GSDC

Global Skill Development Council

Best AI Tools for Cybersecurity

CATEGORY 1

Microsoft Security Copilot

An AI security analyst assistant built on GPT-4, integrated across Microsoft Sentinel, Defender, Intune, and Entra ID. Security Copilot lets analysts investigate incidents and run queries through plain English conversation — fundamentally transforming how SOC teams interact with security data.

Applications

- **Incident Summarization**: Instant summaries generated from correlated alert data — no manual correlation required.
- **Natural Language SIEM**: Query Microsoft Sentinel in plain English — no KQL knowledge required from analysts.
- **Threat Intelligence Enrichment**: Automated enrichment during investigations and AI-powered malicious script deobfuscation.
- **Script Analysis**: AI deobfuscation of malicious scripts and automated threat actor attribution.

Key Benefits

- **10x Faster Investigation**: Cuts investigation time from hours to minutes through AI-assisted triage and correlation.
- **Democratizes Senior Analyst Capability**: Makes advanced investigation skills accessible to junior staff — dramatically accelerating SOC analyst onboarding.
- **No New Infrastructure**: Deploys within existing Microsoft licenses for Microsoft-stack organizations.
- **Executive-Ready Reporting**: AI-generated incident reports and executive summaries reduce documentation burden.

Google Threat Intelligence

Combines Google's global internet visibility, Chronicle SIEM, and Mandiant's elite threat research into one AI-powered platform. Teams gain access to one of the world's largest threat intelligence datasets — with petabyte-scale telemetry and Mandiant's frontline expertise encoded directly into detection models.

Applications

- **AI Intelligence Synthesis**: Cross-source synthesis across Google, Mandiant, and VirusTotal datasets in a single workflow.
- **Attack Surface Monitoring**: Continuous external attack surface monitoring with AI-powered malware analysis and plain-English explanations.
- **MITRE ATT&CK Attribution**: Automated threat actor attribution mapped directly to the MITRE ATT&CK framework for structured reporting.
- **Natural Language Telemetry**: Query petabyte-scale security telemetry in plain English — no specialized query language required.

Key Benefits

- **Unmatched Global Visibility**: Threat visibility derived from Google's global internet infrastructure — no commercial vendor has comparable data breadth or depth.
- **Elite Research at Scale**: Mandiant's elite threat research is encoded directly into AI detection models, bridging the gap between intelligence and automated defense.
- **Compressed Detection Timelines**: Compresses threat intelligence to detection rule deployment from days to hours — dramatically reducing adversary dwell advantage.
- **Enterprise-Scale Log Handling**: Handles log volumes that overwhelm traditional SIEMs, making it viable for the largest enterprise environments.

IBM QRadar SIEM with AI

One of the most widely deployed enterprise SIEMs globally, with Watson AI adding behavioral analytics, natural language querying, and automated investigation workflows on top of the traditional SIEM foundation. Directly addresses alert fatigue — the defining operational challenge of modern SOC environments.

Applications

- **AI Alert Correlation** reduces alert volume by 50–70% through intelligent correlation and noise suppression.
- **UEBA**Behavioral baselines with anomaly scoring to detect insider threats and compromised accounts.
- **Natural Language Querying** Watson interfaces allow plain English queries — no specialized query language required.
- **Automated Compliance Reporting** Automated compliance report generation for regulated industries.
- **AI-Assisted Threat Hunting** Guided threat hunting playbooks powered by Watson AI.

Key Benefits

- **Solves Alert Fatigue** Directly addresses the defining operational challenge of large SOC environments through intelligent correlation.
- **700+ Integrations**: Integrates with 700+ security products — fits into virtually any existing security stack.
- **Strong Compliance Reporting** Particularly valuable for regulated industries requiring detailed audit trails and compliance evidence.
- **Flexible Deployment** supports on-premise and cloud deployment for data sovereignty and hybrid environment needs.

CATEGORY 2

CrowdStrike Falcon with Charlotte AI

A cloud-native EDR platform using AI behavioral models for real-time endpoint threat detection without signatures. Charlotte AI adds a conversational interface for threat hunting and investigation across the entire Falcon platform — enabling junior analysts to perform senior-level threat hunts through natural language.

