ISSUE: 01

SkillWeed

CYBER MAGAZINE

TABLE OF CONTENTS

1. EDITOR'S NOTE:

BY AKINGBADE AKINFENWA, FOUNDER OF SKILLWEED

WELCOME TO THE FIRST-EVER ISSUE OF SKILLWEED CYBER MAGAZINE

When I started Skillweed, the goal was clear: to create a platform that would level the playing field and give aspiring cybersecurity professionals — especially Africans in the diaspora — a fair shot at meaningful careers. Today, that mission expands.

This magazine is more than a publication. It's a living, breathing reference point for everyone invested in cybersecurity. Whether you're just starting your journey, leading a SOC team, building secure infrastructure, or running a business that depends on tech resilience — *Skillweed Cyber Magazine* is built with you in mind.

I want a beginner to pick this up and feel guided — to know where to go, what to learn, and who to follow. I want professionals to read an article and nod in agreement and spur critical thinking, I want entrepreneurs and hiring managers to see this as a ranking tool — a window into the best players, practices, and progress in cybersecurity Globally.

This is our first issue. It's the beginning of something audacious. And you're reading it — which makes you part of the movement.

Welcome to *Skillweed Magazine* — where skill meets insight, and growth becomes inevitable.

INSIDE THIS MAIDEN ISSUE

This first edition of *Skillweed Magazine* sets the stage for what we hope will become an essential reference for cybersecurity professionals, learners, and leaders across the globe.

We've curated this issue to deliver both insight and action — blending practical tools, expert voices, and global trends in a format that's clear, informative, and empowering.

INDUSTRY PULSE

We begin with a scan of the current cybersecurity landscape — from major breaches and emerging threat vectors to global compliance updates like GDPR, NIST, ISO, and local regulations that impact the way we secure systems.

TOOL & TECHNOLOGY RANKINGS

Choosing the right tools can make or break your security posture. This section features our **Top 10 SIEM Solutions for 2025**, comparative reviews of **Endpoint Protection Platforms**, and a

spotlight on **emerging cybersecurity tools** to watch. Each ranking is based on real user feedback, expert testing, and performance metrics.

RESOURCE HUB

For the lifelong learners, we've gathered the best **free and paid platforms**, **certification programs**, **books**, **research papers**, **newsletters**, and **forums** to help you stay updated, connected, and continuously growing in your field.

IN-DEPTH TOOL ANALYSIS

Need help choosing between **Splunk, QRadar, or LogRhythm**? Want to understand how **GRC platforms** like Archer and LogicGate stack up? We've done the deep dives — with hands-on comparisons and key takeaways for every category, including **cloud security** and **pen testing suites**.

EXPERT INSIGHTS

In this issue, we hear from CISOs, Skillweed instructors, and global thought leaders on the frontlines of security. Expect bold opinions, grounded advice, and a look ahead into the future of cybersecurity — especially for African professionals around the world.

CAREER & CERTIFICATION GUIDE

Whether you're switching careers, just starting out, or mapping your next move, this guide breaks down roles, skills, and certification pathways (CompTIA, CISSP, CISM, and more). Plus, hear real "How I Broke In" stories from Skillweed alumni — and explore our **curated job board**.

CASE STUDIES & SUCCESS STORIES

From real-world breach investigations to student transformations and organizational GRC overhauls, these stories show the wins, the mistakes, and the lessons that stick.

COMMUNITY SPOTLIGHT

We shine a light on the Skillweed community — from member milestones to expert-led Q&As and upcoming community events, hackathons, and webinars. It's about learning *and* lifting each other up.

PRACTICAL LABS & CHALLENGES

This hands-on section includes labs on **risk assessment**, **vulnerability scanning**, and **incident response**, plus our **monthly Capture the Flag (CTF)** challenge — complete with walkthroughs to sharpen your skills.

MARKETPLACE & PRODUCT WATCH

Get the latest on product launches, vendor updates, and exclusive reader discounts. Whether you're a buyer, builder, or budgeter — we've got you covered.

EVENTS CALENDAR

Don't miss a beat — we've compiled upcoming **global cybersecurity events**, **Skillweed-hosted webinars**, and key dates worth saving.

FEEDBACK & NEXT ISSUE PREVIEW

We want to hear from *you*. Share your thoughts, rate this issue, and get an early peek at what's coming next — including themed features and deep dives.

BONUS FEATURES

Rounding off the issue, we're introducing a few special editions, including **Women in Cybersecurity**, **Cybersecurity for Startups**, and a dedicated **Legal & Compliance Corner** for navigating regulatory waters.

This is more than a magazine. It's your map, your mentor, and your momentum.

Let's build together.

Team Skillweed

2. INDUSTRY PULSE

Staying ahead in cybersecurity means keeping a finger firmly on the industry's ever-shifting pulse. This section gives you a rapid yet authoritative overview of the issues that demand your attention now - even if you're a practitioner, executive, or simply cyber-curious. Discover what's changing, what's trending, and what risks are looming on the horizon—equipping you to make smarter, faster, and safer decisions in a connected world.

LATEST CYBERSECURITY NEWS AND TRENDS

As we settle into mid-2025, the cybersecurity landscape continues to evolve at a breakneck pace, demanding vigilance and innovation from all stakeholders. Here are some trends to look out for.

HARNESSING AI FOR ADVANCED THREAT INTELLIGENCE

Artificial intelligence (AI) in 2025 continues to revolutionize cybersecurity by enabling real-time threat detection and automated response. AI-powered systems analyze vast data streams using predictive analytics to identify potential cyber threats before they strike, significantly reducing response times. Businesses effectively integrating AI into their cybersecurity strategies gain a competitive edge in combating evolving threats such as adaptive malware and phishing campaigns that evade traditional defenses.

ADOPTION OF ZERO-TRUST ARCHITECTURE

Zero-Trust security has become a standard approach for modern cybersecurity frameworks. It eliminates implicit trust, requiring continuous verification of all users and devices, regardless of their location inside or outside the network perimeter. The model's emphasis on least-privilege access, micro-segmentation, and continuous session validation is crucial as hybrid and remote work environments expand attack surfaces. Organizations adopting Zero-Trust report improved containment of breaches and reduced lateral movement risks.

SECURING 5G NETWORKS

The worldwide rollout of 5G networks increases connectivity but simultaneously introduces new risks. Faster speeds and more connected devices expand the attack surface, exposing networks to potential data interception and unauthorized access. Security experts recommend robust encryption, strong authentication protocols, and continuous network monitoring tailored to 5G's architecture. Effective 5G security strategies ensure reliable and safe operation of the next-generation internet infrastructure.

IOT DEVICE SECURITY CHALLENGES

The explosion of Internet of Things (IoT) devices in businesses and homes greatly expands potential vulnerabilities. Many IoT endpoints lack adequate security measures, making them attractive targets for cybercriminals who can use compromised devices as entry points into larger networks. Organizations must enforce strong authentication, multi-factor authentication (MFA), and implement regular patch management to protect these devices and mitigate risks.

BIOMETRIC ENCRYPTION FOR ENHANCED AUTHENTICATION

Traditional passwords are increasingly insufficient against sophisticated cyber threats. Biometric encryption, leveraging fingerprints, facial recognition, or iris scans, is gaining traction by providing higher security levels and mitigating risks like identity theft. By converting biometric data into encrypted keys, this method strengthens access control systems and aligns with evolving cybersecurity demands.

CLOUD SECURITY TAKES CENTER STAGE

With cloud adoption surging, securing cloud environments is critical. Data breaches, misconfigurations, and unauthorized access remain common issues. Adoption of multi-cloud strategies, encryption of data at rest and in transit, and regular security audits are essential practices. Organizations must also comply with regulations to maintain robust cloud security postures.

RISING THREAT OF AI-POWERED CYBERATTACKS

Cybercriminals are increasingly using AI to craft adaptive attacks that mutate malware and phishing techniques in real time, evading conventional detection tools. AI-generated phishing campaigns and deepfake technology exacerbate social engineering threats. Defenders must leverage AI-driven anomaly detection and advanced threat hunting techniques to counter these sophisticated attacks effectively.

SUPPLY CHAIN ATTACKS AND VENDOR RISKS

Supply chain vulnerabilities remain a top concern. Attackers exploit third-party software and vendor weaknesses to launch widespread breaches, as evidenced by high-profile cases like SolarWinds. Organizations are strengthening vendor risk management through continuous monitoring, contractual security requirements, and real-time compliance checks to reduce exposure.

EMERGING THREATS: QUANTUM COMPUTING AND DEEPFAKES

While quantum computing remains nascent, its potential to break current encryption standards drives early adoption of quantum-resistant algorithms. Deepfake technology also poses rising social engineering risks, enabling realistic impersonation in scams and disinformation campaigns. Cybersecurity professionals are prioritizing preparedness for these emerging threats.

CONVERGENCE OF IT AND OT SECURITY

Integration of Information Technology (IT) and Operational Technology (OT) environments, especially in critical infrastructure and manufacturing, creates new security challenges.

Attackers target OT to disrupt production lines or critical systems. Organizations are implementing unified monitoring and advanced security controls to protect the full spectrum of their environments.

REGULATORY UPDATES (GDPR, NIST, ISO, LOCAL LAWS)

Remaining compliant in an increasingly complex regulatory environment is vital for cybersecurity resilience. Here are some updates.

GDPR (GENERAL DATA PROTECTION REGULATION) UPDATES

- Artificial Intelligence & Data Protection:

  Regulators across the EU have issued new guidance on the use of AI in processing personal data, emphasizing transparency, fairness, and the right to explanation for automated decisions. Organizations must now clearly document AI models' decision-making logic and ensure data minimization when using AI tools on personal data.

- Enforcement Actions Rise:

  2025 has seen record fines for data breaches, with enforcement increasingly targeting both large corporations and SMEs. Regulators are closely scrutinizing cross-border data transfers, particularly when using cloud providers or third countries.

- Children's Privacy Focus:

  Greater regulatory attention is on protecting minors, requiring additional parental consent mechanisms and stricter processing standards for platforms frequented by young users.

- Data Subject Rights:

  Emphasis on facilitating easier data subject access requests, deletion, and portability, with regulators penalizing delays and non-compliance.

NIST CYBERSECURITY FRAMEWORK (CSF)

- NIST CSF 2.0 Launched:

  The newest version, NIST CSF 2.0, released in early 2025, emphasizes integrating *governance* as a new core function and expands guidance on *supply chain risk management*.

- AI & Emerging Tech Governance:

  Updated guidelines now address managing AI/ML risks and securing emerging technologies like quantum computing. The framework includes more actionable controls for risk assessment, threat intelligence, and incident response tailored to dynamic threat environments.

