برنامج الأمن السيبراني من نتوركات – The Shield 🛡️

رحلتك من التأسيس إلى التخصص في أمن المعلومات

مقدّمة البرنامج

في ظلّ الارتفاع المستمر في معدّلات الهجمات الرقمية حول العالم، أصبح الأمن السيبراني من أكثر المجالات طلبًا في سوق العمل التقني.
صُمّم خصيصًا ليأخذك في رحلة احترافية تبدأ من الصفر وتصل إلى مستوى المحترف، ومن هنا تقدّم لك **شركة نتوركات** برنامجًا تدريبيًا متكاملًا بعنوان **The Shield**، باحتراف (SIEM) من المفاهيم الأساسية وحتى تحليل التهديدات والتعامل مع أنظمة المراقبة الأمنية.

يتكوّن البرنامج من **ثلاث مراحل تدريبية متتابعة** تغطي مختلف أبعاد أمن المعلومات:

1. **CompTIA Security+** – الأساسيات والمفاهيم الجوهرية للأمن السيبراني.
2. **EC-Council Certified SOC Analyst (CSA)** – التطبيق العملي داخل بيئة مركز العمليات الأمنية (SOC).
3. **SIEM Fundamentals: Mastering Splunk & ELK for Beginners** – التخصّص العملي في أدوات المراقبة والتحليل الأمني.

لماذا تختار The Shield؟ من نتوركات

- محتوى مصمم وفق أحدث المعايير الدولية في الأمن السيبراني.
- يشمل جميع المهارات المطلوبة من مستوى المبتدئين إلى محترفي المراقبة والتحليل.
- تدريب عملي باستخدام أدوات حقيقية مثل **Splunk** و **ELK Stack** عبر منصة **Cyber Defenders**.
- دعم فني وتقني مستمر مع تواصل مباشر مع المحاضر.
- تسجيل المحاضرات وإرسالها خلال 24 ساعة من انتهاء الجلسة.
- شهادات حضور مع إمكانية التقدّم للاختبارات الدولية.
- مقدم حصريًا من **Networkat**، المؤسسة الرائدة في التدريب التقني الاحترافي.

التراك الأول: CompTIA Security+

المدة: 20 ساعة تدريبية – المستوى التأسيسي

الموضوعات الرئيسية:

- مفاهيم الأمن الأساسية ومبادئ حماية البيانات.
- أنواع الهجمات والتهديدات الأمنية.
- حماية الأجهزة، التطبيقات، والشبكات.
- إدارة الهوية والمصادقة والتحكم في الوصول.
- مفاهيم التشفير والشهادات الرقمية.
- التوافق التشغيلي والقانوني وإدارة المخاطر.
- استمرارية الأعمال والتعافي من الكوارث.

🔹 هذا التراك مثالي للمبتدئين ويمثل قاعدة الانطلاق للتراكات التالية.

التراك الثاني: EC-Council Certified SOC Analyst (CSA)

المدة: 30 ساعة تدريبية – المستوى المتوسط

الموضوعات الرئيسية:

- بيئة عمل مركز العمليات الأمنية (SOC) وأدوار المحللين.
- مراقبة التهديدات وتحليل السجلات.
- استخدام أدوات **SIEM** مثل **Splunk – OSSIM – ELK**.
- تحديد مؤشرات الاختراق (IOCs) والاستجابة للحوادث.
- تطوير القواعد الأمنية وتحسين أداء المراقبة.
- كتابة التقارير الفنية والتوصيات الأمنية.

🔹 مناسب للراغبين في العمل كمحللي أمن من المستوى الأول والثاني داخل مراكز *SOC*.

التراك الثالث: SIEM Fundamentals – Mastering Splunk & ELK for Beginners

المدة: 32 ساعة تدريبية – المستوى المتقدم
منصة التدريب العملي : Cyber Defenders

وصف التراك:

Security Information and Event Management (SIEM) يقدّم هذا التراك تدريبًا عمليًا متقدمًا لفهم أنظمة وأهميتها في الكشف المبكر عن التهديدات الأمنية.

ELK Stack (Elasticsearch, Logstash, Kibana)و **Splunk** الحقيقية مثل SIEM سيعمل المتدرب على أدوات لتطبيق المفاهيم في بيئة تحاكي مراكز العمليات الأمنية الفعلية.

