

BlackHack Cybersecurity Map

The whole field as one connected map — four teams, every discipline, and the method behind each. Built so an Ethical Hacker can see how the work is actually done, and where to go next.

WHAT IS INSIDE

- 01Start Here — find your path
- 02The Master Map
- 03The four teams, their maps & methods
- 04Careers, certifications & skills
- 05Purple Team Mentality — the signature
- 0637 disciplines, one page each

WHO THIS IS FOR

THE NEWCOMER

Doesn't know where to start. This is the map.

THE PRACTITIONER

Deep in one lane, blind to the others.

THE OPERATOR

Works across lanes, needs the connections.

THE LEADER

Translates all of it to the people who decide.

THE PREMISE

"The industry has a map of attack. Nobody drew the whole field."

MITRE ATT&CK describes one terrain. Six offensive zones had to build their own. This map holds all of it — RED TEAM, BLUE TEAM, GREEN TEAM, PURPLE TEAM — on one canvas, with a page for every discipline and a path for every newcomer.

▶ START HERE // SCAN & CONNECT

Continue Your Cybersecurity Journey

Start with the Academy and the Security+ track, taught through the Purple Team Mentality in cohort-based training. Scan any code below to go straight there.



SCAN OR TAP · blackhackacademy.com

20% OFF ANY BLACKHACK CONTENT

BLACKHACKSTART

Use at checkout · one use per customer · no expiration

The Security+ track and every BlackHack course run through the Academy. Bring the map, use the code, start the climb.

THREE DOORS INTO THE SAME HOUSE



THE COMMUNITY
blackhacksociety.com ↗



THE ACADEMY
blackhackacademy.com ↗



THE GEAR
getblackhack.com ↗

► CONTENTS // JUMP TO ANY SECTION

Table Of Contents

Every entry is a live link — click to jump straight to that section.

The Authorization Boundary	05	Start Here — Find Your Path	06
The Master Map	07	The Framework Map	09
Purple Team Mentality	15	Careers, Certifications & Skills	18
Professional Tradecraft	21	The Lexicon	22
Where To Practice — Free	23	RED TEAM	24
BLUE TEAM	37	GREEN TEAM	49
PURPLE TEAM	64	Framework Index	73
Discipline Index (A-Z)	74	About BlackHack Society	75
Get Involved	76		

► HOW TO READ THIS MAP

One Map, Many Ways In

The disciplines are grouped into four teams. Each team is organized by its own natural shape, so the same field reads differently depending on where you stand. Every discipline gets its own page — mental model, frameworks, method, references, certifications, and the roles that do the work.

RED TEAM — TERRAIN

Organized by what you attack.

BLUE TEAM — CYCLE

Organized by the defensive function loop.

GREEN TEAM — STACK

Organized by layers of the build.

PURPLE TEAM — TRANSLATION

Carries the work to the people affected.

THE SIX PILLARS

Honesty · Integrity · Authenticity · Humility · Accountability · Gratitude

Built evergreen. Mental models and established frameworks are the content. Tools, vendors, and certifications are durable examples, not endorsements — and the map is built to stay true for a year or two without revision.

▶ AUTHORIZED USE ONLY

The Authorization Boundary

BlackHack trains **Ethical Hackers**. The line between a security professional and a criminal is one thing: authorization. This map teaches offensive and defensive tradecraft so you can protect people - never to harm them.

The boundary. This material is for lawful research, isolated labs, sanctioned CTFs, and explicitly authorized security engagements. Do not use it on systems, accounts, networks, data, or identities without documented permission and defined scope. Know and follow the laws that apply to you.

WHERE THE WORK IS ALLOWED

AN ISOLATED LAB YOU OWN

Local VMs, containers, intentionally-vulnerable targets, public datasets - environments you control end to end.

A SANCTIONED CTF / RANGE

Capture-the-flag events and practice ranges that explicitly invite the activity, within their rules.

AN AUTHORIZED ENGAGEMENT

A real target only with documented permission and a defined scope - written authorization, in advance.

THIS IS THE SIX PILLARS, LIVED

Honesty · Integrity · Authenticity · Humility · Accountability · Gratitude

Find Your Path

START HERE // FOUR WAYS IN – EACH CLIMBS THE SAME LADDER

RED TEAM

Want to break things?

Learn how attacks really work.

FOUNDATION

PRACTITIONER

OPERATOR

LEADERSHIP

Security+ → OSCP → Red Team Operator

BLUE TEAM

Want to defend?

Detect, hunt, respond, recover.

FOUNDATION

PRACTITIONER

OPERATOR

LEADERSHIP

Security+ → CySA+ → Threat Hunter / DFIR

GREEN TEAM

Want to build?

Engineer systems that resist attack.

FOUNDATION

PRACTITIONER

OPERATOR

LEADERSHIP

Security+ → CSSLP → Cloud / Platform Security

PURPLE TEAM

Want to lead & translate?

Carry the work to the people who decide.

FOUNDATION

PRACTITIONER

OPERATOR

LEADERSHIP

from RED/BLUE → SEC565 → vCISO / Risk

SOURCES [BHS FRAMING] the on-ramp – four paths, one climb; certs are a dated layer, verify live

© 2026 BlackHack Society – Home for Ethical Hackers. All rights reserved. · blackhacksociety.com · blackhackacademy.com · getblackhack.com
BlackHack Cybersecurity Map, by BlackHack Society. Share it unaltered and with credit. No resale or derivative works without written permission.

START HERE

The Cybersecurity Atlas

MASTER MAP // 37 DISCIPLINES • FOUR TEAMS • ONE VIEW

RED TEAM

organized by terrain • upstream → downstream

Capability Creation

Enterprise & AD Intrusion

Application & Software

Human Layer

Synthetic Media

Physical Pentest

Wireless & RF

Cyber-Physical & Hardware

Crypto & Web3

Criminal Economy

BLUE TEAM

organized by the defensive cycle • Govern → Recover

GRC & Governance

Vuln & Exposure Mgmt

Threat Intelligence

SOC & SecOps

Detection Engineering

Threat Hunting

Incident Response / DFIR

Resilience / BC-DR

Malware Analysis

GREEN TEAM

organized by the build stack • foundation → application

Coding & Scripting

OS Hardening & Internals

IaC & Policy-as-Code

Comms-Sec Engineering

Cloud Security / CNAPP

Container & K8s Security

DevSecOps / Secure SDLC

Supply-Chain Security

Platform Eng / SRE

Application Security

AI Engineering

Security Architecture

PURPLE TEAM

organized by Purple Team Mentality • Attacker • Defender • Victim-Stakeholder

Adversary Emulation

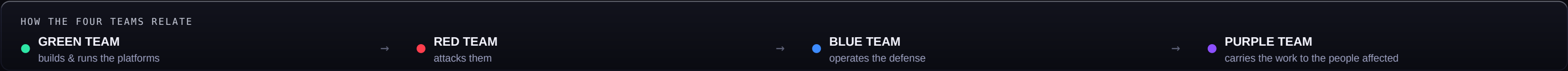
Detection Validation

Threat-Informed Defense

Deception / Engage

Human-Layer Risk Translation

THE HUMAN



Which Teams Touch Which Domain

DOMAIN × TEAM // MOST DOMAINS ARE SHARED

	RED TEAM	BLUE TEAM	GREEN TEAM	PURPLE TEAM
Network & Comms	●	●	●	•
Application & Software	●	●	●	•
Cloud	●	●	●	•
Identity & Access	●	●	●	•
Endpoint	●	●	●	•
Data & Privacy	•	●	●	●
OT / ICS	●	●	●	•
AI / ML	●	●	●	●
Cryptography	●	•	●	•
GRC / Risk	•	●	•	●
Incident Response	•	●	•	●
Threat Intelligence	●	●	•	●

SOURCES [BHS FRAMING] domain-to-team coverage from the map research — modern work crosses colours

© 2026 BlackHack Society — Home for Ethical Hackers. All rights reserved. • blackhacksociety.com • blackhackacademy.com • getblackhack.com
BlackHack Cybersecurity Map, by BlackHack Society. Share it unaltered and with credit. No resale or derivative works without written permission.

Which Framework Governs Which Discipline

FRAMEWORK MAP // EVERGREEN · MAPS METHODS, NOT TOOLS

		ATT&CK	NIST CSF	OWASP	KiLL Chain	PTCERL	Zero Trust	STRIDE	CIS / STIG	SLSA	Pyramid	Intel cycle	ICS / SPARTA	AI RMF	FAIR
RED TEAM	Capability Creation	●	●	●	●		●		●	●	●	●	●	●	●
	Enterprise & AD Intrusion	●	●	●	●		●		●	●	●	●	●	●	●
	Application & Software	●	●	●			●	●	●	●	●	●	●	●	●
	Human Layer	●	●	●	●		●	●	●	●	●	●	●	●	●
	Synthetic Media	●	●	●	●		●	●	●	●	●	●	●	●	●
	Physical Pentest	●	●	●	●		●	●	●	●	●	●	●	●	●
	Wireless & RF	●	●	●	●		●	●	●	●	●	●	●	●	●
	Cyber-Physical & Hardware	●	●	●	●		●	●	●	●	●	●	●	●	●
BLUE TEAM	Crypto & Web3	●	●	●	●		●	●	●	●	●	●	●	●	●
	Criminal Economy	●	●	●	●		●	●	●	●	●	●	●	●	●
	GRC & Governance	●	●	●	●		●	●	●	●	●	●	●	●	●
	Vuln & Exposure Mgmt	●	●	●	●		●	●	●	●	●	●	●	●	●
	Threat Intelligence	●	●	●	●		●	●	●	●	●	●	●	●	●
	SOC & SecOps	●	●	●	●		●	●	●	●	●	●	●	●	●
	Detection Engineering	●	●	●	●		●	●	●	●	●	●	●	●	●
	Threat Hunting	●	●	●	●		●	●	●	●	●	●	●	●	●
GREEN TEAM	Incident Response / DFIR	●	●	●	●	●	●	●	●	●	●	●	●	●	●
	Resilience / BC-DR	●	●	●	●		●	●	●	●	●	●	●	●	●
	Malware Analysis	●	●	●	●		●	●	●	●	●	●	●	●	●
	Coding & Scripting	●	●	●	●		●	●	●	●	●	●	●	●	●
	OS Hardening & Internals	●	●	●	●		●	●	●	●	●	●	●	●	●
	IaC & Policy-as-Code	●	●	●	●		●	●	●	●	●	●	●	●	●
	Comms-Sec Engineering	●	●	●	●		●	●	●	●	●	●	●	●	●
	Cloud Security / CNAPP	●	●	●	●		●	●	●	●	●	●	●	●	●
PURPLE TEAM	Container & K8s Security	●	●	●	●		●	●	●	●	●	●	●	●	●
	DevSecOps / Secure SDLC	●	●	●	●		●	●	●	●	●	●	●	●	●
	Supply-Chain Security	●	●	●	●		●	●	●	●	●	●	●	●	●
	Platform Eng / SRE	●	●	●	●		●	●	●	●	●	●	●	●	●
	Application Security	●	●	●	●		●	●	●	●	●	●	●	●	●
	AI Engineering	●	●	●	●		●	●	●	●	●	●	●	●	●
	Security Architecture	●	●	●	●		●	●	●	●	●	●	●	●	●
	Adversary Emulation	●	●	●	●		●	●	●	●	●	●	●	●	●
PURPLE TEAM	Detection Validation	●	●	●	●		●	●	●	●	●	●	●	●	●
	Threat-Informed Defense	●	●	●	●		●	●	●	●	●	●	●	●	●
	Deception / Engage	●	●	●	●		●	●	●	●	●	●	●	●	●
	Human-Layer Risk Translation	●	●	●	●		●	●	●	●	●	●	●	●	●

Each Team Thinks in a Different Shape

FOUR METHODOLOGIES // TERRAIN • CYCLE • STACK • TRANSLATION

RED TEAM

Kill-chain ARC

Recon

Access

Execute

Persist

Escalate

Move

Impact

BLUE TEAM

CSF CYCLE

Govern

Identify

Protect

Detect

Respond

Recover

GREEN TEAM

Build STACK

Code

OS

Infra

Pipeline

Platform

App

PURPLE TEAM

Validate → translate

Emulate

Detect

Validate

Translate

The Human

SOURCES [BHS FRAMING] the four native geometries – from the BlackHack Cybersecurity Map research [A] NIST CSF (cycle); MITRE ATT&CK (kill chain)

© 2026 BlackHack Society – Home for Ethical Hackers. All rights reserved. • blackhacksociety.com • blackhackacademy.com • getblackhack.com
BlackHack Cybersecurity Map, by BlackHack Society. Share it unaltered and with credit. No resale or derivative works without written permission.

METHODOLOGIES

Six Zones, Six Maps of Attack

WHY MITRE ATT&CK IS ONE MAP OF MANY

MITRE ATT&CK describes **one** terrain. Six offensive zones had to build their own equivalent because the standard map does not reach them.



Enterprise & AD

◇ own matrix: MITRE ATT&CK Enterprise



Cyber-Physical / OT

◇ own matrix: MITRE ATT&CK for ICS



Space / Satellite

◇ own matrix: SPARTA · Aerospace Corp



AI / ML

◇ own matrix: MITRE ATLAS



Wireless / RF

◇ own matrix: RF kill chain



Crypto / Quantum

◇ own matrix: harvest-now-decrypt-later

SOURCES [A] MITRE ATT&CK · ATT&CK for ICS · ATLAS — mitre.org; SPARTA — Aerospace Corp [BHS FRAMING] the six-matrix observation from the map research

© 2026 BlackHack Society — Home for Ethical Hackers. All rights reserved. · blackhacksociety.com · blackhackacademy.com · getblackhack.com

BlackHack Cybersecurity Map, by BlackHack Society. Share it unaltered and with credit. No resale or derivative works without written permission.