- Global Alignment:

  NIST 2.0 is increasingly harmonized with international standards (like ISO/IEC 27001), making compliance easier for multinational organizations.

ISO STANDARDS (FOCUS: ISO/IEC 27001 & FRIENDS)

- ISO/IEC 27001:2022 Transition Deadline Nearing:

  Organizations must transition from the 2013 version to ISO/IEC 27001:2022 by October 2025 to maintain certification. This updated standard includes:

  - Expanded cloud security requirements
  - Explicit risk management guidance
  - New controls covering threat intelligence, physical security monitoring, and data masking

- ISO/IEC 42001: AI Management System:

  A new standard for managing risks related to artificial intelligence launched in 2025. This aims to ensure ethical and secure AI design, implementation, and operation.

- Sector-Specific Updates:

  Ongoing revisions to related standards (ISO/IEC 27701 for privacy, ISO/IEC 22301 for business continuity) further align information security with privacy and resilience requirements.

LOCAL & NATIONAL CYBERSECURITY LAWS

- US State Privacy Laws:

  Over a dozen new or revised state-level privacy laws (e.g., California CCPA/CPRA amendments, Virginia's VCDPA, Texas Data Privacy and Security Act) have taken effect in 2025. These generally provide:

  - Expanded rights for consumers (such as opt-out of targeted advertising)
  - Stronger notification mandates for breaches
  - Obligations for risk and impact assessment, especially for sensitive personal data

- EU Digital Operational Resilience Act (DORA):

  Enters into force January 2025 for financial services and related sectors, imposing strict cyber resilience, incident reporting, and third-party risk management obligations.

- National Critical Infrastructure Rules:

  Several countries now mandate baseline cybersecurity controls for operators in sectors like energy, healthcare, and transport. These laws require adherence to international standards (often NIST or ISO-inspired) and regular audits.

- Cross-Border Data Transfer Mechanisms:

  Ongoing developments in international data transfer frameworks, such as the EU-U.S. Data Privacy Framework, are providing new legal bases for transatlantic data flows post-Schrems II.

Staying updated on these evolving regulations is essential for compliance and robust cyber risk management. Organizations should review their current controls, update documentation, and train staff on new requirements to maintain resilience and avoid costly penalties. Is your organization compliant?

GLOBAL THREAT LANDSCAPE: NEW ATTACK VECTORS AND MAJOR BREACHES

As of mid-2025, the global cybersecurity threat landscape is more complex and perilous than ever. Recent reports highlight a surge in state-sponsored attacks, AI-powered cybercrime, and sophisticated ransomware campaigns, placing governments, enterprises, and individuals under constant risk.

STATE-SPONSORED CYBER ATTACKS ESCALATE

Alleged Middle - Eastern hackers have dramatically increased their offensive operations, targeting U.S. critical infrastructure sectors such as transportation and manufacturing with a 133% surge in attacks tracked in recent months. Multiple advanced persistent threat (APT) groups, including MuddyWater and OilRig, have exploited vulnerabilities in operational technology and industrial control systems, signaling a shift toward more destructive cyber warfare tactics. European nations, particularly France, face similar espionage attempts from Chinese-backed groups using zero-day exploits on VPN appliances to infiltrate government

networks. Meanwhile, North Korean cyber operations continue covert recruitment for regime funding. These activities underline the growing geopolitical dimension of cyber threats in 2025.

AI-POWERED CYBERCRIME IS ON THE RISE

Artificial Intelligence is a double-edged sword—while enhancing defense mechanisms, cybercriminals are deploying AI to automate and sophisticate attacks. AI-generated phishing campaigns and malware variants adapt in real-time, evading traditional defenses and increasing success rates.

Deepfake technology compounds social engineering threats, with an expected explosion in fake videos and audio impersonations used to deceive individuals and manipulate public opinion.

RANSOMWARE REMAINS A DOMINANT THREAT

Ransomware gangs continue refining "double extortion" tactics, encrypting data while threatening public release to pressure victims. Recent large-scale attacks have shut down essential services, underscoring the critical need for effective backup strategies and incident response readiness.

EMERGING TECHNICAL VULNERABILITIES

July's Microsoft Patch Tuesday unveiled 137 security flaws across widely used products, including a high-profile zero-day in SQL Server. Automotive cybersecurity also faces new risks, with Bluetooth vulnerabilities in millions of vehicles enabling remote code execution potentially allowing attackers to control vehicle systems or spy on occupants. These technical exposures reinforce the urgency for rapid patching and proactive vulnerability management.

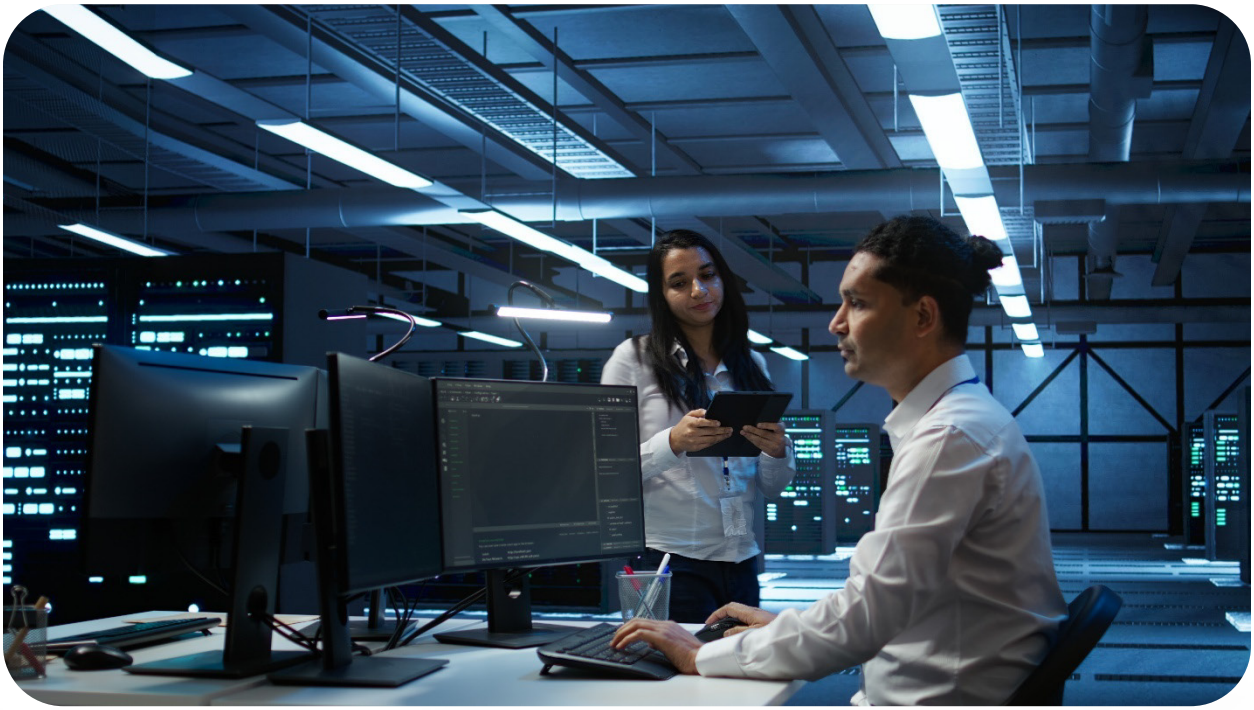
SUPPLY CHAIN AND CLOUD RISKS

More than half of large organizations cite supply chain vulnerabilities as their biggest cybersecurity barrier. Attacks exploiting third-party software and services remain a top cause of breaches, requiring continuous vendor monitoring and strict security controls. Cloud misconfigurations continue to cause significant data exposures, driving greater adoption of multi-cloud security governance.

TALENT SHORTAGE AND HUMAN RISK

The global cybersecurity workforce gap widens, leaving two-thirds of organizations understaffed and vulnerable. Attackers increasingly exploit human error—phishing remains the top vector—highlighting the need for comprehensive training and security awareness. Understanding these evolving threats helps organizations prioritize defenses, implement cutting-edge technologies, and cultivate a security-first culture. Stay vigilant, update your systems regularly, and educate your teams to reduce risk in this dynamic cybersecurity environment.

3. TOOL & TECHNOLOGY RANKINGS



Selecting the right tools and technologies is crucial for protecting organizations against increasingly sophisticated threats. Our Tool & Technology Rankings deliver a comprehensive evaluation of the best cybersecurity solutions available in 2025, based on critical performance metrics.

These rankings help security leaders and professionals navigate the complex market by highlighting solutions that combine innovative features—including AI-driven threat detection and automated incident response—with practical usability and strong customer support.

Based on our metrics, here are Top 10 SIEM Solutions for 2025.

Here is a comparative analysis table including strengths, weaknesses, and available pricing insights for the top SIEM solutions in 2025:

SIEM Solution	Strengths	Weaknesses	Pricing Overview (Estimated)
Hunters AI-Driven SIEM	- Ease of use, AI-driven automation - Fast incident detection and response - Ideal for small to medium teams	- May lack extensive customization for large enterprises - May require tuning for complex environments	Pricing details are not widely public but positioned as cost-effective for SMEs. Vendor quotes required for specifics.
IBM QRadar	Combines AI with deep threat intelligence Strong compliance modules Scalable for enterprises	Can be complex to deploy and manage Potentially high costs for smaller businesses	Typically subscription-based; pricing may depend on EPS (Events Per Second). Estimated enterprise pricing in $thousands.
Rapid7 InsightIDR	Strong endpoint detection and behavioral analytics Integrated automation and threat intelligence	Pricing can be high for smaller organizations May require expertise for advanced customization	Subscription pricing based on assets or users. Mid-to-high range pricing tier.
Securonix	Advanced UEBA and big data ingestion Flexible detection rules	Requires careful tuning and engineering support Complexity can challenge smaller teams	Pricing often by EPS or license; high-end enterprise pricing typical.
Panther Labs	Custom detection-as-code (Python) Real-time processing pipelines Strong DevSecOps integration	Best suited for engineering-heavy teams Can have a steeper learning curve	Pricing generally based on data ingestion or per asset; scalable model but may be premium for feature-rich usage.
Splunk Enterprise Security	High coverage and scalability Strong threat intelligence and automation Widely adopted in large enterprises	Complex to deploy Potentially expensive licensing and operational costs	Ingest-based pricing from approx. $1,800 to $18,000+ per year for 1-10 GB/day data volumes. Flexible but costly.

