GSDC
Global Skill Development Council

GENERATIVE AI CYBERSECURITY

CHEAT SHEET

www.gsdcouncil.org

1.1 Core Gen AI Concepts Every Security Professional Must Know

Generative AI

AI that creates new content — text, code, images, audio — by learning patterns from large datasets. In cybersecurity, it works both ways: defenders use it to build smarter protection, and attackers use it to build smarter threats. Understanding both sides is the foundation of this certification.

Large Language Models (LLMs)

AI models trained on massive text datasets that can understand, generate, and reason with human language. In security contexts, LLMs power threat report generation, vulnerability explanation, incident summarization, and security policy drafting.

Transformers

The architecture behind most modern Gen AI models. Transformers use an attention mechanism that allows them to understand context across long sequences of text or code — making them powerful for analyzing malware code, log files, and network traffic patterns simultaneously.

GANs (Generative Adversarial Networks)

A model architecture where two networks compete: a Generator creates synthetic content, and a Discriminator tries to detect it. In cybersecurity this is critical to understand because attackers use GANs to generate synthetic malware, deepfakes, and evasion techniques that bypass traditional detection systems.

Core Gen AI Concepts (Continued)

RAG (Retrieval-Augmented Generation)

AI that retrieves information from specific knowledge bases before generating a response. In security, RAG powers internal threat intelligence assistants that query your organization's own CVE database, incident history, and security policies before answering analyst questions.

AI Agents

Autonomous AI systems that plan and execute multi-step tasks. In cybersecurity, AI agents are being deployed for continuous vulnerability scanning, automated incident response, and real-time threat hunting — operating faster than any human SOC team.

Prompt Injection

A cyberattack specific to AI systems where malicious input manipulates an LLM into ignoring its instructions or revealing sensitive data. Security professionals must understand this as both an attack vector to defend against and a technique attackers use against AI-powered systems.

Hallucination in Security Context

When AI generates confident but incorrect threat assessments, CVE descriptions, or incident reports. In cybersecurity, hallucinations are not just inconvenient — they can lead to missed threats or false incident responses. **Always verify AI security outputs against authoritative sources.**

1.2 Traditional AI vs. Generative AI in Cybersecurity

Capability	Traditional AI/ML	Generative AI
Threat Detection	Flags known patterns	Detects novel, unseen attack patterns
Malware Analysis	Signature matching	Behavioral code analysis and explanation
Incident Reports	Structured data output	Full narrative incident reports
Threat Intelligence	Classifies known threats	Synthesizes intelligence from unstructured sources
Attacker Simulation	Rule-based red teaming	AI-driven adaptive attack simulation
Analyst Support	Dashboard alerts	Conversational security assistant

1.3 Key Gen AI Models Relevant to Cybersecurity

GPT-based Models (OpenAI, Azure OpenAI)

Used for threat report generation, security policy drafting, phishing email detection, and analyst Q&A. Microsoft Security Copilot is built on GPT-4.

Code LLMs (GitHub Copilot, CodeLlama)

Analyze and explain malicious code, generate secure code suggestions, identify vulnerabilities in source code during development.

GANs in Security

Used by both defenders (generating synthetic training data for anomaly detection models) and attackers (generating polymorphic malware and synthetic phishing content).

BERT and Encoder Models

Used for log analysis, anomaly detection in network traffic, and classifying security events from large volumes of unstructured log data.