Applications

- **Behavioral Detection**AI-powered endpoint threat detection without signature updates — catches novel malware on first execution.
- **Charlotte AI Hunting**Natural language threat hunting queries across all endpoint data — no query language expertise required.
- **Attack Mapping**Automated attack timeline and lateral movement mapping with instant endpoint isolation capability.
- **Vulnerability Management**Unified agent covers EDR, threat intelligence, and vulnerability management in a single lightweight footprint.

Key Benefits

- **Cloud-Native Speed**: Threat intelligence updates are instant and globally distributed — no local update cycles or signature delays.
- **Analyst Uplift** Charlotte AI brings junior analysts to senior hunting capability — multiplying SOC effectiveness without headcount.
- **Unified Agent**: A single lightweight agent covers EDR, threat intelligence, and vulnerability management—minimizing endpoint footprint.
- **Adversary Intelligence** tracks 200+ named adversary groups — providing unmatched attacker context for every detection.

SentinelOne Singularity with Purple AI

An autonomous endpoint security platform where AI makes real-time detection and response decisions at machine speed. Purple AI adds natural language threat hunting and investigation capability, making it one of the most intuitive analyst experiences available in enterprise EDR.

Applications

- **Autonomous Threat Containment**Autonomous threat containment and remediation without analyst involvement — response at machine speed.
- **Natural Language Hunting**Natural language queries translated into PowerQuery across the data lake — no query expertise required.
- **Automated File Rollback**Automated file rollback after ransomware or destructive attacks — unique capability in the EDR market.
- **Full Attack Story Visualization**Complete attack story from first activity to impact across Windows, macOS, Linux, cloud, and IoT.

Key Benefits

- **Millisecond Response:** Autonomous response contains threats in milliseconds — not minutes — before damage spreads.
- **Ransomware Rollback** Automated rollback restores files without paying ransom — a unique and highly valuable capability.
- **Intuitive Hunting Interface** One of the most intuitive natural language hunting interfaces available in enterprise EDR.
- **MITRE ATT&CK Results** Consistently strong results in independent MITRE ATT&CK evaluations — validated detection coverage.

Darktrace

An AI cybersecurity platform using unsupervised machine learning to learn the behavioral pattern of every user, device, and system — detecting deviations without rules or signatures. Antigena provides autonomous real-time response, surgically slowing suspicious connections without full isolation.

Applications

- **Behavioral Baseline Learning** Continuously learns normal behavior for every user, device, and system — no rules or signatures required.
- **Zero-Day Threat Detection** Detects novel and zero-day attacks with no prior knowledge — genuinely complementary to rule-based tools.
- **OT & IoT Coverage** Covers OT and IoT environments most security tools cannot reach — critical for manufacturing and utilities.
- **Autonomous Response (Antigena)**Surgically slows suspicious connections without full isolation — preserving business continuity during response.

Key Benefits

- **Catches What Rules Miss**Detects novel attacks that rule-based and signature tools consistently miss — genuinely complementary coverage.
- **OT & IoT Reach Speed** Covers environments most security tools cannot reach — critical for industrial and operational technology organizations.
- **Pre-Human Response Speed** Autonomous response acts before humans can respond — containing threats at machine speed.
- **No Prior Knowledge Required** Unsupervised learning means no threat intelligence feeds or rule updates needed to detect new attack patterns.

CATEGORY 3

Recorded Future

The world's largest commercial threat intelligence company. AI continuously collects and analyzes intelligence from open web, dark web, and technical sources — delivering structured, actionable intelligence in real time. Recorded Future transforms raw threat data into finished analysis that security teams can act on immediately.

Applications

- **Real-Time Web Monitoring:** Continuous monitoring across millions of open and dark web sources — detecting emerging threats before they materialize.
- **Credential & Dark Web Detection:** Leaked credential identification and dark web access sale detection — enabling proactive response before account compromise.
- **Supply Chain Intelligence:** Third-party and supply chain risk intelligence monitoring — essential for organizations with complex vendor ecosystems.
- **CVE Enrichment:** CVE enrichment with real-world exploitation evidence and continuously updated threat actor TTP profiles.