SIX MATRICES

From 101 to Leadership

THE CLIMB // FOUNDATION -> LEADERSHIP · CERTS ARE A DATED LAYER

RED TEAM

BLUE TEAM

GREEN TEAM

PURPLE TEAM

LEADERSHIP

- GRC & Governance
 - Resilience / BC-DR
- Security Architecture
- Human-Layer Risk Translation
 - THE HUMAN

OPERATOR

- Capability Creation
 - Criminal Economy
 - Crypto & Web3
 - Cyber-Physical & Hardware
 - Synthetic Media
 - Wireless & RF
- Detection Engineering
 - Incident Response / DFIR
 - Malware Analysis
 - Threat Hunting
 - Threat Intelligence
- AI Engineering
 - Cloud Security / CNAPP
 - Container & K8s Security
 - Platform Eng / SRE
 - Supply-Chain Security
- Adversary Emulation
 - Deception / Engage
 - Detection Validation
 - Threat-Informed Defense

PRACTITIONER

- Application & Software
 - Enterprise & AD Intrusion
 - Physical Pentest
- SOC & SecOps
 - Vuln & Exposure Mgmt
- Application Security
 - Comms-Sec Engineering
 - DevSecOps / Secure SDLC
 - IaC & Policy-as-Code
 - OS Hardening & Internals

FOUNDATION · 101

- Human Layer
- Coding & Scripting

CERTIFICATION CROSSWALK

DATED LAYER · [verify at use](#)

LEADERSHIP

- CISSP
- CISM
- CCISO
- CRISC

OPERATOR

- OSCP
- OSEP
- GXPN
- GCFA

PRACTITIONER

- CySA+
- PenTest+
- GCIH

FOUNDATION

- Security+
- Network+
- CC

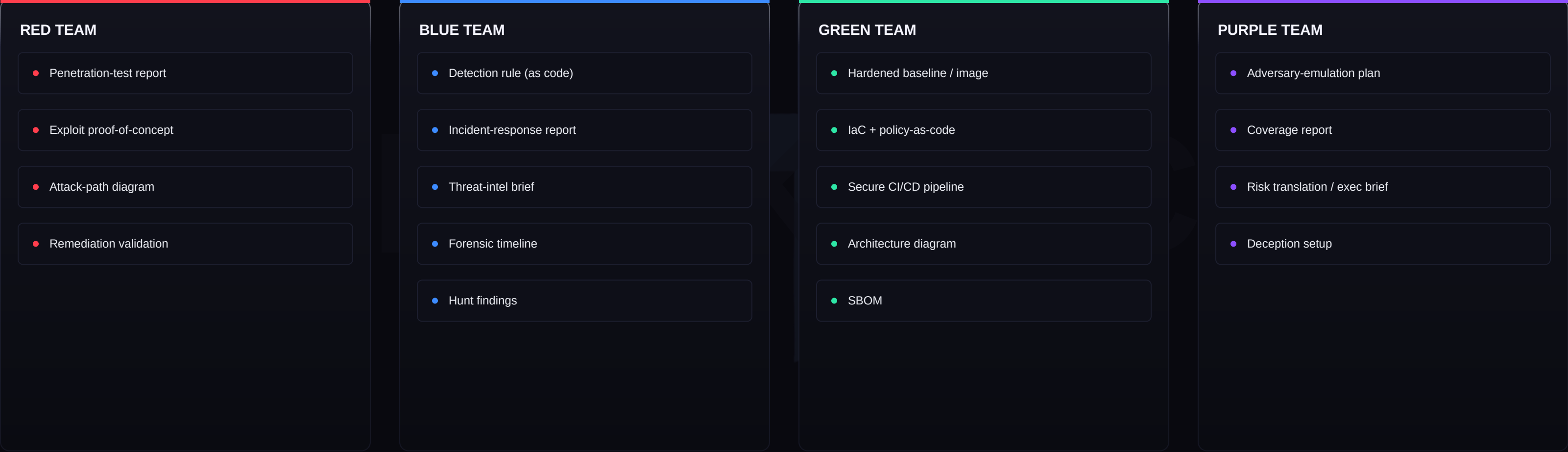
SOURCES [A] Paul Jerim� security certification roadmap – pauljerim�.com [BHS FRAMING] altitude mapping; certs = perishable, verify live

© 2026 BlackHack Society – Home for Ethical Hackers. All rights reserved. · blackhacksociety.com · blackhackacademy.com · getblackhack.com
BlackHack Cybersecurity Map, by BlackHack Society. Share it unaltered and with credit. No resale or derivative works without written permission.

THE CLIMB

What You Actually Produce

PROOF OF WORK // EVERY DISCIPLINE OUTPUTS AN ARTIFACT



SOURCES [BHS FRAMING] proof-of-work artifacts per team – what a portfolio is made of

© 2026 BlackHack Society – Home for Ethical Hackers. All rights reserved. · blackhacksociety.com · blackhackacademy.com · getblackhack.com
BlackHack Cybersecurity Map, by BlackHack Society. Share it unaltered and with credit. No resale or derivative works without written permission.

PROOF OF WORK

The Tools, by Category

TOOL CATEGORIES // CAPABILITIES, NOT BRANDS – EVERGREEN

RED TEAM

C2 / implant framework

Vulnerability scanner

Intercepting proxy

Coverage-guided fuzzer

Exploit framework

OSINT toolkit

BLUE TEAM

SIEM

EDR / XDR / NDR

SOAR

Forensics suite

Malware sandbox

Threat-intel platform

GREEN TEAM

IaC & container scanner

CSPM / CNAPP

Policy engine (PaC)

SAST / DAST / SCA

Secrets scanner

SBOM generator

PURPLE TEAM

Breach-&-attack simulation

Adversary-emulation framework

Coverage tracker

Deception / honeypot

SOURCES [BHS FRAMING] tool categories, not products – brands change, categories endure

© 2026 BlackHack Society – Home for Ethical Hackers. All rights reserved. · blackhacksociety.com · blackhackacademy.com · getblackhack.com
BlackHack Cybersecurity Map, by BlackHack Society. Share it unaltered and with credit. No resale or derivative works without written permission.

TOOL CATEGORIES

Purple Team Mentality

THE SIGNATURE // THREE PERSPECTIVES, HELD AT ONCE
Every operator holds three perspectives at once.

ATTACKER

How real adversaries think, move, and create impact — the offensive truth behind every control.

DEFENDER

How a team detects, investigates, contains, and recovers — the operational reality of the response.

VICTIM / STAKEHOLDER

What the person or organization actually experiences — the human cost, the decisions, the trust on the line.

For an experienced operator, an incident may be routine — something they trained for. For the person affected, it may be the worst day of their professional life. Purple Team Mentality is holding both truths at once, and bringing competence, calm, and care to the room.

THE FIREFIGHTER MODEL

The firefighter model: train before the emergency, specialize to act under pressure, help prevent the next fire — and never forget that the people you serve are not experiencing this as routine.

SOURCES [BHS FRAMING] Purple Team Mentality – BlackHack Society core doctrine

© 2026 BlackHack Society – Home for Ethical Hackers. All rights reserved. • blackhacksociety.com • blackhackacademy.com • getblackhack.com
BlackHack Cybersecurity Map, by BlackHack Society. Share it unaltered and with credit. No resale or derivative works without written permission.

Four Layers Run Through Everything

CROSS-CUTTING // NOT TEAMS – THEY CUT ACROSS ALL FOUR

RED TEAM

BLUE TEAM

GREEN TEAM

PURPLE TEAM

INTELLIGENCE / OSINT

Who, what, why — feeds every attack and every defense.



OPSEC / PRIVACY

Staying unseen and protecting the people in the work.



AI

Target, accelerant, and autonomous actor across all four teams.



SUPPLY CHAIN

The vector into any zone — trust what you build from.



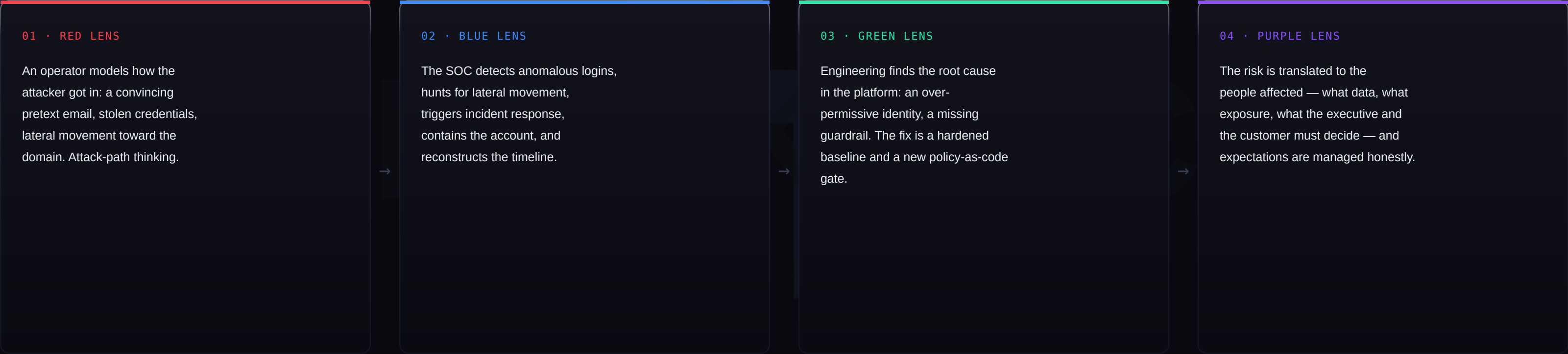
SOURCES [BHS FRAMING] the four cross-cutting layers from the map research

© 2026 BlackHack Society – Home for Ethical Hackers. All rights reserved. · blackhacksociety.com · blackhackacademy.com · getblackhack.com
BlackHack Cybersecurity Map, by BlackHack Society. Share it unaltered and with credit. No resale or derivative works without written permission.

CROSS-CUTTING

One Incident, Four Teams

WORKED EXAMPLE // PHISHING → RECOVERY ACROSS ALL FOUR TEAMS



SOURCES [BHS FRAMING] the four-lens walkthrough – how the teams interlock on one event

© 2026 BlackHack Society – Home for Ethical Hackers. All rights reserved. · blackhacksociety.com · blackhackacademy.com · getblackhack.com
BlackHack Cybersecurity Map, by BlackHack Society. Share it unaltered and with credit. No resale or derivative works without written permission.

Who Does This Work

CAREERS // ROLES BY TEAM & LEVEL

	RED TEAM	BLUE TEAM	GREEN TEAM	PURPLE TEAM
FOUNDATION 0–2 yrs \$	<ul style="list-style-type: none">Junior Penetration TesterSecurity Analyst	<ul style="list-style-type: none">SOC Analyst ISecurity Operations Analyst	<ul style="list-style-type: none">Junior Security EngineerCloud Support Engineer	<ul style="list-style-type: none">— cross-entry from RED / BLUE
PRACTITIONER 2–5 yrs \$\$	<ul style="list-style-type: none">Penetration TesterWeb App PentesterRed Team Analyst	<ul style="list-style-type: none">SOC Analyst IIDetection EngineerIncident ResponderVuln Management Analyst	<ul style="list-style-type: none">Security EngineerDevSecOps EngineerApplication Security Engineer	<ul style="list-style-type: none">Purple Team Engineer
OPERATOR 5–10 yrs \$\$\$	<ul style="list-style-type: none">Red Team OperatorExploit DeveloperAdversary Emulation EngineerVulnerability Researcher	<ul style="list-style-type: none">Threat HunterDFIR LeadCTI AnalystMalware Analyst	<ul style="list-style-type: none">Cloud Security EngineerPlatform Security EngineerSecurity Automation EngineerAI Security Engineer	<ul style="list-style-type: none">Detection Validation EngineerDeception EngineerThreat-Informed Defense Eng
LEADERSHIP 10+ yrs \$\$\$\$	<ul style="list-style-type: none">Offensive Security LeadHead of Red TeamPrincipal Security Researcher	<ul style="list-style-type: none">SOC ManagerDirector of Security OpsCISOGRC / Risk Manager	<ul style="list-style-type: none">Security ArchitectHead of Product SecurityPrincipal Security Engineer	<ul style="list-style-type: none">vCISOSecurity Risk CommunicatorHead of Threat-Informed Defense

SOURCES [BHS FRAMING] role-by-level mapping – evergreen; titles vary by employer

© 2026 BlackHack Society – Home for Ethical Hackers. All rights reserved. · blackhacksociety.com · blackhackacademy.com · getblackhack.com
BlackHack Cybersecurity Map, by BlackHack Society. Share it unaltered and with credit. No resale or derivative works without written permission.