SIEM Solution	Strengths	Weaknesses	Pricing Overview (Estimated)
Microsoft Sentinel	Cloud-native Integrated SOAR capabilities Excellent for hybrid cloud and compliance	Dependent on Azure ecosystem Costs can grow with data ingestion	Consumption-based pricing; pay-per-use model; cost-effective for Azure-heavy organizations.
LogRhythm	Endpoint monitoring, network analysis, UEBA - Compliance-focused SaaS or on-premises	UI and UX may feel outdated to some users Pricing is enterprise-level	Typically licensed per node or assets monitored; mid to high range pricing common.
FortiSIEM (Fortinet)	Unified monitoring across network, endpoint, application Automated correlation and remediation	Can be complex to configure Best suited for Fortinet ecosystem users	Pricing often EPS or license-based; competitive for organizations already using Fortinet products.
Sumo Logic	Cloud-native real-time analytics Machine learning to reduce false alarms Strong hybrid support	Pricing can escalate with large data volumes Learning curve for complex rule creation	Volume/data ingestion-based pricing; starts reasonably but can increase sharply with data volume growth.

This analysis synthesizes recent industry data and vendor information from multiple sources sighted at the end of the chapter.

BEST ENDPOINT PROTECTION PLATFORMS

Based on key metrics such as user reviews, expert testing, performance (detection rate, response time, false positives), and market reputation from various 2025 sources, here is a ranked comparison table of the Best Endpoint Protection Platforms (EPP) for 2025:

Rank	Endpoint Protection Platform	Strengths	Weaknesse s	Notable Features	Pricing Overview
1	CrowdStrike Falcon	AI-powered threat detection, cloud-native, excellent EDR, real-time response	Pricing can be high for smaller businesses	Lightweight agent, threat hunting, behavioral detection	Premium pricing; enterprise-level
2	Microsoft Defender for Endpoint	Seamless Windows integration, real-time vulnerability management, cost-effective	Best suited for Windows environments; some features require Azure	Integrated with Windows Security, threat intelligence	Consumption-based; affordable for Windows-heavy orgs
3	SentinelOne Singularity	Autonomous AI-driven detection and remediation, unified console, XDR capabilities	Higher cost; learning curve for advanced features	Automated response, machine-speed detection	Subscription; premium tier
4	Sophos Intercept X	Strong anti-ransomware, AI-based malware detection, EDR	Some features require add-ons, limited customization	Ransomware rollback, deep learning models	Mid-range to high pricing
5	Bitdefender GravityZone	Multi-layer ransomware protection,	Complexity in configuring some	Cloud-based threat intelligence, strong	Competitive pricing, flexible plans

Rank	Endpoint Protection Platform	Strengths	Weaknesse s	Notable Features	Pricing Overview
		integrated VPN, lightweight	advanced features	malware detection	
6	Trend Micro Apex One	AI learning for multi-layer ransomware protection, centralized management	Resource-in tensive, potentially high cost	Automated threat detection, data loss prevention	Mid to high pricing
7	McAfee Endpoint Security	Reliable threat detection, multi-device support, strong reporting	Can be resource-he avy, UI dated	Web security, encryption, centralized threat managemen t	Mid-range pricing
8	Webroot Endpoint Protection	Cloud-based real-time threat intelligence, minimal system impact	Limited advanced features, smaller vendor support	Fast scanning, behavioral analysis	Affordable
9	Kaspersky Endpoint Security	High malware detection rates, enterprise-grade encryption	Geopolitical concerns in some markets, cost	Advanced encryption, endpoint control	Mid to high pricing
10	ESET PROTECT Advanced	Cross-platform support, good UI, specific cloud and virtual machine scanning	Limited Linux support, moderate customizati on	Data loss prevention, remote managemen t	Competitive mid-range pricing

EMERGING TOOLS TO WATCH

Based on the metrics for evaluating emerging cybersecurity tools—focusing on innovation, threat detection and response efficiency, coverage and integration, adaptability, risk reduction, productivity gains, market adoption, and compliance alignment—and considering recent authoritative sources identifying innovative startups and new entrants to watch in 2025, here is a ranked comparative table of "Emerging Tools to Watch" including some of the most innovative cybersecurity startups and new entrants shaping the industry this year:

Rank	Startup / Tool Name	Description / Innovation Focus	Strengths	Weaknesses / Challenges	Notable Market Validation & Funding
1	Cyware	Full-stack cyber-fusion platform; threat intelligence and collaboration automation	Strong automation for threat analysis and fusion; trusted by Fortune 500 and government agencies	Enterprise-oriented; complexity may challenge smaller teams	Highly regarded; broad enterprise adoption
2	NordSecurity	Privacy-focused cybersecurity products including VPN, password management	User-friendly, privacy-first tools; strong customer base; unicorn status	Mainly consumer and SMB focus	$1B+ valuation; $100M funding round 2022
3	Snyk	Developer-first application security platform; code-to-cloud security	Focus on securing developer pipelines with integrated vulnerability management	Steep learning curve for non-developer users	Forbes Cloud 100; major clients like Google, Salesforce
4	Orca Security	Agentless cloud security platform for multi-cloud environments	Agentless design reduces operational overhead; comprehensiv	May lack some endpoint features	Ranked #24 CNBC Disruptor 50; strong cloud

Rank	Startup / Tool Name	Description / Innovation Focus	Strengths	Weaknesses / Challenges	Notable Market Validation & Funding
			e cloud workload protection		security presence
5	Torq	No-code automated security orchestration platform	Streamlines workflow automation for EDR, SIEM, XDR; reduces manual effort	Newer platform, adoption in mid-market growing	Well-funded; fast growth in automation space
6	Abnormal Security	AI-driven email security with behavioral analytics	Leading behavioral AI for email threat protection; reduces phishing by ~70%	Specialized on email security	$557M funding, Series D; Forbes Top 50 AI Firms
7	Cycode	Application Security Posture Management with machine learning	Early vulnerability detection in development pipelines; developer-friendly	Primarily SaaS/app developer focused	Growing adoption; strong ML integration
8	GitGuardian	Automated secret detection to prevent sensitive data leaks	Real-time secret detection in source code repositories	Niche focus on secrets management	Widely used by developer, security & compliance teams

Collectively, this chapter equips you with a structured understanding of current leaderboards and the frontier of cybersecurity solutions. It balances technical depth with strategic insight, fostering informed tool selection and future-proof security planning in an increasingly complex cyber threat environment.

4. RESOURCE HUB

In a field that evolves as fast as cyber threats do, staying current isn't optional — it's essential. If you're just starting out or sharpening your expertise, the right resources can make all the difference. This chapter curates the best of the best: from trusted **free and paid learning platforms**, to **must-read books and groundbreaking research**, and the **podcasts, newsletters, and forums** that keep the global cyber community connected. Think of this as your go-to guide for lifelong learning, skill building, and staying ahead of the curve in cybersecurity. Let's dive in.

FREE & PAID LEARNING PLATFORMS

Below are the top three free and paid cybersecurity learning platforms in 2025, featuring highly regarded MOOCs, certifications, and training portals based on expert reviews and user feedback.

TOP FREE LEARNING PLATFORMS

1. TRYHACKME

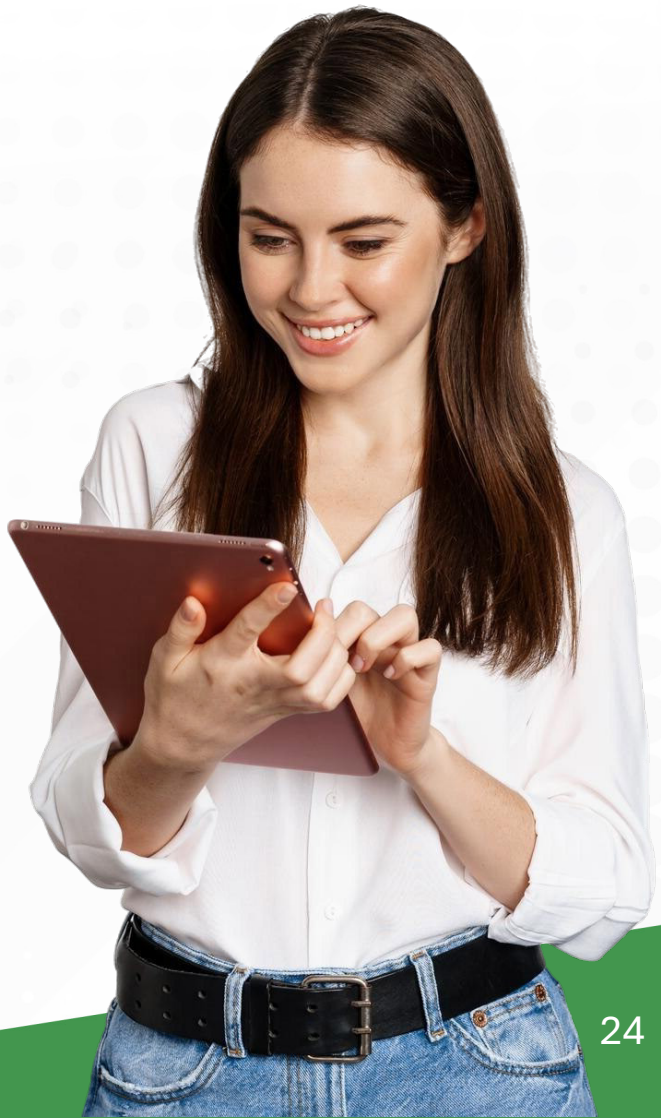
TryHackMe is widely celebrated for its hands-on, beginner-friendly approach to cybersecurity education. It offers comprehensive modules from complete beginner to advanced levels, covering topics such as Linux fundamentals, network security, cryptography, and penetration testing. Interactive Capture the Flag exercises and walkthroughs allow learners to practice skills in realistic scenarios, making it ideal for self-paced learning without cost.

2. HACK THE BOX

Primarily focused on offensive security, Hack The Box provides a live training environment where learners hack into intentionally vulnerable machines. It offers both free and paid tiers, giving users access to retired challenges with community-written guides as well as active challenges to test skills and gain rankings. This platform is excellent for users wanting practical penetration testing experience and deep understanding of vulnerabilities.

3. EC-COUNCIL ESSENTIALS SERIES

The EC-Council Essentials Series offers a free foundational set of courses in Ethical Hacking, Digital Forensics, and Network Defense. Designed for beginners and early-career professionals, it combines expert videos, detailed manuals, and optional hands-on labs to build practical cybersecurity skills. This free series is a great starting point for those seeking industry-recognized baseline certifications.



TOP PAID LEARNING PLATFORMS AND CERTIFIATIONS

1. GOOGLE CYBERSECURITY PROFESSIONAL CERTIfiCATE (COURSERA)

This beginner-friendly, self-paced certificate program emphasizes practical skills in using industry-standard tools like SQL, Linux, IDS, and Python. It also includes AI training, which is highly valued by employers. The course prepares learners for roles such as cybersecurity analyst and security administrator. Available via Coursera Plus for about $59 per month, it combines affordability with excellent career preparation.

