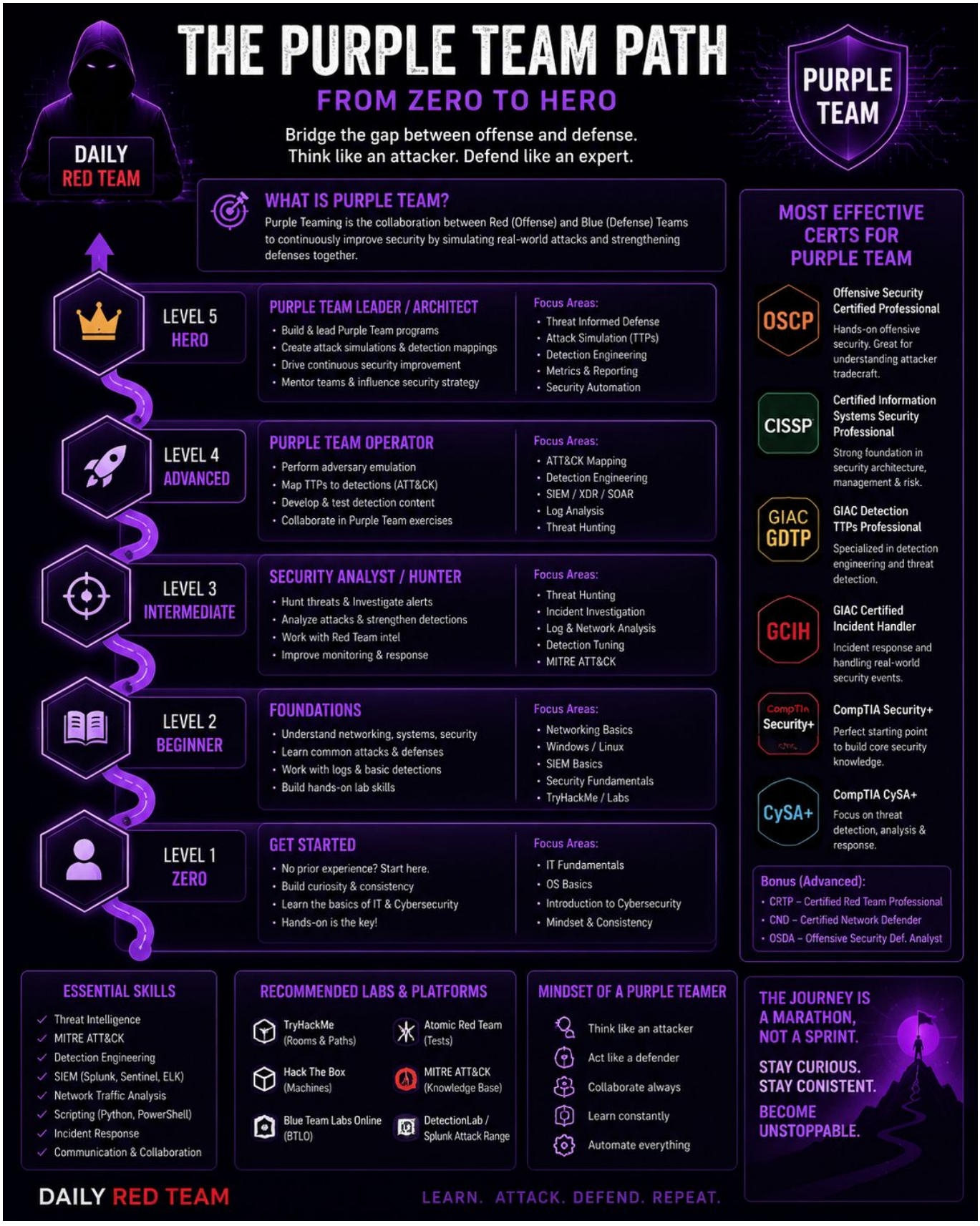
Purple Team


THE PURPLE TEAM PATH
FROM ZERO TO HERO
Bridge the gap between offense and defense.
Think like an attacker. Defend like an expert.
DAILY RED TEAM
PURPLE TEAM
WHAT IS PURPLE TEAM?
Purple Teaming is the collaboration between Red (Offense) and Blue (Defense) Teams to continuously improve security by simulating real-world attacks and strengthening defenses together.
LEVEL 5 HERO
PURPLE TEAM LEADER / ARCHITECT
Build & lead Purple Team programs
Create attack simulations & detection mappings
Drive continuous security improvement
Mentor teams & influence security strategy
Focus Areas:
Threat Informed Defense
Attack Simulation (TTPs)
Detection Engineering
Metrics & Reporting
Security Automation
LEVEL 4 ADVANCED
PURPLE TEAM OPERATOR
Perform adversary emulation
Map TTPs to detections (ATT&CK)
Develop & test detection content
Collaborate in Purple Team exercises
Focus Areas:
ATT&CK Mapping
Detection Engineering
SIEM / XDR / SOAR
Log Analysis
Threat Hunting
LEVEL 3 INTERMEDIATE
SECURITY ANALYST / HUNTER
Hunt threats & Investigate alerts
Analyze attacks & strengthen detections
Work with Red Team intel
Improve monitoring & response
Focus Areas:
Threat Hunting
Incident Investigation
Log & Network Analysis
Detection Tuning
MITRE ATT&CK
LEVEL 2 BEGINNER
FOUNDATIONS
Understand networking, systems, security
Learn common attacks & defenses
Work with logs & basic detections
Build hands-on lab skills
Focus Areas:
Networking Basics
Windows / Linux
SIEM Basics
Security Fundamentals
TryHackMe / Labs
LEVEL 1 ZERO
GET STARTED
No prior experience? Start here.
Build curiosity & consistency
Learn the basics of IT & Cybersecurity
Hands-on is the key!