What Proves the Work

CERTIFICATIONS // BY TEAM & LEVEL • EARNED vs TENURED

EARNED vs TENURED

A certification just earned opens the door and proves baseline knowledge. The same certification backed by 3–5 years of doing the work signals mastery — it moves you toward the top of a pay band and toward the next level. Certs accelerate entry and leadership credibility; experience is what converts a cert into seniority. Read every

	RED TEAM	BLUE TEAM	GREEN TEAM	PURPLE TEAM
FOUNDATION 0–2 yrs • \$	<ul style="list-style-type: none">• Security+• Network+	<ul style="list-style-type: none">• Security+• BTL1	<ul style="list-style-type: none">• Security+• Cloud Practitioner	<ul style="list-style-type: none">• (from RED / BLUE base)
PRACTITIONER 2–5 yrs • \$\$	<ul style="list-style-type: none">• eJPT• PenTest+• PNPT	<ul style="list-style-type: none">• CySA+• GCIH• BTL2	<ul style="list-style-type: none">• CSSLP• AWS SAA	<ul style="list-style-type: none">• SANS SEC565
OPERATOR 5–10 yrs • \$\$\$	<ul style="list-style-type: none">• OSCP• OSEP• CRT0• GXPN	<ul style="list-style-type: none">• GCFA• GREM• GCTI• GCIA	<ul style="list-style-type: none">• CCSP• AWS Security• CKS• GDSA	<ul style="list-style-type: none">• SEC699• GRTP• GDAT
LEADERSHIP 10+ yrs • \$\$\$\$	<ul style="list-style-type: none">• OSEE• CISSP	<ul style="list-style-type: none">• CISSP• CISM• GSE	<ul style="list-style-type: none">• CISSP-ISSAP• SABSA	<ul style="list-style-type: none">• Board Risk Comms• CISM• CISA• CRISC

Pay rises with level (left → right), and within a level with tenure. Offensive specialties (RED), cloud & AI engineering (GREEN), and leadership / risk roles (PURPLE • GRC) command the steepest premiums. Tiers are relative and durable — not dollar figures — so this stays true as the market moves.

SOURCES [A] official certification bodies — ISC2 • OffSec • GIAC • CompTIA • ISACA [BHS FRAMING] level mapping; certs = door, experience = seniority

© 2026 BlackHack Society — Home for Ethical Hackers. All rights reserved. • blackhacksociety.com • blackhackacademy.com • getblackhack.com
BlackHack Cybersecurity Map, by BlackHack Society. Share it unaltered and with credit. No resale or derivative works without written permission.

Skills, and Where They Live

SKILLS // MOST CRAFT IS SHARED ACROSS TEAMS

Coding & Scripting	built by GREEN · wielded by RED (tooling) & BLUE (detection-as-code)
Networking & Comms-Sec	built by GREEN · attacked by RED · monitored by BLUE
Cloud	built by GREEN · attacked by RED · monitored by BLUE
Reverse Engineering	RED capability creation ⇄ BLUE malware analysis — same craft, opposite intent
OSINT / Intelligence	feeds RED recon & BLUE threat intelligence
AI / ML Security	built by GREEN · attacked by RED · monitored by BLUE · translated by PURPLE
Detection Engineering	owned by BLUE · validated by PURPLE
Risk Communication	home of PURPLE · shared with BLUE leadership (GRC)
OPSEC / Privacy	cross-cutting — every team
Supply-Chain Security	built by GREEN · exploited by RED · tracked by BLUE

SOURCES [BHS FRAMING] cross-team skill ownership from the map research – modern work crosses colours

© 2026 BlackHack Society – Home for Ethical Hackers. All rights reserved. · blackhacksociety.com · blackhackacademy.com · getblackhack.com
BlackHack Cybersecurity Map, by BlackHack Society. Share it unaltered and with credit. No resale or derivative works without written permission.

The Skills That Aren't Cybersecurity — but Decide Cybersecurity Careers

PROFESSIONAL TRADECRAFT // THE NON-TECHNICAL OPERATOR

<div>Technical Writing & Reporting</div> <div>The #1 career-limiter. Findings are worthless unwritten and unread.</div>	ALL · critical from practitioner up
<div>Communication & Executive Briefing</div> <div>Translate technical truth into a decision, under pressure.</div>	PURPLE · leadership
<div>Data Literacy & Metrics</div> <div>Measure what matters — MTTD/MTTR, exposure, KPIs, risk in numbers.</div>	BLUE · leadership
<div>Stakeholder Management</div> <div>Manage the people, not just the incident. The human layer.</div>	PURPLE core
<div>Project & Program Management</div> <div>Run the engagement; drive remediation to done.</div>	ALL · leadership
<div>Negotiation & Influence</div> <div>Vendor, budget, buy-in — BATNA, ZOPA, anchoring.</div>	PURPLE · leadership
<div>Business & Financial Fluency</div> <div>Risk in dollars — moat, runway, ROI, the capital lane.</div>	leadership
<div>Teaching & Mentorship</div> <div>Raise the people around you; knowledge that outlives you.</div>	senior · ALL
<div>Ethics & Professional Conduct</div> <div>The Six Pillars and the authorization boundary, lived.</div>	ALL · foundation up

SOURCES [BHS CANON] Purple Team Mentality + the Lexicon's leadership/negotiation/capital domains [BHS FRAMING] the non-technical operator – already in BHS doctrine

© 2026 BlackHack Society – Home for Ethical Hackers. All rights reserved. · blackhacksociety.com · blackhackacademy.com · getblackhack.com
BlackHack Cybersecurity Map, by BlackHack Society. Share it unaltered and with credit. No resale or derivative works without written permission.

Words for the Models You Already Think In

THE LEXICON // SELECTED TERMS • THE FULL REFERENCE RUNS 257

<div>blast radius</div> <div>How far damage spreads from a single compromise — the first-, second-, and third-order consequences of one failure.</div>	<div>chokepoint</div> <div>A narrow path every attacker or defender must pass through; control it and you control the flow.</div>	<div>cascade</div> <div>When one failure triggers the next, and the next — a chain reaction across tightly coupled systems.</div>
<div>attack-path</div> <div>The chained route from a first foothold to the objective; attackers think in paths, defenders too often in lists.</div>	<div>bulkhead</div> <div>A deliberate wall that keeps a failure in one compartment from sinking the whole system.</div>	<div>circuit breaker</div> <div>A guard that trips to stop a failing call from cascading, buying the system time to recover.</div>
<div>backpressure</div> <div>Pushing back on upstream load so a flooded system degrades gracefully instead of collapsing.</div>	<div>idempotent</div> <div>An operation safe to repeat — run it once or a hundred times and the result is identical.</div>	<div>error budget</div> <div>The agreed amount of failure you may spend before reliability work must take priority over features.</div>
<div>toil</div> <div>Manual, repetitive operational work with no lasting value — the thing automation exists to eat.</div>	<div>requisite variety</div> <div>A control must be at least as varied as the threats it faces, or it will be out-maneuvered.</div>	<div>second order</div> <div>The consequence of the consequence — what happens after the obvious first effect lands.</div>
<div>reflexive control</div> <div>Shaping an adversary's perception so they choose the move you wanted them to make.</div>	<div>Conway</div> <div>Systems come to mirror the communication structure of the organization that built them.</div>	<div>antifragile</div> <div>Not merely surviving stress but growing stronger because of it.</div>
<div>coupling</div> <div>How tightly parts depend on each other; tight coupling spreads failure, loose coupling contains it.</div>	<div>BATNA</div> <div>Your Best Alternative To a Negotiated Agreement — the walk-away option that sets your true leverage.</div>	<div>ZOPA</div> <div>The Zone Of Possible Agreement — the overlap where a deal can actually be struck.</div>
<div>anchoring</div> <div>The first number quietly frames every number after it; whoever anchors shapes the whole range.</div>	<div>semantic infiltration</div> <div>Winning an argument by slowly redefining its words until your conclusion is built in.</div>	<div>preference falsification</div> <div>People hiding what they really think in public — the gap between stated and true belief.</div>
<div>salience</div> <div>What stands out and seizes attention; good detection raises the salience of what actually matters.</div>		

Where to Practice - Free, on a 16 GB Laptop

PRACTICE // \$0 BASELINE • FREE/OPEN • LOCAL-FIRST

RED TEAM

practice the craft

● OverTheWire

overthewire.org ↗

● picoCTF

picoctf.org ↗

● TryHackMe

tryhackme.com ↗

● Hack The Box

hackthebox.com ↗

● VulnHub

vulnhub.com ↗

● OWASP Juice Shop

owasp.org/www-project-juice-shop ↗

BLUE TEAM

practice the craft

● CyberDefenders

cyberdefenders.org ↗

● Blue Team Labs Online

blueteamlabs.online ↗

● DetectionLab

github.com/clong/DetectionLab ↗

● Splunk BOTS

github.com/splunk ↗

● MalwareBazaar

bazaar.abuse.ch ↗

GREEN TEAM

practice the craft

● Docker (local)

docker.com ↗

● VirtualBox

virtualbox.org ↗

● GitHub

github.com ↗

● Terraform / OpenTofu

opentofu.org ↗

● Cloud free tier

aws.amazon.com/free ↗

PURPLE TEAM

practice the craft

● Atomic Red Team

atomicredteam.io ↗

● MITRE Caldera

caldera.mitre.org ↗

● ATT&CK Navigator

mitre-attack.github.io/attack-navigator ↗

● DetectionLab

github.com/clong/DetectionLab ↗

“BlackHack trains the operator, not their wallet: if a skill is core, there must be a free path to learn, practice, and prove it on a 16 GB laptop.”

SOURCES [A] established free practice platforms - OWASP • MITRE • OverTheWire • community ranges [BHS FRAMING] the \$0 / 16GB lab-accessibility standard

© 2026 BlackHack Society — Home for Ethical Hackers. All rights reserved. • blackhacksociety.com • blackhackacademy.com • getblackhack.com
BlackHack Cybersecurity Map, by BlackHack Society. Share it unaltered and with credit. No resale or derivative works without written permission.

WHERE TO PRACTICE

Offense Is Terrain.

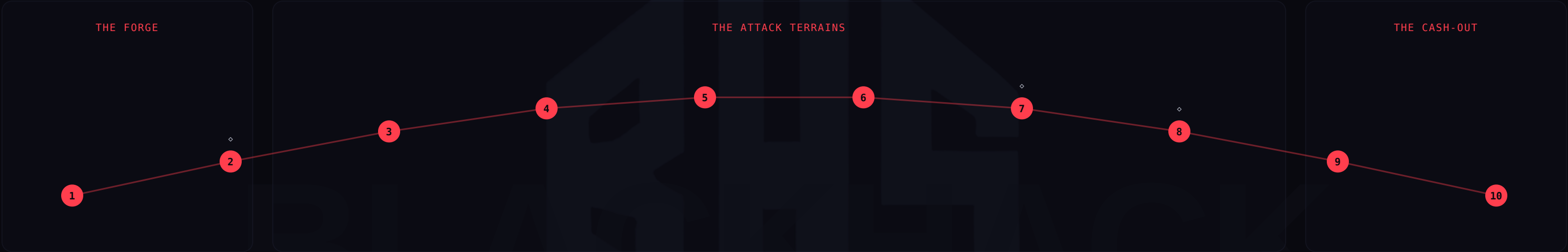
Red is the offensive discipline: understanding and exercising how systems, people, and processes are attacked. Its native geometry is TERRAIN — a landscape of attackable things, from the upstream forge where capability is built, across the attack terrains, to the downstream criminal economy where access becomes money. The reveal of the whole atlas lives here: MITRE ATT&CK, which the industry treats as the map of offense, describes only ONE of these terrains (enterprise intrusion). Six red zones have had to build their own ATT&CK-equivalent matrix because the field's standard map doesn't reach them.

Governing frameworks

MITRE ATT&CK (enterprise + ICS) • Cyber Kill Chain • PTES • OWASP testing guides • SPARTA (space) • ISA/IEC 62443 (OT) • vulnerability-research lifecycle

Offense Is Terrain

RED TEAM // THE ARC — UPSTREAM FORGE → DOWNSTREAM CASH-OUT



- 1

Capability Creation
VR · RE · exploit dev · malware
- 2

Enterprise & AD Intrusion
MITRE ATT&CK Enterprise · ◊ own matrix
- 3

Application & Software
web · API · mobile · cloud off.
- 4

Human Layer
social eng · scams · fraud
- 5

Synthetic Media
deepfake · voice clone · synthetic ID

- 6

Physical Pentest
covert entry · RFID · dropbox
- 7

Wireless & RF
wifi · BLE · cellular · GNSS · ◊ own matrix
- 8

Cyber-Physical & Hardware
OT/ICS · auto · drone · silicon · space · ◊ own matrix
- 9

Crypto & Web3
smart-contract · DeFi · bridges
- 10

Criminal Economy
markets · IABs · RaaS · laundering

SOURCES [BHS FRAMING] RED TEAM native geometry — the upstream-downstream arc

© 2026 BlackHack Society — Home for Ethical Hackers. All rights reserved. · blackhacksociety.com · blackhackacademy.com · getblackhack.com
BlackHack Cybersecurity Map, by BlackHack Society. Share it unaltered and with credit. No resale or derivative works without written permission.

RED TEAM · ANATOMY

Offense Is Terrain

RED TEAM // ORGANIZED BY TERRAIN · UPSTREAM → DOWNSTREAM

UPSTREAM — THE FORGE

Capability Creation

VR · RE · exploit dev · malware

MIDSTREAM — ATTACK TERRAINS

Enterprise & AD Intrusion

MITRE ATT&CK Enterprise

◊ own matrix

Application & Software

web · API · mobile · cloud off.