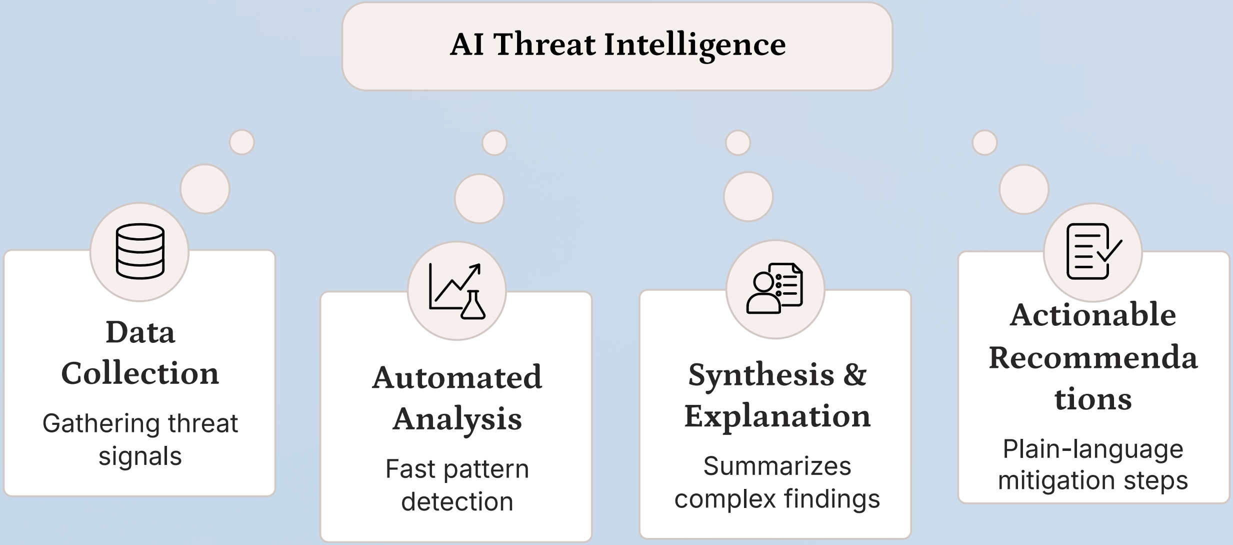
Multimodal Models

Process text, images, and audio simultaneously. Relevant for deepfake detection, visual phishing analysis, and analyzing screenshots of malicious activity.

DOMAIN 2: AI-POWERED THREAT INTELLIGENCE

2.1 What Is AI Threat Intelligence

Threat intelligence is the process of collecting, analyzing, and acting on information about current and emerging cyber threats. Generative AI transforms this from a slow, analyst-heavy process into a near-real-time intelligence operation. AI doesn't just collect threat data — it synthesizes it, explains it, and recommends actions in plain language.



AI Threat Intelligence

Data Collection
Gathering threat signals

Automated Analysis
Fast pattern detection

Synthesis & Explanation
Summarizes complex findings

Actionable Recommendations
Plain-language mitigation steps

2.2 Gen AI Applications in Threat Intelligence

→ Automated Threat Report Generation

AI reads raw threat feeds, CVE databases, dark web data, and OSINT sources and generates structured, readable threat intelligence reports automatically. Analysts receive synthesized intelligence rather than raw data to wade through.

→ Indicator of Compromise (IoC) Extraction

AI scans unstructured sources — security blogs, forums, paste sites, malware reports — and automatically extracts and categorizes IoCs: IP addresses, domains, hashes, URLs, and email addresses associated with threat actors.

→ Threat Actor Profiling

AI builds and maintains profiles of threat actors by aggregating information from public disclosures, incident reports, and dark web monitoring. It identifies TTPs (Tactics, Techniques, and Procedures) aligned to the MITRE ATT&CK framework automatically.

→ MITRE ATT&CK Mapping

AI maps observed attack behaviors to MITRE ATT&CK framework techniques automatically, giving security teams a standardized way to understand and communicate threats without manual framework analysis.

→ Predictive Threat Intelligence

AI analyzes historical attack patterns and current threat actor behavior to predict which attack vectors are most likely to be used against your organization in the near term — shifting security posture from reactive to proactive.

→ Dark Web Monitoring

AI agents continuously monitor dark web forums, marketplaces, and communication channels for mentions of your organization, leaked credentials, or sale of access to your systems — providing early warning before an attack materializes.

2.3 Key Threat Intelligence Frameworks to Know

1

MITRE ATT&CK

Knowledge base of adversary tactics and techniques based on real-world observations. Gen AI tools map incidents to this framework automatically. Know the 14 tactic categories: Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, Impact.

