

AT A GLANCE

Format
Pre-recorded videos

Language
Telugu

Lessons
59 · 5 modules

Pace
Self-paced, anytime

Certificate
On completion

AFTER THIS COURSE

- [x] Investigate alerts and logs in Splunk the way a SOC analyst does
- [x] Analyse phishing emails, headers, links and attachments
- [x] Handle evidence and incidents from identification to recovery

TOOLS YOU'LL USE

Splunk · SIEM · SOAR · Windows Event IDs · SPF · DKIM · DMARC · Threat intelligence

SYLLABUS · 5 MODULES · 59 LESSONS

01 SOC Fundamentals

7 lessons

THEORY

- What is a SOC?
- SOC workflow
- What is SIEM?
- What is threat intelligence?
- What is SOAR?
- What is digital forensics?
- What is incident response?

02 Log Analysis & Investigation

18 lessons

SPLUNK FUNDAMENTALS (THEORY)

- Introduction to Splunk
- Splunk architecture & workflow

SPLUNK HANDS-ON (PRACTICAL)

- Splunk demo & your first search
- Understanding Windows Event IDs
- Investigating failed login attempts
- Analysing successful login events
- Process creation monitoring
- New user account creation detection
- Linux SSH log analysis
- Firewall log analysis
- DNS log analysis
- Email log analysis & phishing detection
- Brute-force attack investigation (end to end)
- Password spraying detection
- Suspicious PowerShell detection
- Privilege escalation detection
- Malware infection investigation
- Data exfiltration investigation

03 Email Phishing Analysis

12 lessons

THEORY

- Introduction to email phishing
- Email authentication
- Email header analysis
- SPF (Sender Policy Framework)
- DKIM (DomainKeys Identified Mail)
- DMARC (Domain-based Message Authentication, Reporting & Conformance)

03 Email Phishing Analysis (continued)

PRACTICAL

- Phishing email analysis
- Email header analysis
- SPF, DKIM & DMARC verification
- Sender domain analysis
- URL analysis
- Attachment analysis

04 Digital Forensics

14 lessons

THEORY

- Introduction to digital forensics
- The digital forensics process
- Identify
- Preserve
- Collect
- Examine
- Analyse
- Report

PRACTICAL

- Evidence identification
- Evidence preservation
- Evidence collection
- Evidence examination
- Evidence analysis
- Forensics report preparation

05 Incident Response

8 lessons

THEORY

- Introduction to incident response
- The incident response lifecycle

PRACTICAL

- Incident response workflow
- Incident identification
- Containment techniques
- Malware eradication
- System recovery
- Incident documentation & lessons learned

Ready to start SOC Analyst?

Free live demo: Saturday 6:00 – 7:00 PM · Sunday 11:00 AM – 12:00 PM · Sunday 7:00 – 8:00 PM (IST). Reply **DEMO** on WhatsApp.

+91 81250 59380 · Call or WhatsApp

contact@secueyes.in

secueyes.in

Scan for this course

SecuEyes

YOUR INSTRUCTOR

Taught by a hacker who investigates cybercrime.



Every class is taught by **Chaitanya Eshwar Prasad**. He doesn't teach from slides: he teaches what he does every week, investigating real cybercrime cases and finding real vulnerabilities.

He started exploring technology in 7th class and was hunting security bugs by 10th. Today he supports cybercrime investigations as a forensic investigator, holds national records for his work, and has taught thousands of students on campus and through his Telugu YouTube channel.

7+	100+	33K+	9+
Years in cybersecurity	Bugs reported & secured	YouTube learners	Campuses as guest speaker

Anisetti Chaitanya Eshwar Prasad
Founder & Lead Instructor, Secueyes

SECURITY RESEARCH · HACKED & REPORTED

Google · YouTube · PayPal · Lenovo · Nokia · Epic Games
Unreal Engine · Rakuten · Kik · CoWIN · MCA, Govt of India · Govt of Telangana

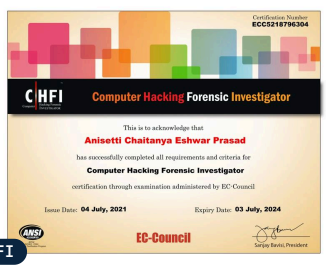
INVITED AS GUEST SPEAKER · UNIVERSITIES & COLLEGES

KL University · Anurag University · GRIET · VNRVJIET · KPRIT
ACE Engineering College · KL SAC · SJB Institute of Technology · Rishi MS Institute for Women

EC-COUNCIL CERTIFICATIONS



CEH



CHFI



CSA