CYBERSECURITY GUIDE Publish 2025

تخصصات الأمن السيبراني

دليلك الشامل للمسار المهني والمستقبل الآمن

PRESENTED BY

SULTAN AYED

Cybersecurity Researcher & Specialist

توجية الطلاب لفهم التخصصات والمسارات المطلوبة في سوق العمل 2025

AGENDA

جدول المحتويات

نظرة عامة على هيكل العرض التقديمي

التخصصات السيبرانية الرئيسية

01 اختبار الاختراق
Penetration Testing

02 الاستجابة للحوادث
Incident Response

03 هندسة الأمن
Security Engineering

04 تحليل البرمجيات الخبيثة
Malware Analysis

05 أمن التطبيقات
Application Security

06 أمن السحابة
Cloud Security

07 الأمن الهجومي
Red Team

08 الأمن الدفاعي
Blue Team

09 الاستخبارات السيبرانية
Threat Intelligence

10 الحوكمة والامتثال
GRC

موارد ومسارات إضافية

المسارات التعليمية والشهادات
Roadmaps & Certs

الموارد والمراجع
Resources

توجهات مستقبلية 2025
Future Trends

نصائح للبداية
Tips for Beginners

الختام
Conclusion

اختبار الاختراق

Penetration Testing & Ethical Hacking

التعريف

عملية محاكاة لهجمات الخصوم الحقيقية لاكتشاف الثغرات الأمنيةفي الأنظمة والشبكات والتطبيقات، مع تقديم توصيات إصلاح عملية وقابلة للتنفيذ.

المهام الأساسية

- اختبار اختراق تطبيقات الويب(Web/API) والشبكات (Internal/Cloud).
- استغلال الثغرات ورفع الصلاحيات(Privilege Escalation) بشكل أخلاقي.
- تنفيذ هجمات الهندسة الاجتماعية(بإذن مسبق) لاختبار الوعي.
- كتابة تقارير فنية وتنفيذية مفصلة تتضمن الأدلة(PoC) وطرق المعالجة.

المتطلبات والشهادات(2025)

المستوى المبتدئ:

- TCM-PNPT
- CompTIA PenTest+
- eJPTv2

المستوى المتقدم/ الاحترافي:

- OffSec OSCP
- OffSec OSEP
- SANS GPEN
- OSWE (Web)

المهارات والأدوات المحورية

- Python/Bash Scripting
- Linux/Kali
- Networking TCP/IP
- Active Directory Attacks
- Metasploit Framework
- Burp Suite Pro
- Nmap & Recon
- OWASP Top 10 (2024)

المسار الوظيفي والنمو

Junior Pentester ← Penetration Tester ← Senior Pentester ← Red Teamer / Consultant

الاستجابة للحوادث

Incident Response (DFIR)

التعريف

عملية منظمة لرصد واحتواء وتحليل الحوادث الأمنية والاختراقات فور حدوثها، بهدف تقليل الأضرار واستعادة التشغيل الآمن وفهم الأسباب الجذرية لمنع تكرارها.

المهام الأساسية

- فرز وتحليل الإنذارات الأولية (Triage) وتحديد مدى خطورة الحادث.
- احتواء الهجوم وعزل الأنظمة المصابة، ثم استئصال التهديد بالكامل.
- جمع الأدلة الرقمية من الذاكرة (Memory) والأقراص للتحليل الجنائي (Forensics).
- تطوير خطط الاستجابة (Playbooks) وتوثيق الدروس المستفادة بعد كل حادث.

المتطلبات والشهادات (2025)

المستوى المبتدئ:

- Blue Team Level 1
- EC-Council ECIH
- CompTIA CySA+

المستوى المتقدم/ الاحترافي:

- FOR508 (SANS)
- OffSec OSIR
- GIAC GCFA
- GIAC GCIH

المهارات والأدوات المحورية

- SIEM (Splunk/Sentinel)
- Digital Forensics
- Threat Hunting
- KAPE / Velociraptor
- Volatility (Memory)
- EDR/XDR Analysis
- Malware Triage
- Windows Artifacts

المسار الوظيفي والنمو

SOC Analyst (L1/L2) ← Incident Responder ← DFIR Specialist ← CSIRT Manager / Lead

هندسة الأمن

Security Engineering & Architecture

التعريف

تصميم وبناء وتنفيذ ضوابط أمنية قوية وبنية تحتية مقاومة للهجمات عبر الأنظمة والشبكات والسحابة، مع دمج الأمان في كل مرحلة من مراحل التطوير والتشغيل.