2

STIX/TAXII

Structured Threat Information eXpression and Trusted Automated eXchange of Intelligence Information. The standardized format and protocol for sharing threat intelligence that AI systems read, generate, and exchange.

3

Cyber Kill Chain (Lockheed Martin)

7-stage attack model: Reconnaissance → Weaponization → Delivery → Exploitation → Installation → Command & Control → Actions on Objectives. Gen AI maps detected behaviors to kill chain stages to identify where in an attack the defender currently is.

4

Diamond Model

Analyzes intrusions across four features: Adversary, Infrastructure, Capability, and Victim. AI uses this model to cluster related incidents and attribute attacks to specific threat actor groups.

DOMAIN 3: ANOMALY DETECTION & THREAT HUNTING

3.1 How Gen AI Powers Anomaly Detection

Traditional anomaly detection relied on predefined rules and signatures — effective against known threats, blind to novel ones. Generative AI shifts anomaly detection to behavioral pattern learning — understanding what "normal" looks like across users, systems, and networks, and flagging deviations with contextual explanation.

1

User and Entity Behavior Analytics (UEBA)

AI builds behavioral baselines for every user and entity in the environment. Deviations — logging in at unusual times, accessing unusual resources, large data transfers — trigger risk scores with AI-generated explanations of why the behavior is anomalous.

2

Network Traffic Anomaly Detection

AI analyzes network flow data at scale, detecting unusual communication patterns, unexpected protocol usage, and suspicious connection patterns that signature-based systems miss entirely.

3

Log Analysis at Scale

Security environments generate millions of log entries daily. AI processes and correlates logs from SIEM, firewalls, endpoints, and cloud environments simultaneously, surfacing the small number of genuinely suspicious events from the noise.

4

AI-Powered SIEM Enhancement

Gen AI sits on top of existing SIEM platforms (Splunk, Microsoft Sentinel, IBM QRadar) and provides natural language querying, automatic alert triage, and AI-generated incident summaries — transforming the analyst experience from dashboard management to conversational investigation.

3.2 AI-Driven Threat Hunting

What is Threat Hunting?

Proactive search for threats that have evaded automated detection. Rather than waiting for alerts, threat hunters actively look for signs of compromise. Gen AI dramatically accelerates this process.

1

Hypothesis Generation

AI analyzes current threat intelligence and your environment's specific exposure to generate hunt hypotheses: "Based on recent APT activity targeting your industry, hunt for these specific behaviors in your environment."

2

Natural Language Queries

Analysts ask questions in plain English — "Show me all instances of PowerShell executing encoded commands in the last 7 days" — and AI translates them into the correct SIEM query language, removing the technical barrier for non-expert hunters.

3

Automated Hunt Execution

AI agents execute predefined hunt playbooks continuously, running threat-hunting queries around the clock without requiring an analyst to initiate each one manually.