المحتوى التفصيلي:

- **وعمليات الأمن SIEM مقدمة إلى:**
  - ما هو نظام SIEM؟ ولماذا يُعدّ عنصرًا أساسيًا في استراتيجية الأمن الحديثة؟
  - التعرف على مفهوم الـ CIA Triad (السرية – التكامل – التوفر).
  - الفرق بين الحدث، التنبيه، والحادث الأمني.
  - آلية جمع وتحليل السجلات وتطبيع البيانات.
- **العمل على Splunk:**
  - مكونات Splunk الأساسية (Search Head – Indexer – Forwarder).
  - فهم عملية إدخال البيانات وإنشاء الـ Indexes.
  - استخدام لغة **SPL (Search Processing Language)** للبحث والتحليل.
  - تنفيذ استعلامات لتحديد محاولات الدخول الفاشلة وتحليل سجلات الويب.
  - استخدام الأوامر الإحصائية والتحويلية (stats – chart – timechart).
  - إنشاء لوحات تحكم (Dashboards) وتنبيهات (Alerts) تفاعلية.
- **العمل على ELK Stack (Elastic Stack):**
  - التعرف على مكونات ELK: Elasticsearch، Logstash، Kibana، Beats.
  - استكشاف واجهة Kibana وتحليل السجلات في Discover.
  - إنشاء تصورات بيانية (Pie Charts – Line Graphs – Tables).
  - بناء Dashboard يعرض الأنشطة الأمنية مثل عناوين IP المشبوهة، الطلبات غير المصرح بها، وأصل الهجمات الجغرافي.
- **تحليل الحالات الواقعية:**
  - التحقيق في هجمات الويب الشائعة مثل SQL Injection وXSS.

- تتبع محاولات الاختراق من خلال السجلات وتحليل سلوك المهاجمين.
- تحليل سجلات Windows (مثل PowerShell) لتحديد الأنشطة المشبوهة.
- تتبع تسلسل الأحداث من محاولة تسجيل دخول فاشلة إلى نجاح الاختراق.

- **الصيد التهديدي (Threat Hunting) والتطوير المهني:**
  - مفهوم الصيد التهديدي والفرق بين الأمن الاستباقي والتفاعلي.
  - بناء فرضية وتحليل الأدلة باستخدام أدوات SIEM.
  - محاكاة عملية تحقيق كاملة عبر Cyber Defenders.
  - مراجعة شاملة لأدوات Splunk وELK ومسارات التطور المهني في مجال SOC.

- هذا التراك يُعدّ مرحلة التخصص العملي في البرنامج ويمنحك خبرة ميدانية في تحليل التهديدات وتشغيل أنظمة *SIEM* الاحترافية.

لمن هذا البرنامج؟

- المبتدئون في مجال الأمن السيبراني.
- محللو SOC من المستوى الأول والثاني.
- مهندسو الشبكات والأنظمة الراغبون في الانتقال لمجال الأمن.
- المحترفون الساعون للحصول على شهادات دولية قوية.
- الشركات التي ترغب في تدريب فرقها التقنية على أحدث معايير الأمن.

الأسئلة الشائعة:

هل يشترط خبرة سابقة؟
لا، التراك الأول مخصص للمبتدئين، ويؤهلك لباقي المستويات تدريجيًا +Security.

هل أحصل على شهادة؟
نعم، شهادة حضور لكل تراك، مع إمكانية التقدّم للاختبارات الرسمية .

هل التدريب عملي؟
بشكل كامل – خاصة في تراكَي CSA وSIEM.

هل المحاضرات مسجّلة؟
. نعم، وتُرسل خلال 24 ساعة بعد انتهاء كل جلسة

سجّل الآن

— **Networkat** مع **Cyber Security** ابدأ رحلتك في عالم
رحلة متكاملة من الأساسيات إلى التخصص العملي داخل بيئة مراكز الأمن الاحترافية.
. تعلم، طبّق، وتقدّم نحو مستقبل مهني في واحد من أهم مجالات التكنولوجيا اليوم

🛡️ The Shield – Cyber Security Training Program

Your Complete Journey from Foundations to Professional Threat Analysis

Program Overview

As cyber threats continue to evolve, cybersecurity professionals are in higher demand than ever before.
Networkat proudly presents **The Shield**, a comprehensive, career-oriented training path designed to take you from zero knowledge to advanced hands-on SIEM operations.

The program consists of **three progressive tracks**:

1. **CompTIA Security+** – Build your foundational understanding of cybersecurity.

2. **EC-Council Certified SOC Analyst (CSA)** – Gain practical SOC experience and threat detection skills.