2. STATIONX

StationX offers an expansive library of over 30,000 cybersecurity and IT classes suited for all levels—from novices to seasoned professionals. Their standout Fast Track program provides mentorship, personalized learning paths, virtual labs, and exam simulations. Course bundles range from $19 to $65, while memberships offer deeper career support and community engagement, making it a robust paid option.

3. COMPTIA SECURITY+ CERTIfiCATION TRAINING

Esteemed as an industry-standard certification, CompTIA Security+ covers fundamental security concepts relevant to a broad range of roles. Paid certification training programs are widely available through multiple providers, often including interactive labs and exam preparation materials. It is valued for boosting marketability and entry into cybersecurity careers.

Selecting the right cybersecurity learning platform depends on your current skill level, learning style, and career goals. Free platforms like TryHackMe and Hack The Box provide invaluable hands-on experience without cost, ideal for beginners and those looking to sharpen practical skills. Meanwhile, paid options such as Google's Cybersecurity Professional Certificate, StationX, and CompTIA Security+ training offer structured, mentor-supported education and recognized certifications to accelerate career growth.

Leveraging these top-rated platforms will empower you to build strong cybersecurity knowledge, advance your skills, and stand out in this competitive field in 2025 and beyond.

MUST-READ BOOKS & RESEARCH PAPERS FOR ALL LEVELS

Having access to the right books and research papers can accelerate your learning journey; whether you're a beginner seeking to learn or a pro seeking to improve or stay updated. Below is a curated list of three must-read books and research papers suited for all levels in 2025, designed to offer comprehensive insights across theory, practice, and cutting-edge developments.

1. FOR BEGINNERS: "CYBERSECURITY FOR BEGINNERS" BY RAEF MEEUWISSE

This accessible book provides a solid introduction to essential cybersecurity concepts, including risk management, cryptography basics, network security, and common cyber threats. Written in clear, non-technical language, it is ideal for students and entry-level professionals seeking to build a strong foundational understanding of the cybersecurity landscape.

2. FOR INTERMEDIATE LEARNERS: "THE CUCKOO'S EGG: TRACKING A SPY THROUGH THE MAZE OF COMPUTER ESPIONAGE" BY CLIFFORD STOLL

A classic narrative that explores real-world cybersecurity and incident response through the author's experience tracking a hacker in the 1980s. Beyond its engaging storytelling, this book offers practical lessons on system monitoring, threat hunting, and investigative techniques, making it perfect for those expanding from theory into applied security.

3. FOR ADVANCED PROFESSIONALS: NIST SPECIAL PUBLICATION 800-207, "ZERO TRUST ARCHITECTURE" (2020)

This authoritative research paper outlines the comprehensive framework and guiding principles of Zero Trust security, now a cornerstone of modern cybersecurity strategies. It is critical reading for experts designing and implementing advanced security architectures that move beyond perimeter defenses to continuous verification and risk-based access control.

A balanced reading list that spans foundational books, engaging real-world case studies, and cutting-edge research papers equips cybersecurity professionals at every stage for success.

By integrating these must-read resources into your learning routine, you will sharpen your skills, enhance your strategic perspective, and remain agile in the face of today's complex and rapidly changing cybersecurity challenges.

PODCASTS, NEWSLETTERS & FORUMS

Podcasts, newsletters, and forums offer accessible, timely insights and foster valuable connections with peers, experts, and thought leaders. If you're seeking the latest news, deep technical discussions, or interactive peer support, these resources help you remain current, sharpen your skills, and broaden your professional network.

TOP 3 PODCASTS FOR CYBERSECURITY PROFESSIONALS IN 2025

1. Darknet Diaries

   Hosted by Jack Rhysider, this podcast tells gripping true stories from the dark side of the internet, including hacking incidents, cybercrime investigations, and threat actor profiles. It combines storytelling with technical analysis, making it suitable for both newcomers and advanced practitioners. Available on Spotify, Apple Podcasts, and others.

2. Unsupervised Learning

   Hosted by Daniel Miessler, this weekly podcast delivers curated cybersecurity news and expert insights blending security, technology, and societal trends. With concise episodes that analyze key developments and interviews, it's ideal for staying updated efficiently.

3. CyberWire Daily

   A trusted daily briefing podcast for security professionals covering the latest cybersecurity news, incidents, and expert interviews. It's a great resource for quick, reliable updates on emerging threats and industry trends.

TOP 3 NEWSLETTERS TO FOLLOW IN 2025

- Krebs on Security Newsletter – Brian Krebs offers well-respected investigative journalism and analysis on cybercrime and security trends.
- SANS NewsBites – A twice-weekly digest summarizing the most important cybersecurity news with expert commentary from the SANS Institute.
- Troy Hunt's Weekly Update – Focuses on data breaches, web security, and privacy issues with practical insights from a renowned security researcher.

TOP 3 CYBERSECURITY FORUMS & COMMUNITIES

1. Reddit r/cybersecurity

   A highly active online forum with discussions on news, tools, career advice, and latest vulnerabilities. It's great for crowd-sourced knowledge and community support.

2. Stack Exchange Information Security

   A Q&A forum designed for professional and enthusiast security practitioners to ask technical questions and share expert solutions.

3. CyberSecJobs Forum

   Blends cybersecurity career opportunities with community discussions about tools, certifications, and industry events, valuable for networking and professional growth.

Podcasts, newsletters, and forums provide continual access to cybersecurity knowledge and peer interaction, essential for navigating today's rapidly evolving threat landscape.

By integrating these trusted resources into your routine, you can stay informed about critical developments, discover practical guidance, and connect with a vibrant community of security professionals worldwide.

5. IN-DEPTH TOOL ANALYSIS

Understanding the nuances of top solutions across key categories—Security Information and Event Management (SIEM), Governance, Risk, and Compliance (GRC) platforms, penetration testing suites, and cloud security tools—empowers organizations to build resilient security programs tailored to their unique environments. This in-depth tool analysis dives into leading contenders in each category, highlighting their capabilities, differences, and ideal use cases to help you make informed decisions.

SIEM DEEP DIVE: SPLUNK VS. IBM QRADAR VS. LOGRHYTHM

SPLUNK ENTERPRISE SECURITY

Renowned for its scalability, Splunk excels in handling large data volumes with powerful analytics, anomaly detection, and user behavior analytics (UEBA). Its flexible data ingestion supports a wide variety of sources, making it suitable for large enterprises with complex, heterogeneous environments. Splunk's rich visualization tools and advanced AI/ML capabilities simplify threat hunting and incident response. However, its complexity and higher cost can be challenging for smaller teams or those seeking simpler deployment.

IBM QRADAR

A market leader in enterprise SIEM, QRadar integrates deep threat intelligence and

AI-driven automation to reduce alert fatigue and speed investigations. Its strong compliance reporting and scalable architecture suit organizations with rigorous regulatory demands. QRadar also features advanced network traffic analytics and broad asset coverage. While powerful, implementation can require substantial expertise, and pricing varies based on events per second (EPS), potentially limiting adoption by smaller firms.

LOGRHYTHM

Known for combining endpoint monitoring, network traffic analysis, and UEBA in an integrated platform, LogRhythm is appreciated for its balanced feature set and focus on compliance. It offers both cloud and on-premises deployment flexibility. While its user interface may feel outdated compared to competitors, its robust detection and response capabilities make it a solid choice for organizations requiring comprehensive visibility with moderate complexity.

For enterprises with sprawling IT ecosystems and the budget to match, Splunk is a powerhouse that brings advanced analytics and extensibility. IBM QRadar suits organizations prioritizing compliance and integrated threat intelligence within a scalable framework, while LogRhythm appeals to those wanting a balanced, compliance-friendly SIEM without overwhelming complexity.

GRC PLATFORMS: COMPARING ARCHER, RISKRHINO, AND LOGICGATE

RSA ARCHER

A veteran in GRC, Archer offers a comprehensive, highly configurable platform supporting risk management, compliance, audit, and business continuity. Its strength lies in deep integration capabilities and extensive out-of-the-box content for varied governance use cases. The platform targets large enterprises with mature GRC programs but may be costly and complex to tailor.

RISKRHINO

A rising player, RiskRhino emphasizes user-friendly design and AI-powered risk assessments. It automates risk quantification and vendor risk management while providing dynamic dashboards. Targeted at mid-sized organizations seeking agile, intuitive GRC without heavy customization, it promotes rapid adoption but may lack some enterprise-grade integrations.

LOGICGATE

LogicGate balances flexibility and simplicity through a drag-and-drop workflow designer that suits diverse GRC processes. Known for quick deployment and scalability, it supports risk, compliance, audit, and vendor management. It appeals to organizations across sizes looking for customizable GRC automation with an accessible user interface.

If your GRC needs extensive customization and integration across many business units, Archer offers depth and breadth. For those desiring AI-assisted automation and ease of use, RiskRhino provides a modern, agile approach. LogicGate offers a middle ground with flexible, no-code workflows ideal for organizations wanting quick wins and ongoing scalability.

PENETRATION TESTING SUITES: METASPLOIT, BURP SUITE, AND ALTERNATIVES

METASPLOIT FRAMEWORK

The gold standard for penetration testing, Metasploit provides a vast collection of exploits, payloads, and auxiliary modules. It supports both manual testing and automation, making it a versatile tool for red teams and security researchers. It's open-source, with commercial versions offering enhanced features and support. Its steep learning curve necessitates skilled operators.

BURP SUITE

Focused on web application security, Burp Suite provides a powerful proxy, scanner, and vulnerability analysis tools. The Professional edition enhances automation and advanced testing options. Its user-friendly interface and comprehensive suite make it ideal for security analysts concentrating on app-layer threats. Burp Suite integrates well with CI/CD pipelines.

Alternatives:

- Nmap: Primarily used for network discovery and security auditing.
- Nessus: A vulnerability scanner suited for identifying weaknesses across systems.
- OWASP ZAP: An open-source web app scanner, good for beginners and automated testing.

For expert penetration testers needing a versatile arsenal, Metasploit remains indispensable due to its comprehensive exploit repository. Web security professionals benefit immensely from Burp Suite's specialized tooling. Smaller teams or those new to pentesting might find OWASP ZAP or Nessus a gentle introduction before advancing to full-fledged suites.

CLOUD SECURITY TOOLS: AWS SECURITY HUB, AZURE SENTINEL, PRISMA CLOUD

AWS SECURITY HUB

AWS Security Hub centralizes security findings across AWS services and integrated third-party tools, providing continuous compliance checks against best practices like CIS benchmarks. It suits organizations deeply invested in the AWS ecosystem seeking aggregated cloud security posture visibility with automated alerting and remediation workflows.