Key Benefits

- **Broadest Data Collection:** Widest data collection of any commercial intelligence vendor — unmatched source breadth across surface, deep, and dark web.
- **Finished Analysis:** Intelligence delivered as finished analysis — not raw data dumps. Analysts receive context-rich, actionable output.
- **Seamless Integration:** Integrates directly into SIEM, SOAR, and ticketing workflows — intelligence flows to the tools analysts already use.
- **Supply Chain Focus:** Particularly valuable for organizations with complex supply chains facing third-party and vendor-originated risk.

Anomali ThreatStream

An AI-powered Threat Intelligence Platform (TIP) that aggregates, normalizes, and enriches intelligence from hundreds of sources — commercial feeds, ISAC sharing communities, open source, and internal — into one unified operation. AI relevance scoring surfaces only the intelligence specific to your environment.

Applications

- **Multi-Source Aggregation** Normalizes intelligence from commercial, ISAC, open source, and internal feeds into a single unified workflow.
- **AI Relevance Scoring** Filters global intelligence to what matters specifically for your environment — eliminating noise from irrelevant global data.
- **STIX/TAXII Sharing** Native STIX/TAXII support for industry peer sharing and regulatory intelligence sharing requirements in critical sectors.
- **SIEM & SOAR Integration** Pushes enriched, relevant indicators directly into SIEM and SOAR platforms for automated response.

Key Benefits

- **Noise Elimination** AI relevance scoring filters global threat data to only what matters for your specific environment — dramatically reducing analyst burden.
- **Unified Intelligence Operation** Consolidates hundreds of intelligence sources into one workflow — eliminating tool sprawl in threat intelligence operations.
- **Industry Sharing Ready** Native STIX/TAXII support enables peer sharing and meets regulatory intelligence sharing requirements in critical sectors.
- **Actionable Output** Intelligence flows directly into operational tools — not siloed in a separate platform analysts must manually check.

VirusTotal with AI (Google)

Google's multi-engine file, URL, domain, and IP analysis service — simultaneously scanning against 70+ security engines. Code Insight AI adds plain-language behavioral explanation to the multi-scanner approach, making malware analysis accessible to analysts without reverse engineering expertise.

Applications

- **Multi-Engine File Scanning** Simultaneous scanning against 70+ security engines — seconds to verdict on any file or hash.
- **AI Script Explanation** Code Insight AI explains malicious script behavior in plain English — no reverse engineering expertise required.
- **URL & IP Reputation** URL, domain, and IP reputation checking against global threat intelligence datasets.
- **YARA Retrohunt** Find historical samples matching a new detection rule across the entire VirusTotal corpus.

Key Benefits

- **Free Tier Value** Free tier provides significant analytical value at zero cost — accessible to any security team at any budget level.
- **Accessible Malware Analysis** Makes malware analysis accessible without reverse engineering expertise — democratizes advanced analysis capability.
- **Community-Powered Dataset** Continuously updated by global security researchers — one of the most current threat datasets available.
- **Universal SOC Standard** first-check tool for IOC verification in SOC environments worldwide — a foundational analyst skill dataset

Tenable One with AI

An exposure management platform combining vulnerability scanning, cloud security posture, identity exposure analysis, and AI-powered attack path modeling in one unified platform. Tenable One moves beyond raw vulnerability counts to genuine organizational exposure understanding.

Applications

- **Attack Path Modeling**: Models how vulnerabilities chain to reach critical assets — focusing remediation on paths that actually represent real risk to the business.
- **Predictive Exposure Scoring**: Scoring based on attacker behavior patterns consistently outperforms CVSS-only prioritization in real-world validation testing.
- **Cloud Security Posture**: Unified cloud security posture management alongside traditional vulnerability scanning in one platform.
- **Executive Reporting**: Business-readable executive exposure reporting bridges technical findings to board-level risk language.