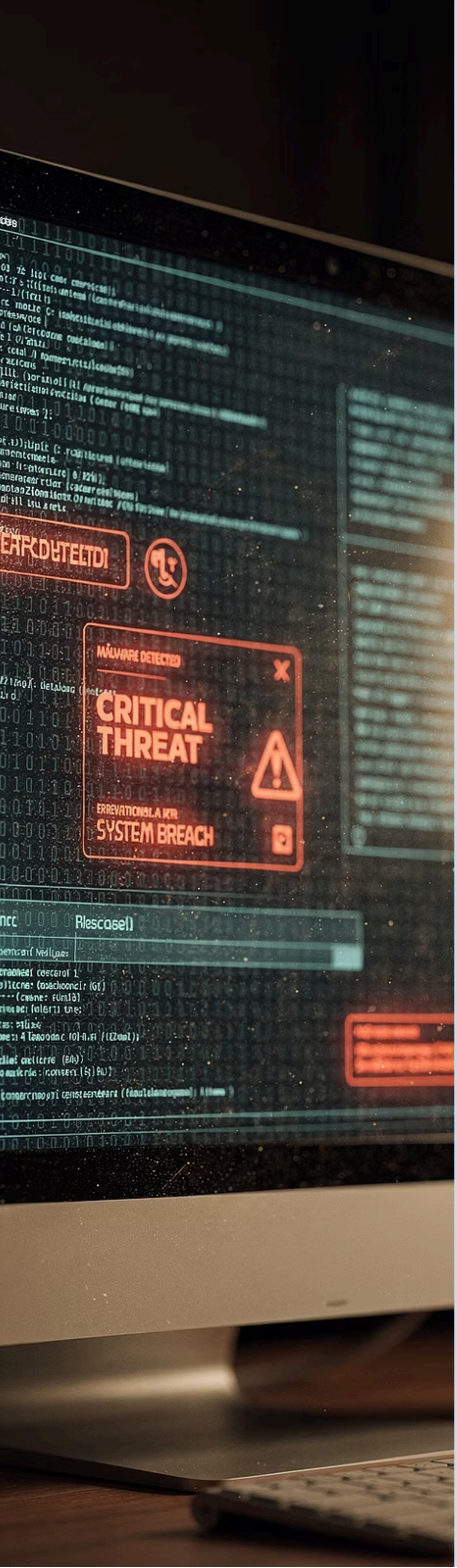
4

Pattern Recognition Across Campaigns

AI identifies connections between seemingly unrelated security events across long time periods — connecting an unusual login 3 months ago with a current data exfiltration attempt that a human analyst would never link manually.

3.3 Key Anomaly Detection Terms

Term	Definition
Baseline	Normal behavioral pattern against which anomalies are measured
False Positive	Alert triggered by legitimate activity — AI reduces these significantly
False Negative	Real threat that goes undetected — AI reduces these through behavioral analysis
Dwell Time	Time between initial compromise and detection — AI shortens this
UEBA	User and Entity Behavior Analytics — AI-powered behavioral profiling
TTP	Tactics, Techniques, and Procedures — attacker behavioral patterns
IOC	Indicator of Compromise — evidence of an attack (hashes, IPs, domains)
IOA	Indicator of Attack — behavioral signals suggesting an attack in progress



DOMAIN 4: MALWARE ANALYSIS WITH GEN AI

4.1 How Gen AI Transforms Malware Analysis

Traditional malware analysis requires highly skilled reverse engineers spending hours or days understanding a single malware sample. Gen AI compresses this timeline dramatically — providing code explanation, behavior prediction, and threat classification at a speed no human analyst can match.

4.2 Gen AI Malware Analysis Techniques

Static Code Analysis

AI reads malware source code or decompiled binary and generates a plain-English explanation of what the code does, what system functions it calls, what data it targets, and what its likely purpose is — in minutes rather than hours.

Dynamic Behavior Analysis

AI monitors malware execution in a sandboxed environment and generates a behavioral report covering: processes spawned, registry keys modified, network connections made, files created or deleted, and persistence mechanisms established.

Malware Family Classification

AI compares new malware samples against known malware families using code similarity analysis, behavioral signatures, and structural patterns — classifying threats faster than traditional signature-based AV engines.

Obfuscation Detection and Deobfuscation

Attackers deliberately obfuscate malware code to evade analysis. Gen AI detects common obfuscation techniques — base64 encoding, XOR encryption, string concatenation — and automatically deobfuscates code for analysis.

Variant Generation Understanding

Because Gen AI understands how attackers use AI to generate malware variants, security teams can use the same models to predict likely variants of known malware and update detection rules proactively.

Automated YARA Rule Generation

YARA rules are patterns used by security tools to detect malware. AI analyzes malware samples and generates YARA detection rules automatically — a task that previously required significant manual effort from experienced malware analysts.

4.3 AI-Generated Malware Threats to Know

1

Polymorphic Malware

Malware that changes its code signature with each infection while maintaining its malicious functionality. Gen AI makes creating polymorphic variants trivial for attackers, challenging signature-based defenses.