AZURE SENTINEL

A cloud-native SIEM and SOAR platform, Azure Sentinel integrates seamlessly with Microsoft services and beyond. Its AI-driven threat detection, investigation, and orchestration capabilities provide comprehensive hybrid and multi-cloud security monitoring. Sentinel is mission-critical for enterprises leveraging Azure and needing scalable, intelligent cloud defense.

PRISMA CLOUD (PALO ALTO NETWORKS)

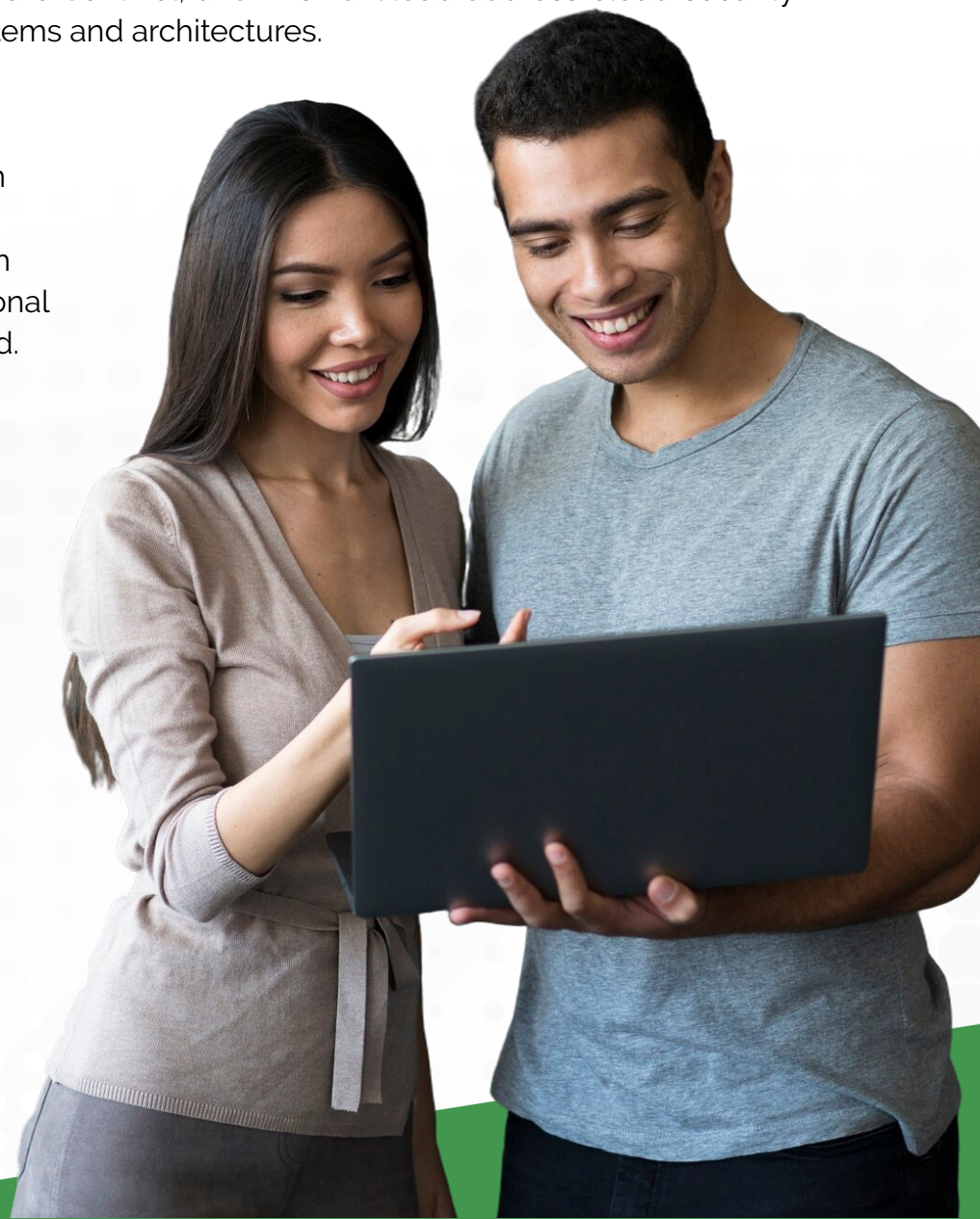
Prisma delivers extensive cloud workload protection across multi-cloud environments, covering infrastructure as code, container security, and runtime protection. It combines vulnerability management, compliance, and threat detection within a unified platform. Ideal for organizations deploying containerized and serverless architectures seeking a holistic cloud security solution.

AWS Security Hub simplifies security management for AWS-heavy shops. Azure Sentinel offers powerful, scalable SIEM capabilities especially attractive for Microsoft-centric infrastructures. Prisma Cloud's broad coverage suits organizations embracing complex, hybrid cloud-native development requiring advanced workload security.

Choosing the right cybersecurity tools is not a one-size-fits-all decision. Understanding each tool's core strengths, limitations, and best-fit scenarios ensures that your security stack aligns with organizational goals, team capabilities, and risk profiles.

- Splunk's advanced analytics empower large enterprises willing to invest in depth and scale.
- IBM QRadar and LogRhythm balance sophisticated detection with compliance focus.
- Archer, RiskRhino, and LogicGate cover the GRC spectrum from complex customization to agile automation.
- Metasploit and Burp Suite remain pen-testing mainstays, with alternatives catering to varying needs.
- AWS Security Hub, Azure Sentinel, and Prisma Cloud address cloud security across vendor ecosystems and architectures.

By evaluating these tools through this lens, security leaders and practitioners can create robust, adaptive defenses that keep pace with evolving threats and operational demands in 2025 and beyond. Embracing the right combination helps your organization stay secure, compliant, and resilient in an increasingly digital world.



6. CAREER & CERTIFICATION GUIDE

Building a fulfilling career requires clear guidance, strategic learning, and real-world inspiration. This Career & Certification Guide is designed to illuminate your pathway into cybersecurity, detailing essential roles, skills, and market realities. It also maps out a structured certification journey to help you gain credentials that truly matter. Alongside, you'll find motivating stories from Skillweed alumni who have successfully broken into the industry and a curated job board showcasing current opportunities to launch or advance your career.

PATHWAYS IN CYBERSECURITY: ROLES, SKILLS, AND SALARY EXPECTATIONS.

Here is a detailed cybersecurity career pathway for three important roles in 2025—Cybersecurity Analyst, Penetration Tester, and Cloud Security Specialist—covering necessary skills, certifications, and career progression:

1. CYBERSECURITY ANALYST PATHWAY

ROLE OVERVIEW:

Cybersecurity Analysts monitor, detect, and respond to cyber threats targeting an organization's IT infrastructure. They analyze security alerts, investigate incidents, and recommend risk mitigation strategies.

KEY SKILLS AND KNOWLEDGE AREAS:

- Understanding of networking fundamentals and protocols (TCP/IP, DNS, VPN, firewalls)
- Familiarity with security tools like SIEM (e.g., Splunk, QRadar), IDS/IPS systems, and endpoint security
- Incident response and forensic basics
- Knowledge of authentication, access control, and encryption methods
- Understanding common attack vectors (phishing, malware, insider threats)
- Strong analytical and critical thinking skills Recommended Certifications:
- Entry Level: CompTIA Security+, CompTIA Cybersecurity Analyst (CySA+)
- Intermediate Level: GIAC Security Essentials (GSEC), Cisco CCNA Security
- Advanced Level: Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM)

CAREER PROGRESSION:

- Start as SOC Analyst or Junior Cybersecurity Analyst (entry roles often through internships or help desk experience)
- Progress to Security Analyst or Threat Intelligence Analyst
- Move into specialized roles like Incident Responder, Forensics Analyst, or Security Operations Lead
- Mature into senior roles such as Security Architect, Security Manager, or CISO with gained leadership and strategic skills

$

TYPICAL SALARY RANGE:

Entry: $60,000 - $80,000 | Mid-Level: $85,000 - $110,000
Senior: $120,000+ annually

2. PENETRATION TESTER (ETHICAL HACKER) PATHWAY

ROLE OVERVIEW:

Penetration Testers simulate cyberattacks against systems, applications, and networks to identify vulnerabilities before malicious actors exploit them. They use hacking tools and methodologies ethically to strengthen security.

KEY SKILLS AND KNOWLEDGE AREAS:

- Proficiency in offensive security tools like Metasploit, Burp Suite, Nmap, and Wireshark
- Strong knowledge of web application security and OWASP Top 10 vulnerabilities
- Familiarity with network protocols and wireless systems
- Programming/scripting skills (Python, Bash, PowerShell) for automation and exploit development
- Understanding of security frameworks and compliance (e.g., PCI DSS, ISO 27001)
- Ability to write detailed vulnerability reports and remediation recommendations Recommended Certifications:
- Entry Level: EC-Council Certified Ethical Hacker (CEH), Offensive Security Certified Professional (OSCP)
- Intermediate Level: GIAC Penetration Tester (GPEN), eLearnSecurity Junior Penetration Tester (eJPT)
- Advanced Level: Offensive Security Certified Expert (OSCE), GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)

CAREER PROGRESSION:

- Begin as Junior Penetration Tester or Security Consultant
- Advance to Senior Penetration Tester or Red Team Operator
- Move into specialized roles like Application Security Engineer or Vulnerability Researcher
- Transition to Security Architect, Security Consultant, or eventually senior leadership roles

$

TYPICAL SALARY RANGE:

Entry: $65,000 - $85,000 | Mid-Level: $90,000 - $120,000
Senior: $130,000+ annually

3. CLOUD SECURITY SPECIALIST PATHWAY

ROLE OVERVIEW:

Cloud Security Specialists design, implement, and manage secure cloud architectures. They protect cloud workloads and data, ensuring compliance with organizational policies and regulations.