Key Benefits

- **Beyond Vulnerability Counts**: Moves from raw CVE counts to genuine organizational exposure understanding — a fundamentally more useful risk picture.
- **Attack Path Intelligence**: Identifies which vulnerabilities actually matter by modeling real attacker paths to critical assets.
- **Unified Platform**: Combines vulnerability, cloud, and identity exposure in one platform — eliminating siloed risk views.
- **Board-Ready Communication**: Executive reporting translates technical exposure into business risk language for informed leadership decisions.

Qualys VMDR with TruRisk AI

A cloud-based vulnerability management platform with TruRisk AI — a risk scoring engine that weighs threat intelligence, asset criticality, and business context to produce genuine organizational risk scores rather than raw vulnerability counts. Particularly valuable for organizations facing direct ransomware risk.

Applications

- **Continuous Asset Discovery**: Continuous asset discovery and vulnerability scanning across the entire environment.
- **TruRisk Scoring**: AI risk scoring across exploitability, threat actor interest, and asset criticality — not raw CVSS scores.
- **AI-Optimized Patch Sequencing**: Patch sequencing optimized for maximum risk reduction speed — prioritizes what matters most.
- **Ransomware Risk Identification**: Specific identification of vulnerabilities actively exploited in ransomware campaigns.

Key Benefits

- **Sophisticated Prioritization**: TruRisk AI is among the most sophisticated vulnerability prioritization approaches available in the market.
- **Cloud-Based**: No scanner infrastructure to maintain — fully cloud-based with no on-premise hardware requirements.
- **Ransomware Focus**: Ransomware risk identification directly addresses the most financially damaging threat category facing enterprises.
- **ITSM Integration**: Direct remediation ticket creation in ServiceNow and ITSM platforms — puts tasks in systems IT teams already use.

Rapid7 InsightVM with AI Analytics

A live vulnerability management solution providing continuous asset discovery, real-world risk prioritization, and AI-powered remediation guidance — designed specifically around security and IT teams working together. InsightVM's live data model means the vulnerability picture never goes stale between scan cycles.

Applications

- **Live Data Model** Vulnerability data updated continuously — not point-in-time scans. The security picture is always current.
- **Real Risk Scoring** AI scoring using exploit availability and asset criticality — not raw CVSS scores that overweight theoretical severity.
- **IT Collaboration** Remediation projects bridge the security-to-IT handoff — the most common operational failure in vulnerability management programs.
- **Container & Cloud Coverage** Container image and registry vulnerability scanning with goal-based risk reduction tracking.

Key Benefits

- **Always-Current Visibility** Live data model eliminates the stale vulnerability picture problem between scan cycles — always accurate.
- **Practical Risk Prioritization** Real-world risk scoring focuses remediation effort on what attackers actually exploit — not theoretical CVSS severity.
- **Security-IT Alignment** Built-in collaboration tools bridge the security-to-IT handoff — solving the most common vulnerability management failure point.
- **Modern Environment Coverage** Container and cloud coverage ensures visibility across hybrid and modern infrastructure environments.

Metasploit with AI Integrations

The world's most widely used penetration testing framework, providing 2,000+ exploits, payloads, and post-exploitation modules. Modern AI integrations add intelligent attack path suggestions and automated reconnaissance — making the already powerful framework smarter and faster.

Applications

- **Exploitability Validation** Tests whether vulnerabilities are genuinely exploitable — validates real risk vs. theoretical scanner findings.
- **Lateral Movement Simulation** Lateral movement and privilege escalation simulation across target environments.
- **Social Engineering Payloads**: Social engineering payload and phishing campaign creation for comprehensive security testing.
- **AI Attack Chain Suggestions** AI-assisted attack chain suggestions across discovered vulnerabilities—accelerates penetration test coverage.

Key Benefits

- **Industry standard skills** are directly transferable across security roles — Metasploit proficiency is valued across penetration testing and red team.
- **Validates Real Exploitability** Confirms actual exploitability vs. theoretical scanner findings—eliminates false prioritization of non-exploitable CVEs.
- **Open-Source Core**: Open-source core is accessible at any budget level — the most democratized professional penetration testing framework available.
- **Rapid CVE Coverage**: The community maintains rapid exploit additions for newly disclosed CVEs — always current with the latest vulnerabilities.