Focus Areas:
IT Fundamentals
OS Basics
Introduction to Cybersecurity
Mindset & Consistency
MOST EFFECTIVE CERTS FOR PURPLE TEAM
OSCP
Offensive Security Certified Professional
Hands-on offensive security. Great for understanding attacker tradecraft.
CISSP
Certified Information Systems Security Professional
Strong foundation in security architecture, management & risk.
GIAC GDTP
GIAC Detection TTPs Professional
Specialized in detection engineering and threat detection.
GCIH
GIAC Certified Incident Handler
Incident response and handling real-world security events.
CompTIA Security+
CompTIA Security+
Perfect starting point to build core security knowledge.
CySA+
CompTIA CySA+
Focus on threat detection, analysis & response.
Bonus (Advanced):
CRTP – Certified Red Team Professional
CND – Certified Network Defender
OSDA – Offensive Security Def. Analyst
ESSENTIAL SKILLS
Threat Intelligence
MITRE ATT&CK
Detection Engineering
SIEM (Splunk, Sentinel, ELK)
Network Traffic Analysis
Scripting (Python, PowerShell)
Incident Response
Communication & Collaboration
RECOMMENDED LABS & PLATFORMS
TryHackMe (Rooms & Paths)
Atomic Red Team (Tests)
Hack The Box (Machines)
MITRE ATT&CK (Knowledge Base)
Blue Team Labs Online (BTLO)
DetectionLab / Splunk Attack Range
MINDSET OF A PURPLE TEAMER
Think like an attacker
Act like a defender
Collaborate always
Learn constantly
Automate everything
THE JOURNEY IS A MARATHON, NOT A SPRINT.
STAY CURIOUS. STAY CONISTENT.
BECOME UNSTOPPABLE.
DAILY RED TEAM
LEARN. ATTACK. DEFEND. REPEAT.

From:
https://wiki.fortier-family.com/ - **Warnaud's Wiki**

Permanent link:
https://wiki.fortier-family.com/cybersecurity/team/purple

Last update: **2026/09/20 14:06**