Key Skills and Knowledge Areas:

- Deep understanding of cloud platforms (AWS, Azure, Google Cloud) and their security models
- Expertise in cloud identity and access management (IAM), encryption, and key management
- Familiarity with cloud security tools such as AWS Security Hub, Azure Sentinel, Prisma Cloud
- Knowledge of container security, serverless architecture, and Infrastructure-as-Code (IaC) security
- Ability to conduct cloud risk assessments and compliance audits (CIS benchmarks, NIST)
- Automation skills using scripting or APIs to enforce security policies Recommended Certifications:
- Entry Level: AWS Certified Security – Specialty, Microsoft Certified: Azure Security Engineer Associate
- Intermediate Level: Certified Cloud Security Professional (CCSP), Google Professional Cloud Security Engineer
- Advanced Level: AWS Certified Advanced Networking, Certified Information Systems Security Professional (CISSP) with cloud focus

CAREER PROGRESSION:

- Start as Cloud Security Analyst or Cloud Administrator with security duties
- Progress to Cloud Security Engineer or Cloud Security Architect
- Take on roles such as Cloud Security Consultant, DevSecOps Engineer, or Cloud Risk Manager
- Advance into leadership roles like Head of Cloud Security or CISO Typical Salary Range:

$

TYPICAL SALARY RANGE:

Entry: $70,000 - $90,000 | Mid-Level: $95,000 - $130,000 | Senior: $140,000+ annually

GENERAL RECOMMENDATIONS ACROSS ROLES

- Gain hands-on experience through internships, labs, capture-the-flag (CTF) competitions, and open-source projects.
- Build a strong foundation in IT fundamentals—networking, operating systems, scripting.
- Pursue relevant certifications progressively aligned with your career stage and specialization.
- Stay updated with current threat landscapes and emerging technologies through learning platforms, industry news, and professional communities.
- Develop soft skills such as communication, teamwork, and problem-solving to complement technical expertise.

These pathways are synthesized from recent comprehensive roadmaps and industry resources and reflect the current cybersecurity market demand in 2025.

If you want, I can prepare detailed learning plans or certification schedules for each role. Sources:

- Simplilearn, "Cyber Security Roadmap and Career Path" (2025)
- IMD Blog, "8 Cybersecurity Career Paths Worth Considering in 2025" (2025)
- Webasha, "Complete Roadmap to Start a Cybersecurity Career in 2025" (2025)
- Caltech Bootcamps, "Exploring Cybersecurity Career Paths in 2025" (2025)

CERTIFICATION ROADMAP: A BEGINNER'S GUIDE TO CYBERSECURITY CREDENTIALS

WHY CERTIfiCATIONS MATTER

Cybersecurity certifications validate your knowledge, skills, and commitment to the field. They prove to employers that you meet industry standards and are equipped to handle security challenges. For newcomers, certifications provide structured learning paths and career credibility, while for professionals, they enable specialization and career advancement.

FOUNDATIONAL CERTIfiCATIONS (IDEAL FOR NEWCOMERS)

1. CompTIA Security+

   - What it is: Widely recognized as the essential starting point for cybersecurity careers.
   - Skills Covered: Basic security concepts, network security, threats and vulnerabilities, compliance, and operational security.
   - Why it matters: It builds foundational knowledge and is often a prerequisite for many entry-level jobs and further certifications.
   - Skillweed Prep: We offer comprehensive CompTIA Security+ prep classes that cover all exam objectives, hands-on labs, and practice tests to build your confidence.

2. CompTIA Cybersecurity Analyst (CySA+)

   - What it is: Builds on foundational security skills focusing on behavioral analytics to detect and combat threats.
   - Skills Covered: Threat detection, analysis, monitoring, and response using tools like SIEM systems.
   - When to pursue: After Security+ or equivalent experience, usually intermediate level.

INTERMEDIATE CERTIfiCATIONS (FOR CAREER GROWTH AND SPECIALIZATION)

3. Certified Information Systems Security Professional (CISSP)

   - What it is: A globally respected certification for experienced security practitioners, managers, and executives.
   - Skills Covered: Broad security domains including asset security, security engineering, identity and access management, security assessment, security operations, and software development security.
   - Prerequisites: At least 5 years of relevant work experience (can be waived with a college degree or certain certifications).

- Importance: Considered a gold standard credential for senior security roles and leadership.
- Preparation Tip: While CISSP requires experience, beginners can enroll in Skillweed's foundational courses to build knowledge towards this certification.

4. Certified Information Security Manager (CISM)
   - What it is: Focuses on security management and governance, ideal for those looking into security leadership and risk management roles.
   - Skills Covered: Risk management, governance, incident management, and program development.
   - Prerequisites: 5 years of relevant work experience (some waivers possible).
   - Skillweed Prep: We offer CISM prep classes that thoroughly cover domains, exam strategies, and real-world application scenarios, helping candidates pass with confidence.

5. CompTIA Advanced Security Practitioner (CASP+)
   - What it is: Designed for advanced practitioners focused on enterprise security, risk management, and integration of computing technologies.
   - Skills Covered: Cryptography, enterprise security architecture, risk management, and incident response.

SPECIALIZED AND GOVERNANCE CERTIfiCATIONS

6. Certified in Risk and Information Systems Control (CRISC)
   - What it is: Designed for IT professionals involved in risk management and control.
   - Skills Covered: Risk identification, assessment, response, and mitigation strategies; information systems control design and monitoring.
   - Skillweed Prep: We provide CRISC exam prep classes combining theoretical insights with practical exercises, ideal for candidates aiming at IT risk management roles.

7. Certified Ethical Hacker (CEH)
   - What it is: Focuses on offensive security skills, teaching ethical hacking methods and penetration testing techniques.
   - Skills Covered: Network and system penetration testing, vulnerability analysis, and ethical hacking tools.
   - Best for: Those interested in penetration testing and red teaming.

8. Certified Cloud Security Professional (CCSP)
   - What it is: For professionals securing cloud environments.
   - Skills Covered: Cloud architecture, operations, risk management, and compliance in cloud computing.
   - When to pursue: After foundational certifications and some cloud security experience.

HOW TO NAVIGATE THIS ROADMAP AS A NEWCOMER

1. Start with foundational certifications like CompTIA Security+ to gain core knowledge. Take advantage of Skillweed's beginner-friendly prep classes that offer practical labs and exam practice.
2. Gain hands-on experience through internships, labs, or entry-level roles while continuing learning.
3. Choose your career focus — whether it's technical (e.g., ethical hacking, cloud security) or managerial (risk, governance).
4. Advance to intermediate certifications such as CISSP or CISM for leadership and broad security knowledge, or CRISC for risk management roles. Skillweed's prep courses for CISM and CRISC help bridge from theory to exam readiness.
5. Continue specialization with certifications that match your job role or industry focus, supported by targeted Skillweed resources and mentorship.

WHY CHOOSE SKILLWEED'S PREP CLASSES?

- Expert-led instruction tailored to each certification's exam objectives.
- Hands-on labs and real-world scenarios for practical learning.
- Mock exams and personalized feedback to build exam confidence.
- Flexible formats that accommodate beginners and busy professionals alike.
- Supportive community and mentorship for continuous career growth.

SUMMARY

The pathway to cybersecurity certification begins with foundational knowledge and progressively builds toward advanced specialties and leadership roles. Certifications like CompTIA Security+ open doors, while CISSP, CISM, and CRISC pave the way to senior and managerial positions. Complementing your certification journey with Skillweed's targeted prep classes significantly increases your chances of success through structured learning and expert guidance.

With persistence and the right preparation, you can confidently navigate this certification roadmap and position yourself for a thriving cybersecurity career in 2025 and beyond.

7. CASE STUDIES & SUCCESS STORIES

In cybersecurity, learning from real-world experiences is invaluable. This chapter presents illustrative case studies and inspiring success stories that shine a light on how organizations and individuals confront, adapt to, and triumph over complex security challenges.

REAL-WORLD BREACH INVESTIGATIONS AND LESSONS LEARNED

Examining actual security breaches helps organizations understand attacker tactics, identify gaps, and improve defenses. This section dives into detailed investigations of notable breaches across industries to extract key lessons.

1. MASSIVE CREDENTIAL LEAK IMPACTING GOOGLE, APPLE, MICROSOFT, FACEBOOK, AND MORE

- In mid-2025, a colossal data breach exposed over 184 million login credentials across tech giants including Google, Apple, Microsoft, Facebook, Instagram, Snapchat, and several others.
- The breach involved leaked usernames, passwords, session cookies, tokens, and metadata—mostly recent credentials harvested via infostealer malware infecting user devices. Some stolen cookies allowed attackers to bypass two-factor authentication.
- Although there was no direct hack on core company systems, the leaked credentials increased the risk of account hijacking, phishing, and business email compromise across platforms.
- Lessons: Users were urged to change passwords immediately, enable multi-factor authentication, and watch for suspicious logins. Organizations were reminded of the persistent threat posed by infostealer malware targeting endpoint security gaps.

2. TELEMESSAGE DATA BREACH AFFECTING US GOVERNMENT OffiCIALS' COMMUNICATIONS

- TeleMessage, a provider of a secure archived communication app used by US government personnel, suffered a breach exposing unencrypted message data.
- Attackers accessed an AWS-hosted server within 20 minutes, obtaining message fragments, contact info, and backend admin credentials. The breach compromised the privacy of many federal users.

- TeleMessage quickly removed service documentation after the breach and is cooperating with authorities.
- Lessons: Highlights risks of misconfigured cloud environments, the importance of encryption in transit and at rest, and the need for robust access control even on archived data.

3. ORACLE CLOUD SSO AND LDAP BREACH

- In March 2025, a threat actor sold data stolen from Oracle Cloud's Single Sign-On (SSO) and LDAP systems, affecting over 140,000 tenants worldwide.
- The compromised information included Java KeyStore files, encrypted SSO passwords, and enterprise manager keys that could allow unauthorized access to cloud workloads.
- Lessons: Emphasizes criticality of securing cloud identity and access management, protecting credential stores, and monitoring cloud infrastructure for suspicious activity.

The breaches of 2025 underscore the persistent and evolving threats facing industries including tech, finance, government, healthcare, education, and IoT. Common vulnerabilities involved stolen credentials, misconfigured cloud resources, ransomware, insider access, and weak multi-factor authentication. The lessons learned emphasize the critical importance of endpoint protection, cloud security hygiene, zero trust practices, comprehensive incident response, and robust backup strategies.

Organizations must approach cybersecurity as a continuous journey, investing in detection, prevention, and resilience. Individuals and enterprises alike benefit greatly from studying these cases to anticipate emerging risks and tailor defenses accordingly.

ORGANIZATIONAL GRC TRANSFORMATIONS

Governance, Risk, and Compliance (GRC) transformations align security with business objectives, mitigate risks systematically, and enable compliance with evolving regulations. This segment highlights diverse companies who have successfully revamped their risk and compliance frameworks to improve security posture, operational efficiency, and regulatory adherence in recent years:

1. SIEMENS: INTEGRATING GRC FOR GLOBAL COMPLIANCE AND RISK MANAGEMENT

Siemens, a global technology giant operating across multiple industries and regions, embarked on a holistic GRC transformation to unify its fragmented risk and compliance processes. They implemented a centralized, technology-enabled GRC platform that consolidated vendor risk assessments, internal audits, policy management, and regulatory reporting.