2

AI-Written Phishing Code

Gen AI creates convincing phishing kits — HTML pages, JavaScript credential harvesters, email templates — that are unique enough to evade template-matching detection systems.

3

LLM-Assisted Exploit Development

Attackers use code LLMs to accelerate the development of working exploits for newly disclosed vulnerabilities — shrinking the window between CVE publication and weaponized exploit availability.

4

Adversarial Machine Learning

Attacks specifically designed to fool AI security systems — crafting inputs that cause AI models to misclassify malicious traffic as benign, or bypass AI-based content moderation.

DOMAIN 5: VULNERABILITY ASSESSMENT & PENETRATION TESTING

5.1 Gen AI in Vulnerability Management

1

AI-Powered Vulnerability Scanning

AI-enhanced scanners go beyond identifying known CVEs to reasoning about how multiple vulnerabilities in combination could create exploitable attack chains — contextual risk assessment rather than raw vulnerability counting.

2

Vulnerability Prioritization

Organizations typically have thousands of open vulnerabilities at any time. AI prioritizes remediation by scoring vulnerabilities against: CVSS score, exploitability in the wild, asset criticality, exposure, and attacker interest — giving security teams a risk-ranked remediation queue.

3

CVE Analysis and Explanation

AI reads raw CVE descriptions and translates them into plain-English explanations of what the vulnerability means, how it could be exploited, what systems are affected, and what the remediation steps are — making vulnerability intelligence accessible to non-specialist team members.

4

Attack Surface Management

AI continuously maps your organization's external attack surface — domains, IPs, cloud assets, APIs, and exposed services — and flags new exposures as they appear, often before attackers discover them.

5.2 Gen AI in Penetration Testing and Red Teaming

→

AI-Assisted Penetration Testing

Gen AI assists penetration testers by suggesting attack paths based on reconnaissance data, generating custom payloads for specific targets, explaining vulnerability exploitation techniques, and drafting comprehensive penetration test reports automatically.

→

Automated Attack Simulation

AI agents simulate multi-stage attack campaigns against your environment — mimicking the tactics of known threat actor groups to test whether your defenses would detect and stop a real attack from that adversary.

→

AI Red Team vs. AI Blue Team

Emerging practice where AI systems are used on both sides simultaneously: a red team AI attacks the environment while a blue team AI defends and responds. This continuous automated adversarial testing identifies gaps faster than periodic manual penetration tests.

→

Social Engineering Simulation

AI generates highly personalized, contextually relevant phishing emails and pretexting scripts for security awareness training and phishing simulation — using information about targets that is publicly available to make simulations realistic.

Key Penetration Testing Phases and AI Role

Phase	Traditional Approach	Gen AI Enhancement
Reconnaissance	Manual OSINT research	Automated intelligence aggregation
Scanning	Tool-based scanning	AI-contextual attack surface mapping
Exploitation	Manual exploit selection	AI-suggested exploit chains
Post-Exploitation	Manual lateral movement	AI-guided privilege escalation paths
Reporting	Manual report writing	AI-generated comprehensive reports

DOMAIN 6: AI-POWERED SECURITY OPERATIONS (SecOps)

6.1 Gen AI in the Security Operations Center (SOC)

1

AI Security Analyst Assistant

Gen AI tools like Microsoft Security Copilot act as always-available AI analysts that answer natural language questions about incidents, run investigation queries, and explain threat context — augmenting every analyst's capability to senior analyst level.

2

Automated Alert Triage

AI classifies incoming alerts by severity, groups related alerts into incidents, filters false positives, and assigns priority — dramatically reducing the alert fatigue that causes analysts to miss genuine threats buried in noise.

3

Incident Investigation Acceleration

AI builds a complete timeline of an incident automatically — correlating events across endpoints, network, identity, and cloud telemetry — a process that takes human analysts hours, AI completes in seconds.

4

Automated Incident Response Playbooks

AI executes predefined response actions automatically when specific conditions are met: isolating a compromised endpoint, blocking a malicious IP, disabling a compromised account — reducing time-to-containment from hours to minutes.

