DINA MOHAMED

Cybersecurity Analyst

AI & SOC Analysis

Exploring the future of cybersecurity roles

Professional Certifications

- CEH MASTER
- ISC2 CC
- Cisco CyberOps
- FCP FortiSIEM 6.3
- CAPT
- Threat Intel Analyst

Core Expertise

- SOC Operations & Monitoring
- Penetration Testing
- Incident Response
- Threat Intelligence

Tools in Production

FortiSIEM | QRadar | McAfee SIEM | Splunk

Real alert triage & tuning

Education & Achievements

B.Sc. Information Systems, University of Bahrain — **1st Place Senior Project (Face Recognition AI)**

Freelance Security Incident Responder

Resolving live incidents independently

3+
Years Experience

100+
Alerts/Day

"I've spent years defending enterprises from real threats. Today's question: can AI do what I do?"

May 2026

Presenter: Dina Mohamed

CRITICAL STATS

LIVE DATA

11,000 cyber attacks occur every minute

AI is watching. But who decides?

4.7M
Workforce Gap
+12% YoY
ISC², 2024

80%
False Positives
-5% vs 2023
SOC alerts avg

194
Days to Detect
-45% with AI
IBM, 2024

1M+
Alerts/day

68%
Don't trust AI

60%
MTTD reduction

24/7
Uptime

The real question isn't "will AI replace analysts?" — it's "what happens if we don't adapt?"

AI processes 1M+ alerts daily

Humans can't match this volume

→ Learn More

What Does a SOC Analyst Actually Do?

The three-tier escalation model in modern Security Operations Centers

Tier 1

Alert Analyst

Triages **100+ alerts** per shift. Most require human context to correctly classify.

- Monitor dashboards
- Triage incoming alerts
- Escalate suspicious events
- Apply SOC playbooks

Tier 2

Incident Responder

Handles escalated threats. Focuses on containment, containment, root cause, and remediation.

- Deep-dive investigation
- Threat correlation
- Forensic analysis
- Remediation guidance

Tier 3

Threat Hunter

Proactively searches for hidden threats that bypassed automated security controls.

- Proactive hunting
- Adversary emulation
- SIEM rule writing
- Zero-day research

Core Tools Across All Tiers

SIEM Platforms | EDR | Threat Intel | Forensic & OSINT

Irreplaceable Human Skills

Contextual Judgment | Stakeholder Comms | Intuition | Ethics

AI Capabilities in the SOC Today

What AI can genuinely accomplish in modern enterprise security environments

AI Strengths

Transforming defense at machine speed

SIEM Alert Correlation

Connects disparate events across the network at true machine speed

UEBA (User & Entity Behavior)

Detects behavioral anomalies seamlessly across millions of active users

SOAR Automation

Automates repetitive response playbooks to free up analyst bandwidth

Threat Intel
Enrichment in ms

24/7 Uptime
Zero analyst fatigue

Vendor Implementations

Microsoft Sentinel
AI-driven SIEM platform

Darktrace
Autonomous threat response

CrowdStrike Falcon
AI-powered EDR

IBM QRadar
Integrated with Watson AI

Splunk SOAR
Automated playbooks

60%
MTTD Reduction
In tested enterprise AI deployments

1M+
Events Per Day
Alert volume impossible for human teams alone

AI Limitations

The crucial gaps no machine learning model can fill alone

Critical Gaps

False Positive Flood

AI flags anomalies it doesn't understand; analysts still drown in noise

No Business Context

AI can't know the CFO always logs in from Dubai at 2am

Novel & Adversarial Attacks

Attackers now use AI to bypass AI-based defenses

Living-off-the-Land (LotL)

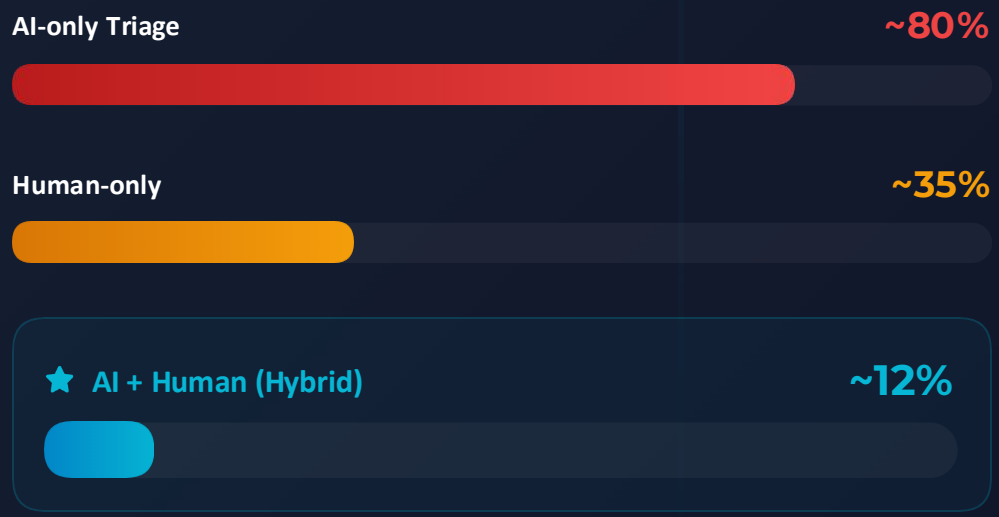
Attacks use legitimate tools — AI sees nothing suspicious