Transformation Highlights:

- Automated workflows reduced manual compliance effort by 45%.
- Real-time dashboards enable executives to monitor risk exposure across hundreds of subsidiaries.
- Introduced role-based training programs to embed risk awareness throughout the global workforce.
- Streamlined reporting accelerated audit preparation and regulatory communications.

This initiative allowed Siemens to maintain consistent compliance with multinational regulations (GDPR, SOX, ISO standards) while improving transparency and decision-making agility.

2. THE COCA-COLA COMPANY: RISK-DRIVEN CULTURE AND GRC RENEWAL

Coca-Cola refreshed its GRC approach to foster a risk-aware culture while addressing emerging cyber and operational threats. They adopted a combined strategy of policy standardization, advanced risk analytics, and continuous monitoring integrated into their business processes.

Key Outcomes:

- Implemented centralized risk registers linking risks to business units and controls.
- Enabled dynamic risk scoring using AI-driven analytics enhancing risk prioritization.
- Rolled out collaborative tools for governance, compliance tasks and reporting, increasing cross-departmental visibility.
- Accelerated incident response and compliance issue resolution times through automated alerts.

This transformation empowered Coca-Cola to shift from reactive compliance towards proactive risk management at all levels.

3. ASTRAZENECA: ACCELERATING DIGITAL GRC IN PHARMA

AstraZeneca, the pharmaceutical leader, implemented a digital GRC platform to comply with stringent healthcare regulations, mitigate supply chain risks, and ensure data integrity in clinical trials.

Transformation Highlights:

- Integrated regulatory requirements from FDA, EMA, and HIPAA into unified control frameworks.
- Automated audit trails and compliance documentation cut manual efforts by 50%.
- Used predictive analytics to foresee supply chain vulnerabilities and quality risks.
- Established continuous compliance monitoring supported by mobile and cloud technology, increasing stakeholder trust.

This digital GRC shift enabled AstraZeneca to accelerate compliance cycles and reduce risk-related delays in drug development.

4. BANK OF AMERICA: TRANSFORMING GRC FOR ENTERPRISE RISK MANAGEMENT

Bank of America undertook an enterprise-wide GRC transformation to centralize risk management, improve regulatory adherence, and streamline audit processes. The bank implemented an integrated risk platform that combined credit, operational, and cyber risk management.

Key Results:

- Increased risk intelligence via consolidated risk data and analytics.
- Enhanced compliance management with automated regulatory updates and control tracking.
- Reduced audit cycle time by integrating continuous controls testing.
- Improved ability to scale governance across rapidly evolving digital operations and regulatory landscape.

This transformation supported Bank of America's strategic vision to embed risk management deeply into business decision-making.

STUDENT AND PROFESSIONAL SUCCESS STORIES

Highlighting how individuals have leveraged training, certifications, and community support to launch or advance cybersecurity careers provides real-world inspiration with relatable pathways.

SUCCESS STORY: TATIANA MABIALA MIKEMBI

Best IT Course Ever – Highly Recommended!

I am so happy, satisfied, and confident after taking this course. In the past, I spent lots of money on IT courses and training, but this CGRC is the best. You have hands- on material, and you can access it anytime and practice and see your progress. Skillweed is so organized, and you can get in touch with the instructor and his partners at all times.

I recommend this course to anyone who wants to change careers or even enhance their knowledge; every aspect of it is worthy and you won't regret it.

TESTIMONIAL: DAVID ADEBOWALE

The topic is very essential for cyber security, and I will gladly recommend it to people, it's a great one, keep it up skillweed.

SUCCESS STORY: KENNETH THOMAS BAIDOO

The GDPR internship was very insightful and refreshing. A very deep assessment of GDPR is very crucial, as it is very crucial to assess data using the CMMI maturity model.

These stories and testimonials showcase diverse journeys exemplifying dedication, targeted learning, and the critical role of support networks and structured training.

CONCLUSION

The stories captured in this chapter spotlight the realities and opportunities within today's cybersecurity landscape. Real-world breach investigations reveal evolving attacker tactics and defense priorities. Organizational GRC transformations highlight how aligning security with business drives measurable improvements and resilience. Individual success narratives emphasize that with the right guidance, practical skills, and perseverance, rewarding cybersecurity careers are within reach.

Embrace these lessons and inspirations as a roadmap to resilience and success.

8. COMMUNITY SPOTLIGHT

The strength of any cybersecurity initiative extends far beyond technology and process – it is deeply rooted in the people who drive knowledge sharing, innovation, and mutual support. The Community Spotlight chapter shines a light on outstanding member achievements, provides expert guidance through interactive Q&A, and highlights upcoming opportunities for engagement through events and competitions. Together, these elements foster a vibrant ecosystem where professionals, students, and enthusiasts grow together and advance the field.

MEMBER ACHIEVEMENTS AND CONTRIBUTIONS

ALUMNI SPOTLIGHT: PETER DIAZ LAUNCHES PCI-ASSISTANT – REVOLUTIONIZING PCI-DSS COMPLIANCE WITH AI

Skillweed Academy is home to Alums who are talented, dedicated, and innovative. Among the many inspiring successes from our alumni community, a standout achievement is the launch of PCI-Assistant, an AI-powered compliance assistant created by alumnus Peter Diaz.

If you have ever wrestled with PCI-DSS (Payment Card Industry Data Security Standard) compliance, you know the challenge all too well:

- Over 280 complex requirements hidden in dense documentation
- 509 testing procedures that are time-consuming and difficult to interpret
- The daunting task of drafting policies, controls, and evidence from scratch

Peter lived through this compliance headache firsthand and decided to build a solution that makes PCI-DSS v4.0.1 compliance 10 times faster and easier.

What PCI-Assistant Does:

- Maps and consolidates all 280+ PCI requirements and 509 testing procedures into a single, intuitive platform
- Offers AI-driven guidance to draft policies, standards, and evidence documents with ease
- Provides Self-Assessment Questionnaire (SAQ) aware views for various merchant types (D, A, P2PE, EP, B, B-IP, C, C-VT, SPoC)
- Includes embedded official PCI Council documents, eliminating the need to hunt through various sources

If you're a compliance officer, IT manager, auditor, or business owner, PCI-Assistant delivers clarity, efficiency, and confidence to navigate PCI requirements without overwhelm.

Beyond simplifying compliance, PCI-Assistant embodies the synergy between cutting-edge AI technology and practical security needs—reflecting broader industry trends where machine learning enhances risk management, compliance automation, and audit accuracy.

Peter invites compliance professionals, security leaders, and small businesses to explore PCI-Assistant and share feedback. This is just the beginning of a journey aimed at transforming PCI-DSS from a painstaking ordeal into a manageable, transparent checklist.

Discover more and try PCI-Assistant here: PCI-Assistant.com

Alumni achievements like Peter's inspire all Skillweed members, illustrating how industry experience, creativity, and technical expertise converge to solve real-world challenges. They remind us progress in cybersecurity is a collective effort—driven by empowered individuals equipped with the right knowledge and tools.

Q&A: "ASK A PRO" – EXPERT ANSWERS TO READER QUESTIONS

This interactive segment connects readers with seasoned cybersecurity experts who provide clear, actionable insights anchored in real-world experience. Here are samples from recent exchanges:

Q: "What's the best way to prepare for the CRISC exam without prior experience?"

A: Experts advise starting with a thorough understanding of the four CRISC domains—Governance, IT Risk Assessment, Risk Response and Reporting, and Information Technology and Security. Combining this with formal study materials such as the ISACA CRISC Review Manual, and enrolling in instructor-led prep courses like those offered by Skillweed, can build foundational knowledge. Hands-on involvement in risk management projects or simulations complements exam preparation. Study groups and practice exams also help reinforce concepts and exam readiness.

Q: "How can a small business implement effective cybersecurity with a limited budget?"

A: Prioritize basics such as strong multi-factor authentication, software patching, phishing awareness training, and endpoint protection. Leverage free or low-cost tools where possible and consider outsourcing to managed security service providers (MSSPs) for critical monitoring.

Q: "What emerging threats should security teams watch out for in 2026?"

A: AI-powered phishing and deepfake scams are increasing in sophistication, alongside supply chain attacks targeting software dependencies. Preparing involves enhancing detection capabilities, strengthening vendor risk assessments, and fostering an adaptive security culture.

Readers are encouraged to submit questions for upcoming editions or live expert panels, turning the Q&A section into an ongoing conversation enriching the entire community.

COMMUNITY EVENTS, WEBINARS, AND HACKATHONS

Engagement with peers through events fuels knowledge, creativity, and camaraderie. Our calendar features a diverse lineup catering to various interests and skill levels:

- Upcoming Webinars: Topics include "Zero Trust Implementation Strategies," "Effective Incident Response in Hybrid Environments," and "Leveraging AI to Enhance SOC Operations." Sessions feature industry leaders and offer Q&A segments.
- Hackathons: The second edition of the Skillweed Hackathon in Partnership with Cympire is coming up in the 3rd quarter of 2025. This simulates realistic attack and defense scenarios to sharpen skills and foster team collaboration.
- Monthly Community Events: Beyond Cybersecurity, Skillweed academy in partnership with Edgeworks Institute is set to organize webinars aimed at building soft skills for Skillweed community members.
- Workshops and Certification Bootcamps: Skillweed-led workshops and prep bootcamps support members pursuing certifications like CRISC, CompTIA

Security+, and CISM. These interactive programs combine instruction, peer collaboration, and exam techniques.

Participating in these events connects members to the pulse of cybersecurity innovation and widens professional networks crucial for career growth.

The Community Spotlight chapter celebrates the lifeblood of cybersecurity—the engaged, dedicated individuals who learn, teach, and innovate together. By partnering with peers, raising questions, and participating actively, members transform learning into action, challenge the status quo, and build resilient, informed communities prepared for what lies ahead.

9. CREATE PUZZLE

CyberSecurity Word Search

I W H I C U S E J R E F Y Z A R D E
M P X R N C Z L C N P T Z U C I E S
R E I H A S M E C N I E T D K S E N
G S T N T A I R R R A H X R I K W O
C N N A L U Y D U O E N B W V R L P
S E I W S P A C E N D H R S O H L S
R P A H T P E R T R E A I E G I I E
P R Y I S S L I O O T A Y T V N K R
E U O W D I C O D T E H N O M O S T
B N K U A A H T I A C Y R K Z N G N
H J O C T R G P P T T A M E I S U E
E L P I A G E Q D H I A F N A T T D
C X O Q U B S X E C O K B I G T P I
E N Z C O M P L I A N C E R T S U C
R A N S O M W A R E V S P F E L Q N
Y T I R U C E S K R O W T E N A U I
A J C S U R I V V B A I T P M O C M
W O U R E K C A H L A C I H T E W H
S L C N O I T A Z I R O H T U A J G
I N F R A S T R U C T U R E S I N V

Authentication
Authorization
AWS
Backup
Breach
CloudSecurity
Compliance
CompTIA
CRISC
DataBreach
Detection
Encryption
EthicalHacker
Governance
IncidentResponse
Infrastructure
InsiderThreat
IoT
Malware
Metasploit
MultiFactorAuth
NetworkSecurity
Phishing
Ransomware
RiskRhino
Scanner
SIEM
Skillweed
SOC
Spyware
Token
Virus
ZeroDay

10. MARKETPLACE & PRODUCT WATCH

The cybersecurity landscape is continuously evolving with new products, innovations, and vendor offerings designed to address ever-changing threats and operational needs.