5

Shift-Left Security

AI integrates security earlier in the development lifecycle — analyzing code for vulnerabilities during development rather than after deployment. This "shift-left" approach is dramatically cheaper than finding and remediating production vulnerabilities.

6.2 Key SecOps Metrics AI Improves

Metric	Definition	AI Impact
MTTD	Mean Time to Detect — average time to detect a breach	Reduced significantly through continuous AI monitoring
MTTR	Mean Time to Respond — average time to contain and remediate	Reduced through automated response playbooks
Dwell Time	Time attacker operates undetected	Shortened through behavioral anomaly detection
Alert Fatigue	Analyst overload from excessive alerts	Reduced through AI triage and false positive filtering
Alert-to-Incident Ratio	Proportion of alerts that are real incidents	Improved through AI correlation and context

6.3 Gen AI Security Tools to Know

Tool	Vendor	Key Capability
Security Copilot	Microsoft	AI security analyst assistant across Microsoft stack
Google Threat Intelligence	Google / Mandiant	AI-powered threat intelligence and investigation
CrowdStrike Charlotte AI	CrowdStrike	Natural language SOC queries and investigation
Darktrace	Darktrace	AI anomaly detection and autonomous response
SentinelOne Purple AI	SentinelOne	Threat hunting with natural language queries
IBM QRadar AI	IBM	AI-enhanced SIEM correlation and triage
Vectra AI	Vectra	Network detection and response with AI
Recorded Future AI	Recorded Future	AI-powered threat intelligence platform

DOMAIN 7: AI ATTACK VECTORS — THE THREAT SIDE

7.1 How Attackers Use Gen AI — What Defenders Must Know

> Understanding how attackers weaponize Gen AI is as important as knowing how defenders use it. The same capabilities that make Gen AI powerful for defense make it equally powerful — and accessible — for offense.

7.2 Gen AI-Powered Attack Techniques

AI-Generated Phishing

Gen AI creates highly personalized, grammatically perfect phishing emails tailored to specific targets using publicly available information. The "poorly written email" heuristic that caught traditional phishing no longer applies. AI phishing is contextually relevant, timely, and indistinguishable from legitimate communication.

Spear Phishing at Scale

Previously, targeted spear phishing required manual research per victim — limiting attackers to high-value targets. Gen AI automates the personalization process, enabling attackers to run spear phishing campaigns against thousands of individuals simultaneously with the same quality as manual targeting.

Deepfakes for Social Engineering

AI-generated audio and video that realistically impersonate executives, vendors, or colleagues. Used in vishing attacks where attackers call employees impersonating the CEO, and in business email compromise (BEC) attacks with video verification.

AI-Powered Malware Development

Attackers use code LLMs to write, test, and refine malware faster than ever. They also use AI to create polymorphic variants that evade signature detection and to adapt existing malware for new targets and environments.

Automated Vulnerability Exploitation

AI reduces the time between CVE publication and working exploit — attackers use LLMs to understand vulnerabilities and generate proof-of-concept exploits faster than defenders can patch.

Adversarial Attacks on AI Systems

Attacks specifically targeting AI security systems: crafting inputs that cause AI models to misclassify malicious traffic, injecting adversarial examples into training data to degrade model performance, or using prompt injection to manipulate AI security tools.

Credential Stuffing Enhancement

AI generates realistic password variations based on known information about targets — significantly improving the success rate of credential stuffing attacks beyond simple dictionary attacks.

7.3 AI Attack vs. AI Defense — The Arms Race

AI Attack Capability	AI Defense Response
AI-generated phishing	AI phishing detection and email analysis
Polymorphic malware	Behavioral AI detection vs. signature matching
Deepfake impersonation	Deepfake detection models
Automated exploitation	AI-powered patch prioritization and virtual patching
AI-enhanced reconnaissance	AI attack surface reduction and exposure monitoring
Adversarial ML attacks	Adversarial training and model robustness testing

8.1 Ethical Considerations in AI-Powered Security

1

Bias in Security AI Models

AI security models trained on historical data inherit the biases in that data. If historical incident data over-represents certain user groups as threats, AI will flag those groups disproportionately — creating fairness and legal risk, particularly in access management and insider threat detection.