Human Layer

social eng · scams · fraud

Synthetic Media

deepfake · voice clone · synthetic ID

Physical Pentest

covert entry · RFID · dropbox

Wireless & RF

wifi · BLE · cellular · GNSS

◊ own matrix

Cyber-Physical & Hardware

OT/ICS · auto · drone · silicon · space

◊ own matrix

Crypto & Web3

smart-contract · DeFi · bridges

DOWNSTREAM — CASH-OUT

Criminal Economy

markets · IABs · RaaS · laundering

SOURCES [BHS FRAMING] RED TEAM territory from the BlackHack Cybersecurity Map research

© 2026 BlackHack Society — Home for Ethical Hackers. All rights reserved. · blackhacksociety.com · blackhackacademy.com · getblackhack.com
BlackHack Cybersecurity Map, by BlackHack Society. Share it unaltered and with credit. No resale or derivative works without written permission.

RED TEAM · R-CAP

Capability Creation

The forge.

MENTAL MODEL

The forge. Before any attack happens, someone builds the capability — the exploit, the implant, the tradecraft. You think like a toolmaker: find the flaw, prove it, weaponize it into something reliable and reusable. This sits UPSTREAM of every attack; ATT&CK barely touches it.

METHODOLOGY

1) Reverse the target (binary/protocol/firmware). 2) Discover the flaw (fuzzing, static+dynamic analysis, manual review). 3) Triage & root-cause the crash. 4) Build a reliable primitive (control flow / memory). 5) Defeat mitigations (ASLR/DEP/CFI). 6) Package into a dependable capability.

INTERLOCKS

feeds → every attack terrain (forges their capability) · mirrors ↔ Malware Analysis (same RE craft, opposite intent)

FRAMEWORKS & STANDARDS

Vulnerability research lifecycle (discover → triage → root-cause → PoC → weaponize) · Responsible-disclosure / CVD (coordinated vulnerability disclosure) · CWE (weakness taxonomy) · Memory-safety model (the class of bug determines the class of exploit)

KEY REFERENCES

MITRE CWE — weakness taxonomy [cwe.mitre.org ↗](#)

Exploit-DB — exploit archive [exploit-db.com ↗](#)

Azeria Labs — ARM exploitation [azeria-labs.com ↗](#)

Phrack — underground research zine [phrack.org ↗](#)

CERTIFICATIONS

OSED · OSEE · GXPN

ROLES & JOBS

Vulnerability Researcher · Exploit Developer · Security Researcher

EXAMPLE TOOLS

e.g. IDA Pro · Ghidra (free) · Binary Ninja · AFL/libFuzzer

RED TEAM · R-ENT

I Enterprise & AD Intrusion

◇ OWN MATRIX · ATT&CK

The classic network intrusion — land, look around, move, escalate, persist.

MENTAL MODEL

The classic network intrusion — land, look around, move, escalate, persist. You think in attack PATHS, not asset lists: identity is terrain, and the goal is to chain small footholds into domain control. This is the ONE zone MITRE ATT&CK was built to describe.

METHODOLOGY

Recon the domain → gain initial access → establish execution & persistence → harvest credentials → map trust (who-can-reach-what) → move laterally → escalate to domain/privileged control → act on objective.

INTERLOCKS

validated-by ↔ Detection Engineering (ATT&CK Navigator overlay) · emulated-by → Adversary Emulation · monetized-by → Criminal Economy

FRAMEWORKS & STANDARDS

MITRE ATT&CK Enterprise (14 tactics: recon → resource dev → initial access → execution → persistence → priv-esc → defense evasion → cred access → discovery → lateral movement → collection → C2 → exfil → impact) · Cyber Kill Chain · the identity-as-perimeter model

KEY REFERENCES

MITRE ATT&CK — Enterprise matrix [attack.mitre.org ↗](#)

HackTricks — AD methodology [hacktricks.wiki ↗](#)

SpecterOps — AD attack research [specterops.io ↗](#)

ired.team — red-team notes [ired.team ↗](#)

CERTIFICATIONS

OSCP · OSEP · CRT0 · GPEN

ROLES & JOBS

Penetration Tester · Red Team Operator

EXAMPLE TOOLS

e.g. Cobalt Strike · BloodHound · Impacket · NetExec

RED TEAM · R-APP

Application & Software

Attack the code and the services it exposes.

MENTAL MODEL

Attack the code and the services it exposes. You think in trust boundaries and input: wherever data crosses from untrusted to trusted, there is an edge to test. Spans web, API, mobile, and cloud workloads — each with its own methodology but the same mindset.

METHODOLOGY

Map the attack surface & trust boundaries → enumerate inputs and auth flows → test each boundary (injection, auth, access control, logic) → chain findings → demonstrate impact against a real asset.

INTERLOCKS

mirrors ↔ Application Security (green builds the defenses this attacks) · mirrors ↔ Cloud Security (cloud offense vs cloud built)

FRAMEWORKS & STANDARDS

OWASP Top 10 · OWASP WSTG (Web Security Testing Guide) · OWASP API Security Top 10 · OWASP MASVS/MASTG (mobile) · STRIDE threat model · PTES · the trust-boundary model

KEY REFERENCES

OWASP — Top 10 & testing guides [owasp.org ↗](#)

PortSwigger — Web Security Academy (free) [portswigger.net/web-security ↗](#)

OWASP WSTG — testing methodology [owasp.org/www-project-web-security-testing-guide ↗](#)

CERTIFICATIONS

[OSWE](#) · [BSCP](#) · [GWAPT](#)

ROLES & JOBS

Application Security Engineer · Web App Pentester

EXAMPLE TOOLS

e.g. [Burp Suite](#) · [OWASP ZAP](#) · [Caido](#) · [sqlmap](#)

RED TEAM · R-HUM

I

Human Layer

Attack the person, not the machine.

MENTAL MODEL

Attack the person, not the machine. You think in psychology and pretext: trust, authority, fear, urgency, curiosity. The human is a control that can be social-engineered, and it is present in every organization regardless of its technology.

METHODOLOGY

OSINT the target → craft a credible pretext → choose the vector → make the approach → exploit the trust (credential / access / action) → pivot to the technical layer.

INTERLOCKS

fed-by ← OSINT/Intelligence (recon → pretext) · amplified-by → Synthetic Media · monetized-by → Criminal Economy

FRAMEWORKS & STANDARDS

Social-engineering vectors (phishing · vishing · smishing · physical pretext · media drop) · Cialdini influence principles · the pretext/OSINT→approach→exploit chain · recon-driven targeting

KEY REFERENCES

Social-Engineer.org — framework & research [social-engineer.org ↗](https://social-engineer.org)

SANS SEC467 — social engineering [sans.org ↗](https://sans.org)

OWASP — phishing guidance [owasp.org ↗](https://owasp.org)

CERTIFICATIONS

SANS SEC467

ROLES & JOBS

Social Engineer · Red Team Operator

EXAMPLE TOOLS

e.g. [GoPhish](#) · [Social-Engineer Toolkit](#) · [Evilginx](#)

RED TEAM · R-SYN

I Synthetic Media

Fabricate reality at scale — deepfake voice/video, synthetic identity.

MENTAL MODEL

Fabricate reality at scale — deepfake voice/video, synthetic identity. You think in trust-of-perception: if the victim believes the face, the voice, or the ID is real, the attack lands. A newly-first-class discipline because virtual identity is no longer a reliable trust anchor.

METHODOLOGY

Collect reference material (audio/video/identity data) → generate the synthetic artifact → insert into a social-engineering flow (BEC, verification bypass) → exploit the perception of authenticity.

INTERLOCKS

amplifies → Human Layer · fed-by ← AI (accelerant) · defended-by → identity verification / liveness (blue+green)

FRAMEWORKS & STANDARDS

Synthetic-media attack classes (impersonation · KYC/biometric bypass · synthetic-identity infiltration) · the trust-anchor-collapse model · maps into social-engineering doctrine as an amplifier

KEY REFERENCES

MITRE ATLAS — adversarial AI [atlas.mitre.org ↗](https://atlas.mitre.org)

OWASP — GenAI / deepfake guidance [genai.owasp.org ↗](https://genai.owasp.org)

DARPA SemaFor — media forensics research [darpa.mil ↗](https://darpa.mil)

CERTIFICATIONS

INFERENCE: no established cert yet (emerging lane)

ROLES & JOBS

AI Red Teamer · Fraud / Identity Analyst

EXAMPLE TOOLS

e.g. research-grade generation & detection tooling (fast-moving)

RED TEAM · R-PHY

I

Physical Pentest

Cross the physical boundary to reach the digital one.

MENTAL MODEL

Cross the physical boundary to reach the digital one. You think in layers of physical control — perimeter, door, badge, desk — and in how people hold doors and trust lanyards. The methodology is its own discipline, entirely outside ATT&CK's enterprise matrix.

METHODOLOGY

Recon the site & routines → clone or defeat access control → gain entry (tailgate / bypass / social) → plant a foothold (dropbox / implant) → pivot from physical access to network access.

INTERLOCKS

shares ↔ Human Layer (tailgating/pretext) · pivots-to → Enterprise Intrusion · builds-on ← OPSEC

FRAMEWORKS & STANDARDS

Physical-intrusion methodology (OSINT recon → badge/credential clone → tailgate/bypass → rogue-device drop → pivot to digital) · covert-entry & lock-bypass practice · ASIS physical-security body of knowledge

KEY REFERENCES

- TOOOL — lockpicking community [tool.us](#) ↗
- Red Team Alliance — physical/covert-entry training [redteamalliance.com](#) ↗
- Deviant Ollam — physical security talks [deviating.net](#) ↗

CERTIFICATIONS

Red Team Alliance (physical) · ASIS PSP

ROLES & JOBS

Physical Penetration Tester · Covert Entry Specialist

EXAMPLE TOOLS

e.g. [Proxmark3](#) · [Flipper Zero](#) · lock-bypass sets

RED TEAM · R-RF

Wireless & RF

◊ OWN MATRIX · RF kill chain

Attack the airwaves — wifi, Bluetooth, cellular, GNSS, sub-GHz.

MENTAL MODEL

Attack the airwaves — wifi, Bluetooth, cellular, GNSS, sub-GHz. You think in spectrum and protocol: every signal is an interface, and most were designed for convenience, not adversaries. The field built its OWN kill chain because enterprise ATT&CK doesn't cover radio.

METHODOLOGY

Survey the spectrum → identify the protocol & band → capture/decode traffic → replay or spoof → escalate (evil-twin, GPS spoof, keyfob replay) → pivot or disrupt.

INTERLOCKS

overlaps ↔ Cyber-Physical (GNSS/OT radio) · own-matrix: RF kill chain

FRAMEWORKS & STANDARDS

RF/wireless attack kill chain (spectrum recon → sniff → replay/spoof → jam → inject) · protocol-by-band taxonomy (802.11 · BLE · cellular · GNSS · RFID · sub-GHz) · SDR methodology

KEY REFERENCES

Great Scott Gadgets — SDR (HackRF) greatscottgadgets.com ↗

Aircrack-ng — wifi tooling aircrack-ng.org ↗

GNU Radio — SDR framework gnuradio.org ↗

CERTIFICATIONS

OSWP · GAWN

ROLES & JOBS

Wireless Security Tester · RF Security Researcher

EXAMPLE TOOLS

e.g. [HackRF](#) · [RTL-SDR](#) · [Ubertooth](#) · [Wi-Fi Pineapple](#)

RED TEAM · R-CPS

Cyber-Physical & Hardware

Attack where bits move atoms — industrial control, vehicles, drones, silicon, satellites.

MENTAL MODEL

Attack where bits move atoms — industrial control, vehicles, drones, silicon, satellites. You think in physical process and safety: the goal often isn't data but a pump, a brake, a rotor, a chip. Multiple sub-lanes, each with its OWN framework (OT has ATT&CK-ICS; space has SPARTA).

METHODOLOGY

Map the process & architecture (Purdue levels / segments) → reach the control network → analyze the protocol (Modbus/CAN/etc.) → manipulate the process or defeat the silicon → account for safety/physical consequence.

INTERLOCKS

own-matrix: ATT&CK-ICS · SPARTA · overlaps ↔ Wireless (GNSS/telemetry) · built-by ← green comms-sec/OT

FRAMEWORKS & STANDARDS

MITRE ATT&CK for ICS (OT tactics/techniques) · Purdue Model (OT segmentation levels 0–5) · ISA/IEC 62443 · ISO/SAE 21434 + UNECE WP.29 (automotive) · SPARTA (space) · side-channel & fault-injection models (hardware)

KEY REFERENCES

MITRE ATT&CK for ICS attack.mitre.org/matrices/ics ↗

SANS ICS — OT security ics.sans.org ↗

SPARTA — space attack matrix sparta.aerospace.org ↗

NewAE — ChipWhisperer (hardware) newae.com ↗

CERTIFICATIONS

[GICSP](#) · [GRID](#) · [GICSP](#)

ROLES & JOBS

ICS/OT Security Engineer · Hardware Hacker · Automotive Security Researcher

EXAMPLE TOOLS

e.g. [ChipWhisperer](#) · *protocol analyzers* · *logic analyzers*

RED TEAM · R-WEB3

I Crypto & Web3

Attack value encoded as code — smart contracts, DeFi, bridges.

MENTAL MODEL

Attack value encoded as code — smart contracts, DeFi, bridges. You think in economic logic and immutability: the code IS the bank, bugs are permanent, and exploits pay instantly. A mature discipline with its own vuln taxonomy and audit practice.

METHODOLOGY

Read the contract & its economic assumptions → model the value flows → find a class flaw (reentrancy / oracle / access) → prove it on a fork → quantify extractable value.