المهام الأساسية

- تبني Zero Trust وتقسيم الشبكات (Segmentation).
- إدارة الهوية والوصول (IAM) والبنية التحتية للمفاتيح العامة (PKI).
- نمذجة التهديدات (Threat Modeling) وهندسة السجلات والمراقبة.
- أتمتة العمليات الأمنية ودمجها في خطوط التطوير (DevSecOps).

المتطلبات والشهادات (2025)

الأساسيات والشهادات التقنية:

- CompTIA Security+
- Vendor (Cisco/Palo Alto)
- CCSP (Cloud)

المستوى المتقدم/ القيادي:

- ISC2 CISSP
- SABSA / TOGAF
- GSEC / GCED

المهارات والأدوات المحورية

- Python Scripting
- Encryption & PKI
- Architecture Design
- Firewalls (NGFW)
- IaC (Terraform)
- Containers / K8s
- CI/CD Pipelines
- SIEM Engineering

المسار الوظيفي والنمو

Security Engineer ← Senior Sec Engineer ← Security Architect ← CISO / Principal Eng

تحليل البرمجيات الخبيثة

Malware Analysis & Reverse Engineering

التعريف

لفهم سلوكها وآلية (Malware) عملية تفكيك ودراسة البرمجيات الخبيثة عملها، بهدف بناء قواعد كشف فعّالة وتطوير دفاعات استباقية ضدها.

المهام الأساسية

- إجراء التحليل الساكن (Static) والديناميكي (Dynamic) للعينات.
- فك التغليف (Unpacking) وتفكيك التشفير (De-obfuscation).
- استخراج مؤشرات الاختراق (IOCs) وتطوير قواعد YARA.
- تتبع عائلات برمجيات الفدية (Ransomware) وسارقي المعلومات (Infostealers).
- كتابة تقارير تحليل معمقة حول قدرات البرمجية الخبيثة وتأثيرها.

المتطلبات والشهادات (2025)

الشهادات التأسيسية:

- TCM-PMAT
- eLearnSecurity eCMAP

المستوى المتقدم/الاحترافي:

- SANS GREM
- SANS FOR610
- OSEE (Advanced)

المهارات والأدوات المحورية

- Assembly x86/x64
- C/C++ Internals
- Windows API
- Ghidra / IDA Pro
- x64dbg / OllyDbg
- Wireshark
- YARA Rules
- Sandbox Evasion

المسار الوظيفي والنمو

Junior Malware Analyst ← Malware Analyst ← Threat Researcher ← Reverse Engineering Lead

أمن التطبيقات

Application Security & DevSecOps

التعريف

لضمان (SDLC)دمج الأمانفي جميع مراحل دورة حياة تطوير البرمجيات (Secure by Design).بناء تطبيقات آمنة من التصميم وحتى التشغيل

المهام الأساسية

- (Threat Modeling).ونمذجة التهديدات (SSDLC)تطبيق ممارسات التطوير الآمن
- (DAST/IAST).وللتطبيقات (SAST)إجراء فحوصات الأمان الآلي للكود
- .وتأمين سلاسل الإمداد (SCA)تحليل مكونات البرمجيات المفتوحة المصدر
- (Containers).والحاويات APIمراجعة الأكواد البرمجية وتأمين واجهات

(2025)المتطلبات والشهادات

المستوى الأساسي:

OWASP Foundations | CASE | GWEB / GSSP

المستوى المتقدم:

GWAPT | OSWE (Advanced Web) | ISC2 CSSLP

المهارات والأدوات المحورية

OWASP Top 10/ASVS | CI/CD Pipelines∞ | Coding (Java/Python/JS)</>

API Security (OAuth/OIDC) | Jenkins/GitLab CI | SonarQube (SAST)

SCA / SBOM | Container Security

المسار الوظيفي والنمو

AppSec Analyst ← AppSec Engineer ← Product Security Lead ← AppSec Architect

أمن السحابة

Cloud Security & Architecture

التعريف

حماية البيئات السحابية (IaaS, PaaS, SaaS) والتطبيقات والبيانات من التهديدات السيبرانية، مع ضمان الامتثال وأمن الهوية وإدارة الوصول.