2

Explainability (XAI) in Security Decisions

When AI flags a user as a threat and triggers account suspension or access restriction, that decision must be explainable. Black-box AI decisions in security contexts create legal, HR, and operational risk. Security AI must be able to explain why it made a decision in terms that humans and regulators can evaluate.

3

Privacy in Security Monitoring

AI security monitoring involves analyzing employee behavior, communications, and activities at a granular level. This creates genuine privacy tensions — particularly in jurisdictions with strong privacy rights (GDPR, CCPA). Organizations must balance security monitoring with employee privacy obligations.

4

Dual-Use Risk

The same Gen AI capabilities that power defensive security tools can be used offensively. Security professionals have a responsibility to consider how AI capabilities they develop or deploy could be misused — and to build appropriate access controls and usage monitoring.

5

Human Oversight Requirements

High-impact security decisions — account suspension, network isolation, incident escalation — should not be fully automated without human review capability. AI can recommend and prepare, but consequential security actions require human accountability.

8.2 Regulatory and Compliance Frameworks for AI in Cybersecurity

1

NIST AI Risk Management Framework (AI RMF)

The US standard for managing AI risk across four functions: Govern, Map, Measure, and Manage. Security professionals should apply this framework to every AI security tool they deploy.

2

EU AI Act

Classifies AI systems by risk. AI used in critical infrastructure security is classified as high-risk, requiring conformity assessment, documentation, human oversight, and transparency. Cybersecurity professionals in EU-regulated organizations must understand compliance requirements.

3

GDPR and Security Monitoring

When AI security monitoring processes personal data of EU residents, GDPR requirements apply — including data minimization, purpose limitation, and data subject rights. Legitimate interest is the most common legal basis for security monitoring, but it has limits.

4

NIST Cybersecurity Framework (CSF)

Five functions: Identify, Protect, Detect, Respond, Recover. Know where Gen AI applies to each function — it touches all five but is most transformative in Detect and Respond.

5

ISO/IEC 27001 and AI

The international information security management standard is being updated to address AI-specific security risks. Understand how AI security tools fit within ISMS (Information Security Management System) governance requirements.

8.3 Responsible AI Integration in Security Operations

→ **Validate AI outputs**

Never act on AI-generated threat assessments without verification against raw data.

→ **Maintain human-in-the-loop**

For all consequential security decisions: account actions, incident escalations, external notifications.

→ **Audit AI security models**

Regularly test for bias, drift, and performance degradation in production security AI systems.

→ **Document AI use**

Maintain records of where AI is used in security operations for regulatory and incident response purposes.

→ **Vendor due diligence**

Evaluate the security and ethics practices of AI security tool vendors before deployment.

→ **Red team your AI**

Specifically test whether your AI security tools can be fooled, bypassed, or manipulated by adversarial inputs.

DOMAIN 9: SECURITY AUTOMATION & AI ORCHESTRATION

9.1 SOAR Enhanced with Gen AI

SOAR (Security Orchestration, Automation, and Response) — Platforms that orchestrate security tools and automate response workflows. Gen AI makes SOAR dramatically more capable by adding natural language interaction, intelligent decision-making, and adaptive playbooks.

Intelligent Playbook Execution

Traditional SOAR playbooks follow fixed decision trees. AI-enhanced playbooks adapt dynamically based on the specific context of each incident — choosing different response paths based on asset criticality, threat actor profile, and attack stage.

Natural Language Playbook Creation

Security engineers describe a response workflow in plain English and AI generates the technical playbook — dramatically reducing the time and expertise required to build automation.

Cross-Tool Orchestration

AI agents orchestrate actions across multiple security tools simultaneously — querying the SIEM, isolating the endpoint in EDR, blocking the IP in the firewall, and creating the incident ticket in ServiceNow — in a coordinated automated response.