3. **SIEM Fundamentals: Mastering Splunk & ELK for Beginners** – Learn real-world SIEM operations using industry tools.

Why Choose The Shield by Networkat?

- Based on top international cybersecurity standards and frameworks.

- Covers all essential technical and managerial skills from beginner to advanced levels.

- Hands-on training using real SIEM tools like **Splunk** and **ELK Stack** via **Cyber Defenders**.

- Continuous technical and academic support.
- Direct access to instructors and recorded sessions.
- Certificates of completion for each track.
- Delivered exclusively by **Networkat**, a leader in professional tech training.

Track 1: CompTIA Security+

Duration: 20 Hours – Beginner Level

Core Topics:

- Security fundamentals and core protection principles.
- Common attacks, threats, and vulnerabilities.
- Device, application, and network security.
- Identity, authentication, and access control.
- Encryption, certificates, and data integrity.
- Operational and legal compliance.
- Business continuity and disaster recovery.

🔹 *Ideal for beginners, forming the foundation for advanced tracks.*

Track 2: EC-Council Certified SOC Analyst (CSA)

Duration: 30 Hours – Intermediate Level

Core Topics:

- Security Operations Center (SOC) structure and functions.
- Threat monitoring and log analysis.
- Working with SIEM tools (Splunk, OSSIM, ELK).

- Detecting and responding to incidents (IOCs).
- Tuning correlation rules and optimizing alerts.
- Technical reporting and incident documentation.

🔹 *Best suited for Tier I–II SOC Analysts and aspiring incident responders.*

Track 3: SIEM Fundamentals – Mastering Splunk & ELK for Beginners

Duration: 32 Hours – Advanced Level
Practical Labs Platform: Cyber Defenders

Course Description:
This advanced track provides hands-on training in **Security Information and Event Management (SIEM)** systems and their vital role within SOC environments.
Students gain direct experience using **Splunk** and **ELK Stack (Elasticsearch, Logstash, Kibana)** through guided labs and real-world simulations on the **Cyber Defenders** platform.

Detailed Curriculum:

- **Introduction to SIEM and Security Operations**
    - Understanding SIEM architecture and importance in cybersecurity.
    - The CIA Triad and event lifecycle.
    - Events vs. alerts vs. incidents.
    - The role of log collection and normalization.
- **Working with Splunk**
    - Splunk components (Search Head, Indexer, Forwarder).
    - Data ingestion and indexing workflows.
    - Searching and filtering with SPL (Search Processing Language).
    - Querying event data for failed logins, suspicious activity, and web anomalies.
    - Using stats, chart, and timechart commands for analysis and visualization.
    - Creating dashboards and alert systems for continuous monitoring.

- **Working with the ELK Stack**
    - Understanding ELK components: Elasticsearch, Logstash, Kibana, Beats.
    - Navigating the Kibana interface (Discover, Visualize, Dashboard).
    - Building visualizations (pie charts, line graphs, tables).
    - Creating integrated dashboards to monitor threat sources and traffic origins.
- **Practical Case Studies**
    - Detecting SQL Injection, XSS, and Directory Traversal attacks.
    - Identifying attacker IPs through log correlation.
    - Analyzing PowerShell logs for suspicious activity.
    - Tracking user behavior from login attempts to system access.
- **Threat Hunting & Professional Development**
    - Introduction to proactive vs. reactive threat hunting.
    - Forming hypotheses and investigating with SIEM tools.
    - Full scenario simulation using Cyber Defenders labs.
    - Review of Splunk and ELK best practices.
    - Career guidance: SOC roles, skill paths, and next-step certifications (e.g., Splunk Core Certified User).

🔹 *This final track transforms learners into hands-on analysts capable of managing real SIEM systems and investigating live threats.*

Who Should Enroll

- Beginners starting a cybersecurity career.
- Tier I & II SOC Analysts.
- Network or system engineers transitioning into security roles.

- IT professionals pursuing international certifications.
- Organizations training their technical teams in modern security operations.

Frequently Asked Questions

Do I need prior experience?
No — Security+ is beginner-friendly and serves as your entry point.

Will I receive certificates?
Yes, you'll receive completion certificates for each track and may apply for official exams.

Is the course practical?
Absolutely — CSA and SIEM tracks are fully hands-on.

Are sessions recorded?
Yes, and recordings are shared within 24 hours after each session.

Enroll Now

Start your cybersecurity journey with **Networkat's The Shield** —
A complete learning path from foundations to advanced SIEM operations.
Learn, analyze, and protect — step into one of the world's most in-demand tech careers.