INTERLOCKS

monetized-by → Criminal Economy · quantum-exposed ← AI/Supply-Chain cross-cutting (HNDL vs reused keys)

FRAMEWORKS & STANDARDS

Smart-contract vulnerability classes (reentrancy · oracle/price manipulation · access-control failure · front-running/MEV · bridge flaws) · the immutability/economic-incentive model · audit methodology

KEY REFERENCES

OWASP — Smart Contract Top 10 [owasp.org ↗](#)

Solidity — language docs [soliditylang.org ↗](#)

Trail of Bits — crytic/Slither [github.com/crytic ↗](#)

SWC Registry — weakness classification [swcregistry.io ↗](#)

CERTIFICATIONS

INFERENCE: community-driven (e.g. auditor contests); no single standard

ROLES & JOBS

Smart Contract Auditor · Web3 Security Researcher

EXAMPLE TOOLS

e.g. [Slither](#) · [Mythril](#) · [Foundry](#) · [Echidna](#)

RED TEAM · R-ECO

Criminal Economy

The cash-out — what happens AFTER impact.

MENTAL MODEL

The cash-out — what happens AFTER impact. You think like a market: access, data, and extortion are products; there are brokers, franchises, and launderers. This sits DOWNSTREAM of every attack and off the end of ATT&CK (which stops at 'impact').

METHODOLOGY

Convert access/data into a sellable product → route through the ecosystem (broker / affiliate / market) → extort or sell → launder proceeds → reinvest.

INTERLOCKS

monetizes ← every attack terrain · studied-by → Threat Intelligence (blue)

FRAMEWORKS & STANDARDS

Cybercrime ecosystem model (access-gathering → monetization flow) · role taxonomy (initial-access brokers · ransomware-as-a-service · carding · laundering) · forum-tiering · the kill-chain-to-cash-out extension

KEY REFERENCES

Krebs on Security — cybercrime journalism [krebsonsecurity.com ↗](#)

Chainalysis — crypto-crime research [chainalysis.com ↗](#)

NCSC (UK) — ransomware ecosystem [ncsc.gov.uk ↗](#)

CERTIFICATIONS

GCTI (threat intel, adjacent)

ROLES & JOBS

Threat Intelligence Analyst · Dark-Web Analyst

EXAMPLE TOOLS

(reference-depth: intel platforms; no operational tooling)

Defense Is a Cycle.

Blue is the defensive operating discipline: detecting, investigating, responding, and governing. Its native geometry is a CYCLE — the NIST CSF function loop (Govern → Identify → Protect → Detect → Respond → Recover) that runs continuously. Blue OPERATES the tools (green builds them). The whole blue side runs on one shared framework fabric — ATT&CK, the Kill Chain, the Diamond Model, the Pyramid of Pain, STIX/TAXII — several of them the SAME frameworks red uses, which is exactly where purple lives. GRC sits at the top altitude of this cycle, not off in its own corner.

Governing frameworks

NIST CSF 2.0 · ISO/IEC 27001 · MITRE ATT&CK/D3FEND · PICERL / NIST SP 800-61 · Diamond Model · Cyber Kill Chain · Pyramid of Pain · STIX/TAXII · intelligence lifecycle · FAIR

Defense Is a Cycle

BLUE TEAM // THE NIST CSF LOOP – GOVERN → RECOVER



PROTECT is mostly engineered by GREEN TEAM; BLUE operates the detection and response that runs on top.

SOURCES [A] NIST CSF 2.0 – nist.gov/cyberframework [BHS FRAMING] BLUE TEAM native geometry – the function cycle

© 2026 BlackHack Society – Home for Ethical Hackers. All rights reserved. · blackhacksociety.com · blackhackacademy.com · getblackhack.com
BlackHack Cybersecurity Map, by BlackHack Society. Share it unaltered and with credit. No resale or derivative works without written permission.

BLUE TEAM · ANATOMY

Defense Is a Cycle

BLUE TEAM // ORGANIZED BY THE DEFENSIVE CYCLE • GOVERN → RECOVER

GOVERN

GRC & Governance

CSF Govern • ISO27001 • FAIR

IDENTIFY

Vuln & Exposure Mgmt

CTEM • CVSS/EPSS • VEX

Threat Intelligence

intel lifecycle • Diamond • STIX

DETECT

SOC & SecOps

SIEM • SOAR • tiered triage

Detection Engineering

Sigma • detection-as-code

Threat Hunting

PEAK • hypothesis-driven

RESPOND • RECOVER

Incident Response / DFIR

PICERL • forensics • timeline

Resilience / BC-DR

recovery • continuity

CRAFT

Malware Analysis

static • dynamic • RE • YARA

BLUE TEAM · B-GRC

GRC & Governance

Run security as a program, not a pile of tools.

MENTAL MODEL

Run security as a program, not a pile of tools. You think in risk, obligation, and accountability: what must we protect, what are we required to do, who owns the decision. This is the leadership altitude of blue — where technical reality becomes board-level risk.

METHODOLOGY

Set governance & risk appetite → identify assets, obligations, and threats → select & map controls to a framework → measure control effectiveness (continuous) → quantify residual risk → report to leadership → govern the loop.

INTERLOCKS

translates → Purple (risk/exec lane) · governs ↓ every blue function · designed-with ↔ Security Architecture (green)

FRAMEWORKS & STANDARDS

NIST CSF 2.0 (Govern · Identify · Protect · Detect · Respond · Recover) · ISO/IEC 27001 (ISMS) · SOC 2 · FAIR + NIST SP 800-30 (risk quantification) · COSO ERM · the risk-appetite / control-objective model

KEY REFERENCES

NIST Cybersecurity Framework [nist.gov/cyberframework ↗](https://nist.gov/cyberframework)

ISO/IEC 27001 [iso.org ↗](https://iso.org)

FAIR Institute — risk quantification [fairinstitute.org ↗](https://fairinstitute.org)

AICPA — SOC 2 [aicpa.org ↗](https://aicpa.org)

CERTIFICATIONS

CISSP · CISM · CRISC · CISA

ROLES & JOBS

GRC Analyst · Risk Manager · Compliance Manager · CISO

EXAMPLE TOOLS

e.g. GRC / audit-management platforms

BLUE TEAM · B-VEM

Vulnerability & Exposure Mgmt

Know what's exposed and fix what matters first.

MENTAL MODEL

Know what's exposed and fix what matters first. You think in prioritization under scarcity: there are always more vulns than hours, so exploitability and reachability beat raw severity. Maps to the Identify function.

METHODOLOGY

Discover assets & exposures → enrich with threat context (EPSS/KEV) → prioritize by exploitability + business value, not CVSS alone → validate real reachability → mobilize remediation → re-scan.

INTERLOCKS

fed-by ← Threat Intelligence · validated-by ↔ Detection Validation (purple CTEM = purple ops) · remediated-by → green

FRAMEWORKS & STANDARDS

CTEM (Continuous Threat Exposure Mgmt: scope → discover → prioritize → validate → mobilize)
· CVSS (severity) + EPSS (exploit likelihood) + KEV (known-exploited) + VEX (exploitability)
· risk-based prioritization model

KEY REFERENCES

FIRST — CVSS first.org/cvss ↗

FIRST — EPSS first.org/epss ↗

CISA — Known Exploited Vulnerabilities (KEV) cisa.gov/known-exploited-vulnerabilities-catalog ↗

NIST — National Vulnerability Database nvd.nist.gov ↗

CERTIFICATIONS

CySA+ · (exposure-management specialist)

ROLES & JOBS

Vulnerability Management Analyst · Exposure Management Engineer

EXAMPLE TOOLS

e.g. Tenable · Qualys · Rapid7

BLUE TEAM · B-CTI

Threat Intelligence

Turn knowledge of adversaries into decisions.

MENTAL MODEL

Turn knowledge of adversaries into decisions. You think in who/what/why: which actors, which TTPs, aimed at whom — so detection and hunting aim at real threats, not noise. The most framework-structured blue discipline.

METHODOLOGY

Set intelligence requirements → collect (OSINT, feeds, internal) → process & correlate → analyze actors/TTPs → disseminate to the right audience (exec→analyst) → feed detection & hunting → gather feedback.

INTERLOCKS

feeds → Detection Eng, Threat Hunting, Vuln Mgmt · four-intel-types map → Purple cross-lane ladder

FRAMEWORKS & STANDARDS

Intelligence lifecycle (planning → collection → processing → analysis → dissemination → feedback) · Diamond Model · Cyber/Unified Kill Chain · MITRE ATT&CK/D3FEND · STIX/TAXII (exchange) · the four intel types (strategic · operational · tactical · technical)

KEY REFERENCES

MITRE ATT&CK [attack.mitre.org ↗](https://attack.mitre.org)

Lockheed Martin — Cyber Kill Chain [lockheedmartin.com/cyber-kill-chain ↗](https://lockheedmartin.com/cyber-kill-chain)

MISP — threat-intel platform (open) [misp-project.org ↗](https://misp-project.org)

OASIS — STIX/TAXII [oasis-open.org ↗](https://oasis-open.org)

CERTIFICATIONS

GCTI · GCIH

ROLES & JOBS

Cyber Threat Intelligence Analyst · Threat Researcher

EXAMPLE TOOLS

e.g. MISP · Recorded Future · Mandiant

BLUE TEAM · B-SOC

SOC & SecOps

The operational hub — eyes on glass, alert to action.

MENTAL MODEL

The operational hub — eyes on glass, alert to action. You think in triage and tempo: classify fast, escalate what's real, automate the rote. Structured as a five-layer stack (telemetry → detection → investigation → response → reporting).

METHODOLOGY

Ingest telemetry → correlate into alerts → triage (classify / close / escalate) → enrich with context → investigate → respond/contain → report & tune. Automate the repeatable steps.

INTERLOCKS

built-on ← green Platform Eng (telemetry platform) · runs → Detection Eng's analytics · escalates → IR

FRAMEWORKS & STANDARDS

The SOC stack model (telemetry · detection · investigation · response · reporting) · tiered-analyst model (triage → investigate → hunt/engineer) · MTTD/MTTR as the governing metrics · ATT&CK for TTP operationalization

KEY REFERENCES

NIST SP 800-61 — incident handling [csrc.nist.gov ↗](#)

MITRE ATT&CK [attack.mitre.org ↗](#)

SANS — SOC resources [sans.org ↗](#)

CERTIFICATIONS

CySA+ · GSOC · GCIH · BTL1

ROLES & JOBS

SOC Analyst (T1-T3) · Security Operations Engineer

EXAMPLE TOOLS

e.g. SIEM · SOAR · EDR/XDR/NDR

BLUE TEAM · B-DET

Detection Engineering

Build the detections, don't just buy them.

MENTAL MODEL

Build the detections, don't just buy them. You think like a software engineer applied to defense: detections are code — versioned, tested, tuned, measured for coverage. The bridge discipline where red's techniques meet blue's response.

METHODOLOGY

Pick a technique (ATT&CK-mapped, CTI-prioritized) → find the highest-pyramid observable → write the detection as code → test against attack simulations → tune on false-positive rate → deploy → measure coverage → iterate.

INTERLOCKS

validates ↔ Enterprise Intrusion (Navigator) · fed-by ← Malware Analysis (YARA keystone) · pipeline built-by ← green DevSecOps

FRAMEWORKS & STANDARDS

Detection-as-code (version control · peer review · CI/CD · test vs simulation · tune FP/FN) · the Pyramid of Pain (detect at the costly tiers) · ATT&CK coverage mapping · the Alerting & Detection Strategy (ADS) framework · Sigma as a portable detection standard

KEY REFERENCES

SigmaHQ — portable detection rules	github.com/SigmaHQ/sigma ↗
Palantir — Alerting & Detection Strategy framework	github.com/palantir/alerting-detection-strategy-framework ↗
Pyramid of Pain (D. Bianco)	detect-respond.blogspot.com ↗
MITRE ATT&CK	attack.mitre.org ↗

CERTIFICATIONS

GCDA · (detection-engineering specialist)

ROLES & JOBS

Detection Engineer

EXAMPLE TOOLS

e.g. *Sigma* · *SIEM query languages* · *YARA*

BLUE TEAM · B-HUNT

Threat Hunting

Assume breach and go looking.

MENTAL MODEL

Assume breach and go looking. You think in hypotheses: what would an adversary have done that detection missed, and where would the evidence be. Proactive, not alert-driven — it finds the gaps that become new detections.

METHODOLOGY

Form a hypothesis (CTI- or baseline-driven) → scope data sources → search (stack-count, cluster, group, baseline-deviate) → analyze findings → confirm/deny → turn confirmed gaps into detections.

INTERLOCKS

fed-by ← Threat Intelligence (hypotheses) · feeds → Detection Engineering (new coverage) · uses ← DFIR artifacts

FRAMEWORKS & STANDARDS

PEAK framework (Prepare · Execute · Act-with-knowledge) · hunt types (hypothesis-driven · baseline · model-assisted) · SANS Hunting Maturity Model · the Pyramid of Pain (hunt the durable tiers) · Analysis of Competing Hypotheses

KEY REFERENCES

Splunk — PEAK threat-hunting framework [splunk.com ↗](#)

SANS — threat hunting [sans.org ↗](#)

MITRE ATT&CK [attack.mitre.org ↗](#)

CERTIFICATIONS

GCFA · (threat-hunting specialist)

ROLES & JOBS

Threat Hunter

EXAMPLE TOOLS

e.g. Velociraptor · osquery · data-lake/SIEM

BLUE TEAM · B-IR

Incident Response / DFIR

When it's real, work the fire methodically.