المهام الأساسية

- تأمين البنية التحتية السحابية وتطبيق مبدأ الامتياز الأقل (Least Privilege) في IAM.
- إدارة أدوات الحماية السحابية الأصلية (CNAPP) مثل CSPM وCWPP.
- تشفير البيانات وإدارة المفاتيح (KMS) وتكوين جدران الحماية السحابية.
- تأمين بيئات الحاويات (Kubernetes/Docker) ككود والبنية التحتية (IaC).

المتطلبات والشهادات (2025)

المستوى الأساسي:

- CCSK
- Azure Fundamentals
- AWS Cloud Practitioner

المستوى المتقدم/التخصصي:

- AWS Security Specialty
- ISC2 CCSP
- CKS (Kubernetes)
- Azure Security (AZ-500)

المهارات والأدوات المحورية

- Terraform (IaC)
- Kubernetes/Docker
- AWS/Azure/GCP
- OPA / Policy as Code
- Linux Containers
- CI/CD Pipelines
- Wiz / Prisma Cloud

المسار الوظيفي والنمو

Cloud Admin/DevOps ← Cloud Security Engineer ← Senior Cloud Sec Eng ← Cloud Security Architect

الأمن الهجومي(Red Team)

Adversary Simulation & Offensive Operations

التعريف

عملية محاكاة لسيناريوهات هجومية معقدة ومستمرة تشبه أساليب الخصوم الحقيقيين(APTs) لقياس جاهزية المؤسسة الدفاعية وكفاءة فرق الاستجابةفي اكتشاف التهديدات وصدها.

المهام الأساسية

- تنفيذ عمليات محاكاة الخصوم(Adversary Emulation) وسيناريوهات التصيد (Phishing).
- الوصول الأولي(Initial Access) والحركة الجانبية (Lateral Movement) داخل الشبكة.
- تجاوز أنظمة الحماية(EDR Evasion) وتطوير برمجيات التحكم والسيطرة (C2).
- التعاون مع الفريق الأزرقPurple Teaming لتحسين الكشف في تمارين.

المتطلبات والشهادات(2025)

الأساسيات القوية:

- eCPPT
- OffSec OSCP

التخصصي /المستوى المتقدم:

- ZeroPoint CRTO / CRTO II
- OffSec OSEP
- OSCE3
- SANS 699

المهارات والأدوات المحورية

- OPSEC & Stealth
- C2 Frameworks (Cobalt Strike/Sliver)
- Active Directory Exploitation
- Malware Dev (C/C++/Nim)
- EDR/AV Bypass
- Social Engineering
- Custom Tooling

المسار الوظيفي والنمو

Pentester ← Red Team Operator ← Senior Red Teamer ← Adversary Simulation Lead

الأمن الدفاعي(Blue Team)

Defensive Security & Operations

التعريف

بناء وصيانة قدرات الرصد والكشف المستمر، والاستجابة الاستباقية للتهديدات لحماية الأصول الرقمية للمؤسسة من الهجمات قبل أو أثناء حدوثها.

المهام الأساسية

- هندسة الكشف(Detection Engineering) وإنشاء قواعد تنبيهات دقيقة.
- ضبط وتحسين أدوات المراقبة(Tuning SIEM/EDR) لتقليل الإيجابيات الكاذبة.
- صيد التهديدات(Threat Hunting) بشكل استباقي للبحث عن مخترقين متخفين.
- رسم خرائط الهجمات باستخدام إطار MITRE ATT&CK وتحسين التغطية الدفاعية.

المتطلبات والشهادات(2025)

المستوى المبتدئ/ المتوسط:

- Microsoft SC-200
- BTL1 (Blue Team L1)
- CompTIA CySA+

المستوى المتقدم/ الاحترافي:

- Splunk Architect
- SANS GMON
- SANS GCIA
- Elastic Certified

المهارات والأدوات المحورية

- Sigma Rules
- KQL / SPL Queries
- SIEM (Splunk/Sentinel)
- Log Analysis
- Network Traffic Analysis (Zeek)
- EDR/XDR Management
- MITRE ATT&CK Framework

المسار الوظيفي والنمو

SOC Analyst (T1) ← SOC Analyst (T2/T3) ← Detection Engineer ← SOC Manager / Lead

الاستخبارات السيبرانية

Cyber Threat Intelligence (CTI) & Analysis

التعريف

جمع وتحليل المعلومات عن التهديدات السيبرانية الحالية والمحتملة، وتحويل البيانات الخام إلى رؤى استخباراتية قابلة للتنفيذ على المستويات الاستراتيجية والعملياتية والتكتيكية لدعم اتخاذ القرار.