9.2 AI in Cloud Security

Cloud Misconfiguration Detection

AI continuously scans cloud configurations against security best practices and compliance requirements, flagging misconfigurations — the leading cause of cloud breaches — before they are exploited.

Cloud-Native AI Security Tools

AWS GuardDuty, Azure Defender, and Google Security Command Center all use ML and increasingly Gen AI to detect threats specific to cloud environments — unusual API calls, compromised credentials, crypto-mining activity, and data exfiltration.

AI for Identity and Access Management (IAM)

AI analyzes access patterns across cloud environments to detect over-permissioned accounts, unused permissions that expand the attack surface, and anomalous access that suggests credential compromise.

9.3 AI in Zero Trust Security Architecture

Zero Trust Principle

Never trust, always verify. Every access request is authenticated and authorized regardless of network location. Gen AI enhances Zero Trust by making the continuous verification process more intelligent and less disruptive.

Continuous Risk Scoring

AI calculates a real-time risk score for every access request based on: user identity, device health, location, behavior patterns, and resource sensitivity — enabling dynamic access decisions that tighten or relax controls based on current risk level.

AI-Enhanced MFA

Beyond static multi-factor authentication, AI determines when additional verification is required based on risk context — stepping up authentication only when behavior or context suggests elevated risk, reducing friction for routine access.

QUICK REFERENCE: Key Terms & Concepts

30 Terms to Know Cold

Term	One-Line Definition
LLM	AI model that understands and generates human language
GAN	Two-network AI architecture used for synthetic content generation
Transformer	Architecture powering most modern Gen AI models
RAG	AI that retrieves from specific knowledge bases before responding
Prompt Injection	Attack that manipulates AI systems through malicious input
Adversarial ML	Attacks designed to fool AI security models
UEBA	AI-powered user and entity behavioral analytics
IoC	Indicator of Compromise — evidence of a breach
IoA	Indicator of Attack — behavioral signal of active attack
TTP	Tactics, Techniques, Procedures — attacker behavior patterns
MITRE ATT&CK	Framework mapping adversary behavior to security controls
Kill Chain	7-stage model of a cyberattack from recon to impact
SOAR	Security Orchestration, Automation, and Response
SIEM	Security Information and Event Management

EDR	Endpoint Detection and Response
XDR	Extended Detection and Response — cross-domain correlation
MTTD	Mean Time to Detect a breach
MTTR	Mean Time to Respond and remediate
Dwell Time	Time attacker operates undetected in environment
Polymorphic Malware	Malware that changes signature with each infection
Deepfake	AI-generated synthetic media impersonating real people
CVE	Common Vulnerabilities and Exposures — standardized vuln IDs
CVSS	Common Vulnerability Scoring System — vuln severity score
Zero Trust	Security model requiring verification of every access request
XAI	Explainable AI — AI systems that explain their decisions
Hallucination	AI generating confident but factually incorrect output
YARA Rules	Pattern-matching rules used to detect malware
STIX/TAXII	Standard format/protocol for sharing threat intelligence
Red Team	Simulated attackers testing defensive capabilities
Blue Team	Defenders responsible for detecting and responding to attacks

GSDC
Global Skill Development Council

CERTIFICATION IN GENERATIVE AI IN CYBERSECURITY

GSDC
Global Skill Development Council
Generative AI in Cybersecurity
CERTIFIED

ABOUT GSDC CERTIFICATION

EBOOK

Extensive and exclusive Ebook created by world's experts to help you with understanding core concepts.

LEARNING MATERIALS

Get access to learning materials such as videos, ebooks, templates, and practice exams, which will help you clear the certification exam.

CREATED BY EXPERTS

GSDC certifications are created and authored by world's leading experts in the field.

LEARNING OBJECTIVE

- Gain insights into autonomous decision-making processes
- Apply knowledge using ready-to-implement templates
- Demonstrate ability to work with Agentic AI models
- Validate your skills wit

Enroll now with the code **LEARN20** To avail **20%** discount

Enroll Now

www.gsdcouncil.org