MENTAL MODEL

When it's real, work the fire methodically. You think in order-of-volatility and chain-of-custody: contain without destroying evidence, reconstruct what happened, remove the adversary, recover cleanly. Forensics splits by artifact domain.

METHODOLOGY

Prepare (plan/jump-kit) → identify & scope the incident → contain (preserve evidence, order-of-volatility) → eradicate (root-cause, remove) → recover to known-good → run lessons-learned → feed detections.

INTERLOCKS

translates → Purple (incident → stakeholder) · fed-by ← Malware Analysis · reconstructs ← Enterprise Intrusion

FRAMEWORKS & STANDARDS

PICERL (Preparation · Identification · Containment · Eradication · Recovery · Lessons-Learned) = NIST SP 800-61 cycle · NIST SP 800-86 (forensics into IR) · order-of-volatility · forensic artifact domains (memory · disk · network · host · cloud · mobile) · super-timeline analysis

KEY REFERENCES

NIST SP 800-61 — incident response csrc.nist.gov/pubs/sp/800/61 ↗

Volatility Foundation — memory forensics volatilityfoundation.org ↗

13Cubed — DFIR training 13cubed.com ↗

SANS DFIR dfir.sans.org ↗

CERTIFICATIONS

GCIH · GCFA · GCFE · GEIR

ROLES & JOBS

Incident Responder · DFIR Analyst · Forensic Examiner

EXAMPLE TOOLS

e.g. [Volatility](#) · [Autopsy](#) · [Velociraptor](#) · [X-Ways](#)

BLUE TEAM · B-BCDR

Resilience / BC-DR

Plan to survive and recover, not just to prevent.

MENTAL MODEL

Plan to survive and recover, not just to prevent. You think in continuity and worst-case: what keeps running, how fast we restore, what 'acceptable loss' means. The Recover function — often owned at the leadership altitude.

METHODOLOGY

Run a business-impact analysis → set RTO/RPO per service → design recovery & continuity plans → build & test backups/failover → exercise the plan → improve from each test and real event.

INTERLOCKS

governed-by ← GRC · follows ← IR (recovery phase) · depends-on ← green infrastructure

FRAMEWORKS & STANDARDS

Business-continuity & disaster-recovery planning · RT0/RP0 (recovery time/point objectives) · business-impact analysis (BIA) · cyber-resilience model · NIST CSF Recover function

KEY REFERENCES

NIST CSF — Recover function nist.gov/cyberframework ↗

ISO 22301 — business continuity iso.org ↗

DRI International drii.org ↗

CERTIFICATIONS

CBCP (DRI) · ISO 22301 Lead Auditor

ROLES & JOBS

BC/DR Manager · Resilience Engineer

EXAMPLE TOOLS

e.g. backup / replication / failover systems

BLUE TEAM · B-MAL

Malware Analysis

Take the adversary's tool apart to defend against it.

MENTAL MODEL

Take the adversary's tool apart to defend against it. You think like a reverse engineer with a defender's goal: understand behavior, extract indicators, write detections. The keystone artifact (a YARA rule) touches all four teams at once.

METHODOLOGY

Triage the sample → basic static (strings/headers/imports) → unpack if needed → disassemble/decompile → detonate & observe behavior → extract IOCs & behaviors → write YARA + feed CTI/detections.

INTERLOCKS

mirrors ↔ Capability Creation (same RE craft) · feeds → Detection Eng (YARA), CTI (IOCs), DFIR (persistence)

FRAMEWORKS & STANDARDS

The static ⇄ dynamic analysis loop (basic static → advanced static/disassembly → basic dynamic/sandbox → advanced dynamic/debugging) · behavioral analysis · YARA as a detection output · reverse-engineering methodology

KEY REFERENCES

YARA — pattern-matching standard virustotal.github.io/yara ↗

Ghidra — RE suite (NSA, free) ghidra-sre.org ↗

abuse.ch — MalwareBazaar bazaar.abuse.ch ↗

Practical Malware Analysis (No Starch) nostarch.com ↗

CERTIFICATIONS

GREM · (FOR610)

ROLES & JOBS

Malware Analyst · Reverse Engineer

EXAMPLE TOOLS

e.g. Ghidra · IDA Pro · Cuckoo/CAPE sandbox · YARA

Engineering Is a Stack.

Green is the engineering build-and-operate discipline: the platforms, pipelines, infrastructure, and code that red attacks and blue operates. Its native geometry is a STACK — abstraction layers from the foundational code and OS, up through infrastructure, pipeline, platform, to the application. Green's structural signature is SECURITY-AS-CODE: controls shifted left into versioned, automated gates (IaC scanning, policy-as-code, signing). Green is foundational precisely because it's the platform layer underneath both red and blue — and AI engineering is one domain within it, not its center.

Governing frameworks

NIST SP 800-207 (zero trust) · CIS Benchmarks / DISA STIG · OWASP ASVS/SAMM · SLSA (supply chain) · NIST SSDF · Infrastructure-as-Code / Policy-as-Code · the SOC/CNAPP posture models · NIST AI RMF

Engineering Is a Stack

GREEN TEAM // ABSTRACTION LAYERS – FOUNDATION → APPLICATION

APPLICATION

- Application Security

threat modeling · ASVS · SAMM
- AI Engineering

ML0ps · agents · guardrails

PLATFORM

- Platform Eng / SRE

IDP · Backstage · golden paths

PIPELINE

- DevSecOps / Secure SDLC

SAST · DAST · SCA · CI/CD
- Supply-Chain Security

SLSA · sigstore · SBOM

INFRASTRUCTURE

- IaC & Policy-as-Code

Terraform · OPA · Kyverno
- Comms-Sec Engineering

NGFW · SASE · segmentation
- Cloud Security / CNAPP

CSPM · CIEM · CWPP
- Container & K8s Security

admission · Falco · runtime

FOUNDATION

- Coding & Scripting

Python · Go · Rust · PowerShell
- OS Hardening & Internals

CIS · STIG · sysinternals

Security
Architecture

spans every layer

Engineering Is a Stack

GREEN TEAM // ORGANIZED BY THE BUILD STACK · FOUNDATION → APPLICATION

FOUNDATION

Coding & Scripting

Python · Go · Rust · PowerShell

OS Hardening & Internals

CIS · STIG · sysinternals

INFRASTRUCTURE

IaC & Policy-as-Code

Terraform · OPA · Kyverno

Comms-Sec Engineering

NGFW · SASE · segmentation

Cloud Security / CNAPP

CSPM · CIEM · CWPP

Container & K8s Security

admission · Falco · runtime

PIPELINE

DevSecOps / Secure SDLC

SAST · DAST · SCA · CI/CD

Supply-Chain Security

SLSA · sigstore · SBOM

PLATFORM & APP

Platform Eng / SRE

IDP · Backstage · golden paths

Application Security

threat modeling · ASVS · SAMM

AI Engineering

MLOps · agents · guardrails

Security Architecture

zero-trust · SABSA · NIST 800-207

SOURCES [BHS FRAMING] GREEN TEAM territory from the BlackHack Cybersecurity Map research

© 2026 BlackHack Society – Home for Ethical Hackers. All rights reserved. · blackhacksociety.com · blackhackacademy.com · getblackhack.com
BlackHack Cybersecurity Map, by BlackHack Society. Share it unaltered and with credit. No resale or derivative works without written permission.

GREEN TEAM · G-CODE

Coding & Scripting

The foundational craft under everything green.

MENTAL MODEL

The foundational craft under everything green. You think like a builder: automate the repeatable, write the tool when none exists, and treat code as the medium all security work is expressed in. The one skill that touches all four teams — the same languages build red's tools, blue's detections, green's platforms.

METHODOLOGY

Choose the right language for the job → write clear, testable, secure code → automate the repeatable → review for the weakness classes (injection, memory, secrets) → ship as reusable capability.

INTERLOCKS

underlies → every green discipline · builds → red tools / blue detections / green platforms

FRAMEWORKS & STANDARDS

Secure-coding principles (OWASP Secure Coding Practices) · the memory-safety model (language choice is a security decision) · automation-first mindset · language-by-role fit (glue · systems · ops)

KEY REFERENCES

OWASP — Secure Coding Practices owasp.org ↗

SEI CERT — secure coding standards wiki.sei.cmu.edu ↗

The Rust Book / language docs doc.rust-lang.org ↗

CERTIFICATIONS

CSSLP · GPYC

ROLES & JOBS

Security Engineer · Security Automation Engineer

EXAMPLE TOOLS

e.g. Python · Go · Rust · Bash/PowerShell

GREEN TEAM · G-OS

OS Hardening & Internals

Build and operate the operating system so it resists attack by default.

MENTAL MODEL

Build and operate the operating system so it resists attack by default. You think in baselines and least-function: every service, port, and privilege is attack surface until justified. Closest green zone to deep systems knowledge.

METHODOLOGY

Start from a benchmark baseline → disable unneeded services/functions → enforce least privilege & MAC → enable audit logging → bake into a golden image → deploy immutable → monitor drift.

INTERLOCKS

hardens → what red attacks · built-with ← IaC/Config-mgmt · feeds ↑ the whole stack

FRAMEWORKS & STANDARDS

CIS Benchmarks (consensus hardening baselines) · DISA STIG (prescriptive baselines) · the least-privilege / least-function model · golden-image lifecycle (build-hardened → immutable → deploy) · the five Linux hardening layers (kernel · services · accounts · MAC · audit)

KEY REFERENCES

CIS Benchmarks — hardening baselines cisecurity.org/cis-benchmarks ↗

DISA STIGs public.cyber.mil/stigs ↗

Microsoft — security baselines learn.microsoft.com ↗

CERTIFICATIONS

RHCSA · Linux+ · CSSLP

ROLES & JOBS

Systems Security Engineer · Hardening Engineer

EXAMPLE TOOLS

e.g. Ansible · OpenSCAP · Lynis

GREEN TEAM · G-IAC

IaC & Policy-as-Code

Define infrastructure and its guardrails as versioned code.

MENTAL MODEL

Define infrastructure and its guardrails as versioned code. You think in declarative desired-state and prevention-at-the-gate: misconfiguration is caught before deploy, not after breach. The structural heart of green's 'security-as-code' signature.

METHODOLOGY

Declare infrastructure as code → scan it against benchmarks pre-deploy → encode policy as code → enforce at the gate (plan/admission/CI) → version everything → let compliance evidence generate itself.

INTERLOCKS

enforces → OS/Cloud/K8s hardening · gates ← DevSecOps pipeline · signature of green = security-as-code

FRAMEWORKS & STANDARDS

Infrastructure-as-Code (declarative, versioned, idempotent) · Policy-as-Code (guardrails not gates) · GitOps · the shift-left model · compliance-as-code (controls → auto evidence)

KEY REFERENCES

Open Policy Agent — policy-as-code openpolicyagent.org ↗

HashiCorp — Terraform docs developer.hashicorp.com/terraform ↗

CIS Benchmarks cisecurity.org ↗

CERTIFICATIONS

HashiCorp Terraform Associate · CDP (DevSecOps)

ROLES & JOBS

DevSecOps Engineer · Cloud/Platform Security Engineer

EXAMPLE TOOLS

e.g. Terraform/OpenTofu · OPA · Checkov · Kyverno

GREEN TEAM · G-NET

Comms-Sec Engineering

Build and run the network so communication is secure by design.

MENTAL MODEL

Build and run the network so communication is secure by design. You think in segmentation and identity-as-policy: who can talk to what, over what, verified how.
Networking/firewalls/cloud-edge as a build-and-operate discipline, not just defense.

METHODOLOGY

Map flows & trust zones → segment by need (least connectivity) → enforce identity-aware policy at the edge → encrypt in transit (mTLS) → converge network + security controls → monitor and tighten.

INTERLOCKS

builds → the terrain Wireless/RF attacks · designed-by ← Security Architecture · segments ↑ everything

FRAMEWORKS & STANDARDS

Zero-trust networking (NIST SP 800-207) · segmentation ladder (VLAN → micro-segmentation → ZT segmentation) · SASE/SSE convergence (network + security as one edge) · defense-in-depth · the identity-as-primary-policy model

KEY REFERENCES

NIST SP 800-207 — Zero Trust Architecture csrc.nist.gov ↗

CIS Benchmarks cisecurity.org ↗

Cloudflare — Zero Trust learning cloudflare.com/learning ↗

CERTIFICATIONS

CCNP Security · GDSA

ROLES & JOBS

Network Security Engineer · Security Architect

EXAMPLE TOOLS

e.g. next-gen firewalls · SASE/ZTNA · segmentation controllers

GREEN TEAM · G-CLOUD

Cloud Security / CNAPP

Build and secure what runs in the cloud.

MENTAL MODEL

Build and secure what runs in the cloud. You think in shared-responsibility and attack-PATH: a misconfig + a vuln + an over-permissive role is one critical path, not three medium findings — the same graph thinking red uses, applied defensively.

METHODOLOGY

Establish the shared-responsibility line → baseline config against benchmarks (CSPM) → right-size identity entitlements (CIEM) → protect workloads at runtime (CWPP) → correlate findings into attack paths (CNAPP) → remediate the paths first.