المهام الأساسية

- للكشف عن (Dark Web) والويب المظلم (OSINT) مراقبة المصادر المفتوحة التهديدات.
- وتغذية الأنظمة الدفاعية بها (IoCs) إدارة مؤشرات الاختراق.
- MITRE ATT&CK إطار عمل (TTPs) ربط تكتيكات المهاجمين.
- إعداد تقارير استخباراتية تدعم فرق الاستجابة للحوادث والقيادة العليا.

المتطلبات والشهادات (2025)

الشهادات التأسيسية:

- CompTIA CySA+
- EC-Council CTIA

الشهادات المتقدمة:

- CREST CCTIM
- FOR578
- SANS GCTI

المهارات والأدوات المحورية

- STIX/TAXII Standards
- Maltego / MISP
- OSINT Techniques
- Cyber Kill Chain
- YARA Rules
- Python Automation
- Diamond Model
- Technical Writing

المسار الوظيفي والنمو

CTI Analyst ← Senior Threat Analyst ← Intel Team Lead ← Intel Program Manager

الحوكمة والمخاطر والامتثال

Governance, Risk & Compliance (GRC)

التعريف

تخصص إداري واستراتيجي يهدف إلى مواءمة الأنشطة الأمنية مع أهداف العمل، وإدارة المخاطر المؤسسية، وضمان الالتزام باللوائح والقوانين والمعايير الدولية.

المهام الأساسية

- إجراء تقييمات المخاطر (Risk Assessments) وتحديد استراتيجيات المعالجة.
- تطوير وصياغة السياسات والإجراءات الأمنية وضمان تطبيقها.
- إدارة التدقيق الداخلي والخارجي وضمان الامتثال للمعايير (مثل ISO 27001).
- إدارة مخاطر الطرف الثالث (Third-Party Risk Management) والموردين.

المتطلبات والشهادات (2025)

الشهادات الأساسية والمتقدمة:

ISO 27001 LA | ISC2 CGRC | ISACA CRISC | ISACA CISM | OCEG GRCP

فهم المعايير والأطر:

PCI-DSS 4.0 | GDPR / PDPL | NIST CSF 2.0

المهارات المحورية

Business Acumen | Auditing | Risk Analysis | Policy Writing | KPIs & KRIs | Vendor Management | Communication

المسار الوظيفي والنمو

GRC Analyst ← Risk/Compliance Manager ← Head of GRC ← CISO / CRO

المسارات التعليمية والشهادات

(2025)خارطة طريق مبسطة للتخصصات الرئيسية

الأساس المشترك

IT Fundamentals

Network+ / CCNA

Security+

Linux Basics

Python / Scripting

نقطة الانطلاق لجميع *

الأمن الهجومي
Penetration Testing

- مبتدئ: **eJPT / PenTest+**
- متوسط: **OSCP / PNPT**
- متقدم: **OSEP / OSWE**

الأمن الدفاعي
SOC / DFIR

- مبتدئ: **CySA+ / BTL1**
- متوسط: **GCIH / GCFA**
- متقدم: **FOR508 / GREM**

هندسة وأمن السحابة
Cloud / AppSec

- أساسيات: **AWS/Azure Sec**
- تخصصي: **CCSP / GWEB**
- خبير: **CSSLP / Architect**

الحوكمة والمخاطر
GRC / Management

- أساسيات: **ISO 27001 LA**
- إدارة: **CISM / CRISC**
- تنفيذي: **CGRC / CISO**

منصات تدريب عملية موصى بها:

Hack The Box · TryHackMe · RangeForce · Immersive Labs

الموارد والمراجع الأساسية

مجموعة مختارة من المصادر الموثوقة للتطوير المستمر ومواكبة السوق

BOOKMARKS

شهادات وتدريب احترافي

- OffSec OSCP, OSIR
- SANS Institute DFIR, GREM
- EC-Council CEH, ECIH
- TCM Security PNPT