Legal & Ethical Accountability

AI cannot sign an incident report or testify in court

False Positive Rate By Approach

The hybrid advantage



** Illustrative data based on aggregate SOC performance metrics*

Case Studies — Real World Deployment

Where AI won and where humans were irreplaceable

AI Succeeded

Financial Sector

Ransomware Containment

Darktrace autonomously isolated infected endpoints **before the human human analyst saw the first alert**.

4	2,800
Seconds to Isolate	Endpoints Protected

Human Was Irreplaceable

GCC Bank

Insider Threat Detection

AI flagged a finance manager's data access as *'normal'*.

A human analyst cross-referenced behavioral patterns with HR records and an and an upcoming resignation — **uncovering deliberate data exfiltration**.

Personal OSINT Note

Investigating suspicious domains revealed threat actor patterns that required human context, not automation.

Speed belongs to AI — **Judgment belongs to Humans**

The Hybrid Model

The Augmented Analyst — AI as co-pilot, not replacement

AI Does

- Alert investigation
- Correlation & Enrichment
- Automated containment
- Pattern detection

Human Does

- Validation & Context judgment
- Escalation decisions
- Stakeholder comms
- Legal sign-off

= The Augmented SOC

Faster, smarter, and fully accountable

SOAR playbooks now include mandatory **"human gate"** checkpoints before destructive actions.

The Centaur Model

Analyst + AI outperforms both alone (proven in chess, now in cyber)

Gartner Forecast (2028)
SOC functions AI-augmented

40%

Industry Trends — What Research Actually Says

Data forecasting the growing need for augmented human analysts (2024–2028)

ISC² 2024 Report

4.7M

Workforce Gap

Global cybersecurity talent shortage means the field needs more professionals, not fewer.

SANS SOC Survey

71%

Increased Headcount

Of SOC teams grew human staff alongside adopting new AI security tools.

Gartner Forecast

New Roles

Job Creation

AI in security is creating entirely new analyst roles and specializations, not deleting existing ones.

IDC Research

↓34%

Quality Drop

Organizations that replaced human analysts with pure AI saw incident response quality plummet.

Future Skills to Stay Indispensable

What analysts must master to thrive in an AI-augmented SOC

AI Literacy

Understand model outputs, tune thresholds, and critically identify bias. Never accept automated alerts blindly without validation.

Threat Intelligence

Contextualize Indicators of Compromise (IOCs) (IOCs) within the broader geopolitical, industry, industry, and organizational reality.

Adversarial Thinking

Adopt a red team mindset. Think like the attacker to shift from purely reactive defense to proactive threat hunting.

Communication

Master the ability to translate complex technical findings for executives, legal teams, and non-technical stakeholders.

Compliance & Law

Navigate GDPR, NCA, and PDPL. Remember: only a human professional can be held legally accountable for security decisions.

SIEM & SOAR Tuning

Write custom detection rules (like Sigma), actively reduce false positives, and build sophisticated automated playbooks.

Independent Responders

Why freelance security professionals offer what AI never can

Client Trust & Continuity

Clients call a person they trust during a crisis—not an algorithm they cannot understand.

Custom Org Context

A freelancer learns the client's specific environment, internal politics, and unique risk appetite.

Legal Accountability

Only a human professional can legally carry liability, sign incident reports, and testify.

Flexibility & Speed

Independent responders engage same-day—bypassing procurement delays and SLA queues.

From Personal Experience

"Resolving live security incidents requires nuanced judgment, delicate client management, and clear communication—all of which remain uniquely human traits that cannot be automated."

The Human Premium

Organizations that have suffered breaches increasingly turn to independent incident responders for the critical first 24–48 hours—because speed, trust, and accountability matter more than automation during a crisis.

The Verdict — Transform, Not Eliminate

> "The analysts who will be replaced are not those replaced by AI — they are those replaced by analysts who use AI."

- AI will transform the SOC analyst role, role, not replace it
- AI handles volume. Humans handle judgment.
- Growing talent shortage demands more more analysts, not fewer
- Your certs & tool experience are your competitive edge
- Greatest risk is refusing to learn how AI how AI works
- The SOC needs both humans and machines

"Don't fear the machine. **Learn to command it.**"

Questions & Discussion

Let's explore how these changes impact your career path.

Q1 What skill are you most worried AI will make obsolete — and why?

Q2 If you could learn one thing to prepare for an AI-augmented SOC, what would it be?

Q3 Have you used any AI security tools? What surprised you?

Dina Mohamed

Let's Connect

dinamohamed.1404@gmail.com

+973-36518051