Cobalt Strike

An advanced threat emulation platform used by professional red teams to simulate sophisticated adversary campaigns — mimicking specific nation-state and cybercriminal TTPs to test whether defenses would actually detect a real advanced attack. The gold standard for realistic advanced persistent threat simulation.

Applications

- **Named Actor Emulation** Simulate specific named threat actor TTPs — test whether your defenses would detect the adversaries most likely to target your organization.
- **C2 Infrastructure Simulation** Realistic command and control infrastructure simulation with lateral movement and persistence mechanism testing.
- **Multi-Operator Campaigns** Multi-operator coordinated red team campaign support — enabling enterprise-scale, realistic advanced attack exercises.
- **Detection Gap Identification** Identifies detection gaps that simpler tools consistently miss — validates whether advanced persistent threat detection actually works.

Key Benefits

- **Most Realistic APT Simulation** Identifies detection gaps that simpler tools consistently miss — provides genuine validation of advanced threat detection.
- **Blue Team Development** gives blue teams genuine experience defending against nation-state techniques before real attacks occur.
- **Career-Relevant Expertise**: Cobalt Strike proficiency is a valued credential in both red and blue team hiring — directly relevant to advanced security roles.
- **Dual-Use Awareness** Understanding Cobalt Strike deeply is essential for defenders seeking to detect and block its use in actual intrusions.

Cymulate Breach and Attack Simulation

An automated BAS platform that continuously tests security controls — email gateway, endpoint, lateral movement, and exfiltration defenses — against real attack scenarios without requiring a manual red team engagement. Delivers red team insights at a fraction of the cost and on a continuous basis.

Applications

- **Continuous Control Validation**: Replaces annual penetration tests with continuous automated testing — catching configuration drift before attackers exploit it.
- **MITRE ATT&CK Gap Mapping**: Clear, standardized coverage visibility showing exactly which techniques your controls detect and which they miss.
- **Email Gateway Testing**: Automated testing of email security controls against real phishing and malware delivery scenarios.
- **Exfiltration Simulation**: Tests data exfiltration defenses across network, endpoint, and cloud egress paths.

Key Benefits

- **Continuous vs. Annual Testing**: Replaces point-in-time penetration tests with always-on validation — catches drift the moment it occurs.
- **No Red Team Required**: Delivers red team insights at a fraction of the cost — democratizes security control validation for any organization.
- **Standardized Coverage Visibility**: MITRE ATT&CK mapping provides clear, comparable coverage metrics for reporting and benchmarking.
- **Configuration Drift Detection**: Catches security control degradation between manual assessments — the most common source of undetected exposure.

Proofpoint with AI

The market-leading enterprise email security platform using AI trained on one of the world's largest email threat datasets. Detects phishing, BEC, malware, and Gen AI-generated email threats before inbox delivery — with particular strength in business email compromise detection, the highest financial loss category in enterprise security.

Applications

- **Gen AI Phishing Detection**: AI detection of Gen AI-generated phishing at scale — trained on dataset breadth that no individual organization can replicate.
- **BEC Detection**: Business email compromise detection through linguistic analysis — the strongest in class against the highest financial loss category.
- **Click-Time URL Protection**: Click-time URL rewriting catches phishing sites built after email delivery — closing the gap legacy pre-delivery filters leave open.
- **VAP Identification**: Very Attacked Person identification enables proactive enhanced protection for highest-risk employees.

Key Benefits

- **Industry-Leading Detection**: Industry-leading detection rates in independent evaluations — validated against the broadest email threat dataset available.
- **BEC Best-in-Class**: BEC detection is strongest in class — directly addressing the email threat category responsible for the greatest enterprise financial losses.
- **Post-Delivery Coverage**: Click-time protection catches phishing sites built after email delivery — addressing a critical gap in pre-delivery-only architectures.
- **Proactive Risk Targeting**: VAP identification enables proactive enhanced protection for the employees most likely to be targeted.