منصات التدريب العملي

- Hack The Box (Labs & Academy)
- TryHackMe (Guided Paths)
- RangeForce (Blue Team)
- LetsDefend (SOC Analysis)

أدلة ومعايير عالمية

- MITRE ATT&CK (TTPs)
- OWASP (Top 10, ASVS, API)
- NIST CSF 2.0 (Framework)
- CIS Benchmarks (Hardening)

تقارير وإحصائيات 2025

- CompTIA State of Cybersecurity
- ISC2 Cybersecurity Workforce Study
- IBM Cost of a Data Breach Report
- Verizon DBIR 2025

مسارات مهنية ووظيفية

- CyberSeek (Job Heatmap)
- SANS Posters (Career Roadmap)
- LinkedIn Learning (Skills)
- Paul Jerimy (Cert Roadmap)

سحابة ومصادر حكومية

- CISA.gov (Resources & Alerts)
- AWS Security (Documentation)
- Microsoft Security (Learn)
- NCA.gov.sa (ضوابط الامن السيبراني)

CAREER PATHWAY
2025 EDITION

المسارات التعليمية والشهادات المهنية

خارطة طريق شاملة لتطوير مهاراتك واعتماد خبرتكفي مجال الأمن السيبراني

المستوى المبتدئ
ENTRY LEVEL

المفاهيم الأساسية

أساسيات الشبكات، أنظمة التشغيل (Linux/Windows)، ومبادئ أمن المعلومات.

الشهادات المقترحة:

- Network+
- CompTIA Security+
- Google Cybersecurity

المستوى المتوسط
PRACTITIONER

المهارات التطبيقية

التعامل مع الحوادث، اختبار الاختراق الأساسي، تحليل السجلات، وأمن السحابة.

الشهادات المقترحة:

- BTL1
- GSEC
- CySA+
- CEH / eJPT

المستوى المتقدم
EXPERT / LEADER

الخبرة والقيادة

إدارة المخاطر، اختبار الاختراق المتقدم، هندسة الأمن، والامتثال للمعايير الدولية.

الشهادات المقترحة:

- CISA
- CISM
- OSCP / OSEP
- CISSP

المسار الأكاديمي والتدريب العملي

أكاديمياً

الدرجات العلمية :بكالوريوس/ماجستير)علوم حاسب، أمن سيبراني، هندسة برمجيات .(منصات التدريب (Labs): HackTheBox, TryHackMe, RangeForce, Blue Team Labs Online.

ابدأ التدريب

ملاحظة :الشهادات المهنية تتطلب تجديداً دورياً للحفاظ على صلاحيتها.

نصائح عملية للبداية والتميّز

Actionable Tips for Success

خطة 90 يوما

اختر تخصصًا واحدًا يناسب شغفك، وضع خطة تعليمية مركزة لمدة 3أشهر بأهداف أسبوعية قابلة للقياس.

بناء معمل منزلي (Home Lab)

لا تكتفِ بالنظر؛ قم بإعداد بيئة افتراضية (VMware/VirtualBox)وجرب الهجمات والدفاعات بنفسك.

المشاريع والتوثيق

نفّذ مشاريع)مثل Keyloggerبسيط أو أداة مسح (وارفع الكود على GitHub. التوثيق هو دليلك الأقوى.

المسابقات والتحديات (CTF)

شارك في مسابقات CTFومنصات Bug Bountyبشكل أخلاقي لتطوير مهارات التفكير خارج الصندوق.

التواصل وبناء العلاقات

تواصل مع المجتمع التقني على LinkedIn وTwitter. الحضورفي المؤتمرات المحلية يفتح أبواب الفرص.

الخبرة المبكرة

ابحث عن فرص تدريب تعاوني (Co-op)أو برامج التلمذة المهنية (Apprenticeships) فهي الاتجاه الأقوى للتوظيف في 2025.

تذكر :الأمن السيبراني هو ماراثون وليس سباق سرعة .الاستمرارية أهم من الكثافة المؤقتة.

"الأمن السيبراني ليس وجهة، بل هو رحلة مستمرة .كن فضولياً،
تعلم كل يوم، وكن أنت الدرع الذي يحمي المستقبل الرقمي"

SULTAN AYED

Cybersecurity Researcher & Specialist