INTERLOCKS

mirrors ↔ Application (cloud offense) · CIEM feeds → blue identity detection (ITDR) · built-on ← IaC

FRAMEWORKS & STANDARDS

Shared-responsibility model · the posture-management pillars (config/CSPM · workload/CWPP · identity/CIEM · data · AI) · CNAPP (attack-path correlation) · CIS cloud benchmarks · least-privilege IAM

KEY REFERENCES

Cloud Security Alliance cloudsecurityalliance.org ↗

CIS — cloud benchmarks cisecurity.org ↗

AWS / Azure / GCP security documentation docs.aws.amazon.com ↗

CERTIFICATIONS

[AWS Security Specialty](#) · [CCSP](#) · [Azure SC-100](#)

ROLES & JOBS

Cloud Security Engineer · Cloud Security Architect

EXAMPLE TOOLS

e.g. Wiz · Prisma Cloud · Microsoft Defender for Cloud · Prowler (open)

GREEN TEAM · G-K8S

Container & K8s Security

Secure the container from image to runtime.

MENTAL MODEL

Secure the container from image to runtime. You think in the image→admission→runtime lifecycle: catch it in CI, reject it at deploy, detect it at runtime. A distinct discipline because orchestration has its own trust and policy model.

METHODOLOGY

Scan images in CI (pre-push) → enforce admission policy at deploy (signatures, non-root, limits) → detect anomalies at runtime (unexpected syscalls/processes) → harden the cluster to the benchmark.

INTERLOCKS

built-on ← IaC/Policy-as-Code · hardens → cloud workloads · runtime feeds → blue detection

FRAMEWORKS & STANDARDS

The container lifecycle model (build/scan → admission control → runtime detection) · CIS Kubernetes & Docker Benchmarks · admission-control policy (reject non-compliant) · runtime behavioral detection (syscall-level)

KEY REFERENCES

Kubernetes — security docs kubernetes.io/docs/concepts/security ↗

CNCF cncf.io ↗

Falco — runtime security (CNCF) falco.org ↗

CIS Kubernetes Benchmark cisecurity.org ↗

CERTIFICATIONS

CKS (Certified Kubernetes Security Specialist)

ROLES & JOBS

Container Security Engineer · Platform Security Engineer

EXAMPLE TOOLS

e.g. Falco · Trivy · Kyverno/OPA Gatekeeper

GREEN TEAM · G-DEVSEC

I DevSecOps / Secure SDLC

Build security INTO the pipeline, not onto the product.

MENTAL MODEL

Build security INTO the pipeline, not onto the product. You think in shift-left and gates-as-guardrails: every stage of delivery is a place to catch a class of flaw cheaply. The canonical 'security-as-code' delivery discipline.

METHODOLOGY

Embed a security gate at each pipeline stage → order scanning by signal (secrets → dependency → source → IaC → container → runtime) → fail fast, guide the developer → measure maturity → tune gates toward guardrails.

INTERLOCKS

builds → blue's detection pipeline · consumes → Supply-Chain Security · gated-by ← IaC/Policy-as-Code

FRAMEWORKS & STANDARDS

The secure SDLC / DevSecOps pipeline model (plan → code → build → test → release → deploy → operate → monitor, gate each) · the scanning taxonomy (secrets → SCA → SAST → IaC → container → DAST) · NIST SSDF · OWASP maturity models (SAMM/DSOMM)

KEY REFERENCES

OWASP — DevSecOps guideline [owasp.org ↗](#)

NIST SP 800-218 — Secure SW Dev Framework [csrc.nist.gov/pubs/sp/800/218 ↗](#)

OWASP SAMM — maturity model [owaspsamm.org ↗](#)

CERTIFICATIONS

CSSLP · CDP/CDE (DevSecOps)

ROLES & JOBS

DevSecOps Engineer · Application Security Engineer

EXAMPLE TOOLS

e.g. [Semgrep](#) · [SonarQube](#) · [dependency scanners](#) · [secrets scanners](#)

GREEN TEAM · G-SUPPLY

Supply-Chain Security

Trust what you build FROM, not just what you build.

MENTAL MODEL

Trust what you build FROM, not just what you build. You think in provenance and attestation: every dependency, image, and build step is a place an adversary can get in before you ship. A discipline that hardened sharply after real-world build-system attacks.

METHODOLOGY

Inventory dependencies (SBOM) → verify provenance of every artifact → sign builds & require signature verification → raise the SLSA level → monitor for dependency compromise.

INTERLOCKS

feeds → DevSecOps · cross-cutting with ← Supply-Chain band (spans all teams) · studied-by → CTI

FRAMEWORKS & STANDARDS

SLSA (Supply-chain Levels for Software Artifacts – provenance ladder) · software signing & attestation (keyless signing · in-toto) · SBOM (CycloneDX/SPDX) · the provenance/integrity model

KEY REFERENCES

SLSA — supply-chain integrity levels [slsa.dev ↗](#)

Sigstore — signing & attestation [sigstore.dev ↗](#)

CycloneDX — SBOM standard [cyclonedx.org ↗](#)

in-toto — supply-chain attestation [in-toto.io ↗](#)

CERTIFICATIONS

INFERENCE: emerging; no single standard yet

ROLES & JOBS

Supply Chain Security Engineer · Software Security Engineer

EXAMPLE TOOLS

e.g. *Sigstore/Cosign* · *Syft/Grype* · *SBOM generators*

GREEN TEAM · G-PLAT

I Platform Eng / SRE

Build the paved road everyone else drives on.

MENTAL MODEL

Build the paved road everyone else drives on. You think in self-service and reliability: make the secure way the easy way, and keep it running within an error budget. The platform layer red attacks and blue operates — so it's security-critical by construction.

METHODOLOGY

Treat the platform as a product → build golden paths with security baked in → offer self-service over tickets → set SLOs & error budgets → operate reliably → fold security guardrails into the paved road.

INTERLOCKS

builds → blue's SOC telemetry platform · is-itself → a red target (over-scoped service accounts)

FRAMEWORKS & STANDARDS

Internal Developer Platform (IDP) as a product · golden paths / paved roads · SRE reliability model (SLI/SLO/error budget) · GitOps · the three-role seam (DevOps · SRE · Platform Eng)

KEY REFERENCES

Platform Engineering community platformengineering.org ↗

Google — SRE Book (free) sre.google ↗

Backstage — internal developer platform (CNCF) backstage.io ↗

CERTIFICATIONS

(SRE / cloud-platform vendor certs)

ROLES & JOBS

Platform Engineer · Site Reliability Engineer

EXAMPLE TOOLS

e.g. Backstage · Argo CD · Crossplane

GREEN TEAM · G-APPSEC

Application Security

Design and verify software to resist the attacks red will try.

MENTAL MODEL

Design and verify software to resist the attacks red will try. You think in threat models and secure-by-design: anticipate the abuse case before the feature ships. The defensive mirror of red's application offense.

METHODOLOGY

Threat-model the design (STRIDE) → define security requirements (ASVS) → build in controls → verify by testing → track maturity (SAMM) → feed findings back into design.

INTERLOCKS

mirrors ↔ Application (red attacks what this defends) · verified-by ↔ red app testing · gated-in ← DevSecOps

FRAMEWORKS & STANDARDS

STRIDE / PASTA threat modeling · OWASP ASVS (verification standard) · OWASP SAMM (maturity) · OWASP Top 10 → architectural controls · secure-by-design / SSDLC

KEY REFERENCES

OWASP ASVS — verification standard owasp.org/www-project-application-security-verification-standard ↗

OWASP SAMM owaspsamm.org ↗

OWASP — Threat Modeling owasp.org/www-community/Threat_Modeling ↗

OWASP Top 10 owasp.org/Top10 ↗

CERTIFICATIONS

CSSLP · GWEB

ROLES & JOBS

Application Security Engineer · Product Security Engineer

EXAMPLE TOOLS

e.g. Semgrep · *dependency scanners* · *threat-modeling tooling*

GREEN TEAM · G-AI

AI Engineering

Build AI systems and the guardrails that keep them safe.

MENTAL MODEL

Build AI systems and the guardrails that keep them safe. You think in input/output control and the new attack surface: a model is a component that can be manipulated, leak, or be poisoned. The newest green discipline — one domain of green, not its center.

METHODOLOGY

Build the AI system (model + retrieval + agent) → add input guardrails (prompt-injection, PII) → add output guardrails (leak, toxicity, format) → evaluate & trace → govern against a framework → monitor the posture.

INTERLOCKS

mirrors ↔ Application (AI/LLM offense, ATLAS) · monitored-by → blue AI-SPM · four-team AI loop

FRAMEWORKS & STANDARDS

AI/LLM security frameworks (OWASP Top 10 for LLM Apps · OWASP ML Top 10) · NIST AI RMF · the guardrails model (input guardrails + output guardrails) · MLOps→LLM0ps→Agent0ps maturity · AI security posture management

KEY REFERENCES

OWASP — Top 10 for LLM Applications genai.owasp.org ↗

NIST — AI Risk Management Framework nist.gov/itl/ai-risk-management-framework ↗

MITRE ATLAS atlas.mitre.org ↗

CERTIFICATIONS

INFERENCE: emerging (e.g. CompTIA SecAI+ · ISACA AAISM)

ROLES & JOBS

AI Security Engineer · ML Security Engineer

EXAMPLE TOOLS

e.g. model guardrail libraries · eval/observability tooling

GREEN TEAM · G-ARCH

Security Architecture

Design the whole system to be secure before it's built.

MENTAL MODEL

Design the whole system to be secure before it's built. You think in trust, layering, and failure: assume breach, segment blast radius, and make the default posture safe. The design discipline that spans every green layer and meets GRC at the top.

METHODOLOGY

Define trust boundaries & assume-breach posture → design layered controls (defense-in-depth) → segment to limit blast radius → map to a control framework → review designs → carry zero-trust from greenfield / overlay on brownfield.

INTERLOCKS

spans → all green layers · meets ↔ GRC (design ≠ governance) · bounds → blast radius for purple

FRAMEWORKS & STANDARDS

Zero-trust architecture (NIST SP 800-207) · defense-in-depth · SABSA (enterprise security architecture) · the blast-radius/bulkhead model · control-framework mapping (CSF/CIS/ISO)

KEY REFERENCES

NIST SP 800-207 — Zero Trust Architecture [csrc.nist.gov ↗](https://csrc.nist.gov)

SABSA — enterprise security architecture [sabsa.org ↗](https://sabsa.org)

The Open Group — architecture frameworks [opengroup.org ↗](https://opengroup.org)

CERTIFICATIONS

CISSP-ISSAP · SABSA SCF · TOGAF

ROLES & JOBS

Security Architect · Enterprise Security Architect

EXAMPLE TOOLS

e.g. architecture-modeling methods & reference architectures

► PURPLE TEAM • NATIVE GEOMETRY: FIELD + BRIDGE

Translation to the Human.

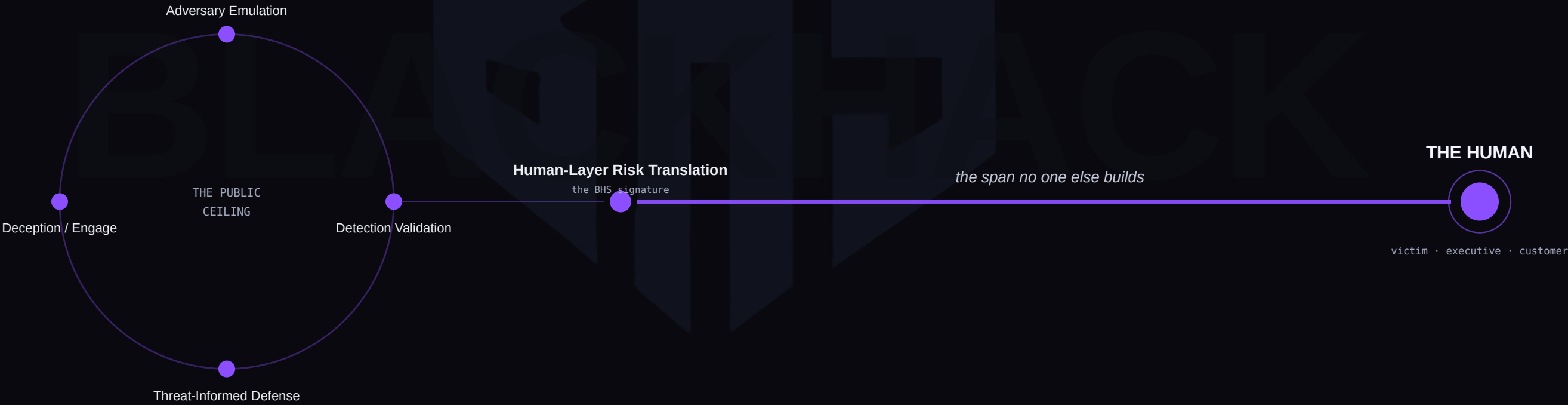
Purple is the integrating discipline — and BlackHack's crown jewel. Its native geometry is a FIELD WITH A VECTOR: a connective WEAVE binding red, blue, and green (it lives in the seams — the ATT&CK Navigator overlay, the YARA keystone, the shared framework fabric), PLUS one bright BRIDGE that crosses to the human. The public field's purple discipline is real but stops at detection coverage — adversary emulation, validation, threat-informed defense, deception. BlackHack's purple extends past that ceiling through the stakeholder/victim perspective and the cross-lane human translation that no public framework models. That extension is the signature.

Governing frameworks

Threat-informed defense (MITRE CTID) • MITRE ATT&CK/D3FEND/Engage • breach-and-attack-simulation / validation loop • adversary-emulation plans • BHS cross-lane translation ladder • order-effects / blast-radius model

Translation to the Human

PURPLE TEAM // THE VALIDATION LOOP – THEN THE BRIDGE NO ONE ELSE BUILDS



SOURCES [BHS FRAMING] PURPLE TEAM native geometry – public validation loop + the human-layer bridge (crown jewel)

© 2026 BlackHack Society – Home for Ethical Hackers. All rights reserved. · blackhacksociety.com · blackhackacademy.com · getblackhack.com

BlackHack Cybersecurity Map, by BlackHack Society. Share it unaltered and with credit. No resale or derivative works without written permission.