Abnormal Security

A cloud-native email security platform using behavioral AI to build communication baselines for every employee — detecting attacks through behavioral deviation rather than content matching. Uniquely effective against Gen AI-generated phishing because it doesn't rely on content analysis at all.

Applications

- **Behavioral Baseline Building:** Per-employee communication baseline detects deviations — not content. Gen AI-generated phishing can't defeat behavioral analysis.
- **API Deployment:** Deploys in minutes via API — no MX record changes or mail flow disruption during deployment.
- **Vendor Compromise Detection:** Detects compromised vendor accounts — addressing BEC variants that originate from legitimate but hijacked supplier email systems.
- **Account Takeover Detection:** Identifies compromised internal accounts through behavioral deviation from established communication patterns.

Key Benefits

- **Gen AI Phishing Resistant:** Behavioral analysis cannot be defeated by Gen AI-generated content — uniquely effective against the fastest-growing phishing threat.
- **Instant Deployment:** API deployment in minutes with no MX record changes — zero mail flow disruption during rollout.
- **Low False Positives:** Exceptionally low false positive rates compared to content-based tools — reducing analyst burden from legitimate email misclassification.
- **Vendor Compromise Coverage:** Detects BEC variants originating from legitimate but hijacked supplier accounts — a gap most email security tools miss.

Vectra AI

A network detection and response platform using AI to detect attacker behavior across network traffic, cloud, and identity — focused specifically on the post-compromise phase when attackers are already inside. Attack signal intelligence correlates network, cloud, and identity signals into coherent, high-fidelity alerts that analysts can act on immediately.

Applications

- **Network Traffic Analysis:** AI analysis of network traffic for C2, lateral movement, and exfiltration behavior — post-compromise focused.
- **Cloud Threat Detection:** Cloud service activity threat detection across AWS, Azure, and GCP environments.
- **Identity Monitoring:** Active Directory and Azure AD privilege escalation monitoring — catches identity-based attack paths.
- **Attack Signal Intelligence:** Correlates network, cloud, and identity signals into coherent, high-fidelity alerts with full attack story assembly.

Key Benefits

- **Post-Compromise Coverage:** Fills the gap perimeter tools leave — detects attackers already inside the network before they achieve their objectives.
- **No Performance Impact:** Metadata-based analysis with no performance or privacy impact of full packet capture.
- **Signal Over Noise:** Attack signal intelligence surfaces genuinely important signals from noise — reducing analyst alert fatigue.
- **Long-Dwell Detection:** Particularly effective at detecting slow, stealthy long-dwell attacks that evade threshold-based detection.

ExtraHop Reveal(x) with AI

A cloud-native NDR platform using machine learning to analyze all network traffic in real time — providing full east-west visibility across hybrid and multi-cloud environments. Particularly strong for ransomware pre-detonation detection, where early lateral movement patterns are identifiable before encryption begins.

Applications

- **East-West Traffic Analysis** Full east-west visibility catches lateral movement that perimeter tools miss entirely — the blind spot where most ransomware operates.
- **Encrypted Traffic Analysis** Threat detection in encrypted traffic without decryption — addressing attackers hiding C2 in HTTPS and TLS sessions.
- **Ransomware Pre-Detection** Identifies staging and lateral movement patterns before encryption begins — stops ransomware before detonation.
- **Cloud-Native Scaling** Architecture scales without performance degradation across hybrid and multi-cloud footprints.

Key Benefits

- **East-West Blind Spot Coverage** catches lateral movement that perimeter tools miss entirely — the most critical gap in traditional network security architectures.
- **Encrypted Traffic Visibility** detects defense threats in encrypted traffic without decryption — maintains visibility as encryption adoption increases.
- **Pre-Detonation Ransomware Defense** Identifies ransomware staging before encryption begins — the only phase where full prevention is still possible.
- **Scalable Architecture** Maintains full visibility as environments grow — no performance degradation at enterprise scale.