Translation to the Human

PURPLE TEAM // ORGANIZED BY PURPLE TEAM MENTALITY • ATTACKER • DEFENDER • VICTIM-STAKEHOLDER

BASE – THE VALIDATION LOOP

Adversary Emulation

CTID library • Caldera

Detection Validation

BAS • VECTR • atomic tests

Threat-Informed Defense

ATT&CK • D3FEND

Deception / Engage

honeypots • MITRE Engage

THE SIGNATURE – HUMAN-LAYER TRANSLATION

Human-Layer Risk Translation

BHS signature • cross-lane • victim experience

THE HUMAN

the span no one else builds

SOURCES [BHS FRAMING] PURPLE TEAM territory from the BlackHack Cybersecurity Map research

© 2026 BlackHack Society – Home for Ethical Hackers. All rights reserved. • blackhacksociety.com • blackhackacademy.com • getblackhack.com
BlackHack Cybersecurity Map, by BlackHack Society. Share it unaltered and with credit. No resale or derivative works without written permission.

PURPLE TEAM · P-EMUL

Adversary Emulation

Act like a specific, real adversary — on purpose, with intel behind it.

MENTAL MODEL

Act like a specific, real adversary — on purpose, with intel behind it. You think in faithful reproduction: not open-ended red teaming, but 'behave like this named actor' so the defense is tested against what it will actually face. The disciplined front end of the purple loop.

METHODOLOGY

Pick an actor relevant to the org (CTI-driven) → build an emulation plan from its known TTPs → execute in a controlled, collaborative exercise → map each action to ATT&CK → hand results to detection.

INTERLOCKS

validated-with ↔ Detection Eng (the loop) · fed-by ← CTI · base tier of purple

FRAMEWORKS & STANDARDS

Threat-informed defense · MITRE ATT&CK (the shared technique language) · adversary-emulation plans (CTID library) · the emulation-vs-red-team-vs-simulation distinction · intel-driven scoping

KEY REFERENCES

MITRE Center for Threat-Informed Defense ctid.mitre.org ↗

MITRE Caldera — automated emulation caldera.mitre.org ↗

Atomic Red Team — technique tests atomicredteam.io ↗

Adversary Emulation Library (CTID) github.com/center-for-threat-informed-defense/adversary_emulation_library ↗

CERTIFICATIONS

SANS SEC565/SEC699 · GRTP

ROLES & JOBS

Adversary Emulation Engineer · Purple Team Operator

EXAMPLE TOOLS

e.g. [Caldera](#) · [Atomic Red Team](#) · [Prelude](#)

PURPLE TEAM · P-BAS

Detection Validation

Prove the detection actually fires — continuously.

MENTAL MODEL

Prove the detection actually fires — continuously. You think in end-to-end pipeline verification: did the log capture it, forward it, fire the analytic, reach the queue? A silent break anywhere is a false sense of safety. Turns 'we have a rule' into 'we have a detection'.

METHODOLOGY

Select a technique → execute a controlled test → trace the detection pipeline (capture → forward → analytic → alert) → record detected/partial/missed + latency → ticket the gaps → re-test after fixes → track coverage over time.

INTERLOCKS

validates → Detection Eng, Vuln Mgmt (CTEM) · feeds → Human-Layer Translation (what it means) · base tier

FRAMEWORKS & STANDARDS

Breach-and-attack-simulation model · attack-to-detection validation loop · ATT&CK Navigator coverage scoring · continuous-validation (not periodic) · the CTEM validation stage

KEY REFERENCES

MITRE ATT&CK Navigator mitre-attack.github.io/attack-navigator ↗

VECTR — purple-team tracking vectr.io ↗

Atomic Red Team atomicredteam.io ↗

CERTIFICATIONS

SANS SEC699

ROLES & JOBS

Purple Team Engineer · Detection Validation Engineer

EXAMPLE TOOLS

e.g. VECTR · breach-and-attack-simulation platforms

PURPLE TEAM · P-TID

Threat-Informed Defense

Prioritize defense against what adversaries actually do.

MENTAL MODEL

Prioritize defense against what adversaries actually do. You think in evidence over fear: use real TTP knowledge to decide what to detect and harden first. The doctrine that ties red knowledge and blue action into one language.

METHODOLOGY

Know the adversary (ATT&CK) → map current defenses (D3FEND/coverage) → find the gaps against relevant TTPs → prioritize by real threat → drive emulation & detection to close them → re-measure.

INTERLOCKS

frames → the whole purple loop · bridges ↔ red knowledge ⇄ blue action · base tier

FRAMEWORKS & STANDARDS

Threat-informed defense (CTID) · MITRE ATT&CK + D3FEND (offense ⇄ defense mapping) · the common-language model · coverage-gap prioritization

KEY REFERENCES

MITRE ATT&CK attack.mitre.org ↗

MITRE D3FEND d3fend.mitre.org ↗

MITRE Center for Threat-Informed Defense ctid.mitre.org ↗

CERTIFICATIONS

(threat-informed-defense specialist)

ROLES & JOBS

Threat-Informed Defense Engineer

EXAMPLE TOOLS

e.g. ATT&CK / D3FEND mapping tooling

PURPLE TEAM · P-ENG

I Deception / Engage

Turn the defender's environment into a trap and a sensor.

MENTAL MODEL

Turn the defender's environment into a trap and a sensor. You think in adversary engagement: plant things attackers touch, learn from their behavior, raise their cost. The active, learn-from-the-adversary edge of the base tier.

METHODOLOGY

Decide the deception goal (detect / delay / learn) → plant honeytokens/canaries/decoys where only an attacker would touch them → alert on interaction → study the behavior → feed it back to detection & intel.

INTERLOCKS

feeds → Adversary Emulation (realism) · feeds → CTI (behavior) · base tier

FRAMEWORKS & STANDARDS

Adversary engagement (MITRE Engage) · deception model (denial · deception · learning) · honeypot/canary methodology · the cost-imposition model

KEY REFERENCES

MITRE Engage — adversary engagement [engage.mitre.org ↗](https://engage.mitre.org)

MITRE D3FEND [d3fend.mitre.org ↗](https://d3fend.mitre.org)

Canary Tokens — free deception [canarytokens.org ↗](https://canarytokens.org)

CERTIFICATIONS

INFERENCE: no established cert

ROLES & JOBS

Deception Engineer · Purple Team Engineer

EXAMPLE TOOLS

e.g. honeypot/canary systems · deception platforms

PURPLE TEAM · P-TRANS

Human-Layer Risk Translation

THE SIGNATURE.

MENTAL MODEL

THE SIGNATURE. Carry a technical event all the way to the human who must act on it. You think in audiences and lanes: the same truth is a different true story to a technician, a risk owner, an executive, and the person whose trust is on the line. This is where BHS purple goes beyond the public field — which stops at detection coverage.

METHODOLOGY

Start from the technical event → trace its blast radius (1st→2nd→3rd order) → re-voice it for each lane up to the human → center the victim/stakeholder experience → manage expectations honestly → convert understanding into a funded decision.

INTERLOCKS

fed-by ← CTI (4 intel types), GRC (risk/exec), IR (incident) · bridge → THE HUMAN

FRAMEWORKS & STANDARDS

BHS cross-lane translation ladder (technical → cybersecurity → risk → operational → finance → executive → human) · order-effects / blast-radius model (1st → 2nd → 3rd order) · the victim-experience lens · expectation-management as a practitioner skill

KEY REFERENCES

FAIR Institute — risk communication fairinstitute.org ↗

NIST CSF — Govern function nist.gov/cyberframework ↗

BHS Practitioner's Lexicon — internal (BlackHack) blackhacksociety.com ↗

CERTIFICATIONS

Board-level cyber-risk communication · CISM

ROLES & JOBS

CISO · vCISO · Security Risk Communicator

EXAMPLE TOOLS

(a communication & reasoning discipline — the BHS cross-lane ladder, not tooling)

PURPLE TEAM · P-HUMAN

The Human

The far end of the bridge, and the point of all of it.

MENTAL MODEL

The far end of the bridge, and the point of all of it. The victim, the executive, the engineer up all night, the customer whose trust is on the line. Public purple ends at detection coverage, over the canyon; BHS builds the span that reaches this node. Everything in the atlas ultimately points here.

METHODOLOGY

(not a method to execute — the destination the whole system serves: the person security exists to protect)

INTERLOCKS

reached-by → only the BHS human-layer bridge · the node no public framework maps

FRAMEWORKS & STANDARDS

Human-centered security · stakeholder/victim perspective · trust as the real asset · the 'protect the people while you fix the system' stance

KEY REFERENCES

Human-centered security — the destination of the whole atlas blackhacksociety.com ↗

CERTIFICATIONS

ROLES & JOBS

EXAMPLE TOOLS

► THE DURABLE SPINE

Framework Index

The established frameworks and standards this map is built on. Tools change; these endure — the reason the map stays evergreen.

Cross-field	MITRE ATT&CK (Enterprise · ICS) · D3FEND · ATLAS · Engage · Cyber Kill Chain · Diamond Model · Pyramid of Pain
Governance / risk	NIST CSF 2.0 · ISO/IEC 27001 · SOC 2 · FAIR · NIST SP 800-30 · COSO ERM
Offense	PTES · OWASP (Top 10 · WSTG · API · MASVS · LLM · ML) · vulnerability-research lifecycle · SPARTA · RF kill chain
Defense ops	NIST SP 800-61 (PICERL) · SP 800-86 · PEAK · intelligence lifecycle · STIX/TAXII · CTEM · CVSS/EPSS/KEV/VEX
Engineering	NIST SP 800-207 · CIS Benchmarks · DISA STIG · NIST SSDF · SLSA · OWASP ASVS/SAMM · Purdue · ISA/IEC 62443 · ISO/SAE 21434 · NIST AI RMF
Integration	threat-informed defense (MITRE CTID) · adversary-emulation plans · breach-&-attack-simulation · cross-lane translation · order-effects / blast-radius

► INDEX // EVERY DISCIPLINE, A TO Z

Discipline Index

All 37 disciplines alphabetically. The colour marks the team; every entry links to its page.

● Adversary Emulation	67	● AI Engineering	62	● Application & Software	29
● Application Security	61	● Capability Creation	27	● Cloud Security / CNAPP	56
● Coding & Scripting	52	● Comms-Sec Engineering	55	● Container & K8s Security	57
● Criminal Economy	36	● Crypto & Web3	35	● Cyber-Physical & Hardware	34
● Deception / Engage	70	● Detection Engineering	44	● Detection Validation	68
● DevSecOps / Secure SDLC	58	● Enterprise & AD Intrusion	28	● GRC & Governance	40
● Human Layer	30	● Human-Layer Risk Translation	71	● IaC & Policy-as-Code	54
● Incident Response / DFIR	46	● Malware Analysis	48	● OS Hardening & Internals	53
● Physical Pentest	32	● Platform Eng / SRE	60	● Resilience / BC-DR	47
● Security Architecture	63	● SOC & SecOps	43	● Supply-Chain Security	59
● Synthetic Media	31	● The Human	72	● Threat Hunting	45
● Threat Intelligence	42	● Threat-Informed Defense	69	● Vulnerability & Exposure Mgmt	41
● Wireless & RF	33				

▶ ABOUT

BlackHack Society

Home for Ethical Hackers. We raise a new generation of Ethical Hackers from diverse backgrounds — bringing new talent into the profession and teaching a hybrid Offensive / Defensive discipline: the **Purple Team Mentality**.

THE SOCIETY

Events, meetups, community, and a national network — the hub at every level.

THE ACADEMY

Structured, hands-on, cohort-based training for real-world readiness.

THE COMMUNITY

Discord, local chapters, CTFs, and hackathons.

THE SIX PILLARS

Honesty · Integrity · Authenticity · Humility · Accountability · Gratitude

Sourcing. Every discipline, framework, and interlock is grounded in the map research. Design choices — the four native geometries, the groupings — are BlackHack's synthesis. Reference links are durable canonical anchors. Built to stay true for a year or two without revision.

[blackhacksociety.com](#) · [blackhackacademy.com](#) · [getblackhack.com](#)

► YOU HAVE SEEN THE MAP

Now Go Build It.

Nobody hands you trust - or a career. You build it, one proof of work at a time. Pick a path, start the climb, and do the reps where it is free and safe to fail.

THE COMMUNITY

Events, meetups, Discord, local chapters, CTFs - the network at every level.

[blackhacksociety.com](#) ↗

THE EDUCATION

Structured, hands-on, cohort-based training for real-world readiness.

[blackhackacademy.com](#) ↗

THE GEAR

Kit and resources for the work.

[getblackhack.com](#) ↗

CONNECT // ALL THE DOORS

[blackhacksociety.com](#) ↗

[blackhackacademy.com](#) ↗

[getblackhack.com](#) ↗

[LinkedIn](#) ↗

[YouTube](#) ↗

[Instagram](#) ↗

[Discord](#) ↗

[Aaron Butler](#) ↗

[founder@getblackhack.com](#) ↗

“Home for Ethical Hackers.”

[blackhacksociety.com](#) · [blackhackacademy.com](#) · [getblackhack.com](#)