This chapter keeps readers informed and ahead of the curve by spotlighting the latest product launches and updates, profiling trusted vendors making significant impact, and sharing exclusive special offers and discounts curated specifically for our audience.

NEW PRODUCT LAUNCHES AND UPDATES

Staying current with new product releases and significant updates to existing solutions enables organizations to adopt tools that improve protection, streamline operations, and enhance visibility. Highlights for 2025 include:

SPLUNK ENTERPRISE SECURITY 8.5

The latest version introduces enhanced AI-driven anomaly detection, improved automated response orchestration, and tighter integrations with cloud-native environments. Key updates accelerate threat detection workflows and reduce alert fatigue, making it a top choice for large-scale enterprise SIEM.

PALO ALTO NETWORKS PRISMA CLOUD 3.0

This new release expands multi-cloud workload protection, integrating AI-based anomaly detection and compliance automation across Kubernetes, serverless, and container environments. Prisma Cloud now supports more granular policy enforcement and real-time cloud posture management.

VECTRA AI COGNITO PLATFORM UPDATE

Vectra's newest update enhances automated threat hunting by adding new machine learning models for cloud and SaaS activity monitoring. The platform now integrates seamlessly with major SOAR tools, increasing response speed.

CROWDSTRIKE FALCON XDR EXPANSION

Expands endpoint detection to XDR capabilities by integrating network telemetry and cloud logs with advanced response automation for holistic threat management.

OPEN SOURCE SPOTLIGHT: ZEEK 4.0

Zeek released major protocol parsing improvements and dynamic scripting capabilities, empowering network detection teams with quicker adaptability to new threats.

VENDOR SPOTLIGHTS

Highlighting vendors who consistently innovate, deliver reliable solutions, and contribute to cybersecurity knowledge fortifies purchasing decisions. Featured vendors include:

SPLUNK

Industry leader renowned for its powerful data analytics, customizable SIEM solutions, and expansive ecosystem supporting hybrid and multi-cloud infrastructures. Splunk's continuous innovation in AI and automation maintains its cutting-edge position.

PALO ALTO NETWORKS

With a comprehensive security portfolio, Palo Alto leads in cloud-native protections and network firewalls, emphasizing integrated zero trust frameworks and advanced threat intelligence sharing.

CROWDSTRIKE

A pioneer in endpoint security and threat intelligence, CrowdStrike's cloud-native architecture delivers scalable, real-time protection enhanced by behavioral analytics and AI.

TENABLE

Focused on vulnerability management, Tenable's platform provides visibility and risk scoring across IT, OT, and cloud assets, helping organizations prioritize and remediate exposures efficiently.

SKILLWEED

Beyond product offerings, Skillweed empowers cybersecurity professionals through high-quality certification prep courses and upskilling programs designed in partnership with industry experts, blending practical skills with theoretical mastery.

SPECIAL OFFERS AND DISCOUNTS FOR READERS

To help our readers access premium cybersecurity tools and training affordably, we have secured exclusive partnerships providing special offers and discounts, including:

Readers should send an email to info@skillweed.com with the title "Special Offers" to get up to 15% off any of Skillweed's courses.

Marketplace & Product Watch serves as your essential guide to the dynamic, fast-paced world of cybersecurity solutions. By spotlighting new product innovations, trusted vendors' stories, and exclusive offers, this chapter enables readers to make smart, cost-effective technology decisions aligned with their security goals.

Being informed about the latest tools not only enhances defense capabilities but also fuels professional growth and operational excellence. We encourage readers to actively engage with showcased vendors, explore trial offerings, and leverage discounts to stay equipped for the complex threat landscape of 2025 and beyond.

11. EVENTS CALENDAR

Staying connected to the vibrant cybersecurity community and ongoing education is key to professional growth and staying ahead of emerging threats. This chapter highlights upcoming global conferences, webinars, and exclusive Skillweed events designed to sharpen skills, foster networking, and inspire innovation.

UPCOMING GLOBAL CYBERSECURITY CONFERENCES AND WEBINARS

- Cyber GRC Program – Skillweed
  - Date: November 1, 2025
  - Description: Join Skillweed's comprehensive Cyber Governance, Risk, and Compliance (GRC) program, designed to equip cybersecurity professionals with advanced skills in risk management frameworks, compliance automation, and governance best practices. This is the final session of 2025, with the next classes launching in early 2026.
  - Registration: Available on Skillweed's Website
- European Cybersecurity Hackathon 2025
  - Date: October 17–19, 2025
  - Location: CyberIsland, Budapest & Online
  - Description: Compete in a high-stakes hackathon featuring realistic cybersecurity scenarios including penetration testing, cryptography, and incident response designed for all skill levels.
  - Registration: CyberIsland Hackathon Official Site

SKILLWEED SPECIAL EVENTS

- Skillweed Cybersecurity Warrior Hackathon
  - Date: To be announced
  - Time: To be announced
  - Format: Live online event on Zoom
  - Description: Test your cybersecurity skills in a gamified environment using the Cympire Learning Platform. The event offers challenges tailored for all experience levels, from beginners to pros, with prizes and recognition.
  - Registration: www.Skillweed.com

LOOKING AHEAD: PROGRAMS TO WATCH IN 2026

- CISM Certification Prep Classes

  Scheduled for introduction in early 2026, Skillweed will launch specialized CISM exam preparation courses, blending governance and risk management training that prepare professionals for managerial-level cybersecurity roles.

- Cyber Deep Classes

  Advanced deep-dive courses covering topics such as threat intelligence, advanced penetration testing, and cloud-native security are planned to debut in 2026, targeting mid to senior-level practitioners aiming to specialize further.

This Events Calendar keeps you plugged into the pulse of global and Skillweed-hosted cybersecurity learning and competitive experiences. From foundational GRC programs to exhilarating hackathons, these events empower learners to sharpen skills, expand networks, and accelerate career trajectories.

Mark your calendars, register early, and join a community dedicated to fostering excellence and innovation in cybersecurity throughout 2025 and into the future.

12. FEEDBACK & NEXT ISSUE PREVIEW

Engaging with our readers is fundamental to building a vibrant cybersecurity community that continuously evolves and improves. This chapter invites feedback through a thoughtfully designed reader survey and feedback form, enabling you to voice your preferences, ideas, and suggestions. Transparency in hearing from you ensures each issue becomes more relevant, informative, and impactful.

Additionally, we offer a sneak peek at next issue's exciting theme and features, providing a glimpse into what you can anticipate and how to prepare for upcoming content that advances your cybersecurity knowledge and career.

READER SURVEY AND FEEDBACK FORM WHY YOUR FEEDBACK MATTERS

Your insights help us tailor content, identify emerging topics of interest, optimize format and delivery, and enhance overall reader experience. Whether you're a novice, seasoned professional, or educator, your voice shapes this publication's direction.

WHAT WE'RE ASKING

- Content Preferences: Which topics do you find most valuable? (e.g., certification guides, tool reviews, threat intelligence, career advice)
- Feature Requests: Are there specific sections, case studies, or interactive content you want more of?
- Learning Formats: What types of content do you prefer? (articles, videos, webinars, podcasts)
- Event Participation: Interest in attending or competing in upcoming webinars, workshops, or hackathons.
- General Feedback: Suggestions on how we can improve usability, accessibility, or engagement.

HOW TO PARTICIPATE

Scan the QR code at the back of this edition or visit skillwed.com/emagazinefeedback to complete the survey quickly and securely. The form uses encryption and anonymization to protect your data according to the latest privacy standards..

SNEAK PEEK: NEXT ISSUE'S THEME AND FEATURES
THEME: EMERGING TRENDS IN CYBERSECURITY FOR 2026

The next issue dives into the technologies, threats, and strategies anticipated to define cybersecurity next year and beyond. Topics include:

- AI and machine learning in threat detection and response
- The evolving zero trust framework beyond foundational adoption
- Advanced cloud security techniques and architecture changes
- Regulatory updates impacting global cybersecurity policies
- Emerging roles and skills critical for future cyber defense professionals

FEATURED SECTIONS

- Deep Dive: How AI is reshaping incident response workflows
- Certification Spotlight: Launch and insights on Skillweed's upcoming CISM prep classes
- Community Voices: Expert panels and member success stories focused on innovation
- Tool Reviews: Evaluations of new cloud security platforms and network analytics tools
- Career Corner: Strategies to pivot into cybersecurity leadership roles in 2026

SPECIAL ANNOUNCEMENTS

- Introduction of Skillweed's new Cyber Deep Classes on threat intelligence and defense tactics.
- Preview of the 2026 Skillweed Cybersecurity Warrior Hackathon focusing on cloud and AI-related challenges.

CONNECT WITH US

Stay connected, informed, and engaged—your journey is our shared mission. Follow Skillweed on social media or visit our website to receive the latest updates, exclusive content offers, event invitations, and breaks on certification prep classes. Your input drives this publication's evolution.

Website: www.skillweed.com

Subscribe to newsletters, join our WhatsApp channel, and engage with the community on forums to be part of a dynamic learning ecosystem.

Join us in shaping the future of cybersecurity education and community empowerment.

Together, we build a more informed, prepared, and resilient cybersecurity community ready to face the challenges of tomorrow.

SOURCES

Sources: Tech.SEC, World Economic Forum Global Cybersecurity Outlook 2025, Integrity360, Network Tigers, CrowdStrike 2025 Global Threat Report, Splashtop, SentinelOne, Invensis Learning, IBM, ISACA, CompTIA 2025 Reports, Cyber Magazine, "Top 12 Cybersecurity Startups to Follow in 2025", CRN, "The 10 Hottest Cybersecurity Startups of 2025", Notable Capital "Rising in Cyber 2025" list of top cybersecurity startups, Exploding Topics, "Top 20 Cybersecurity Companies & Startups to Watch in 2025", Seedtable, "69 Best Cybersecurity Startups to Watch in 2025" LoadFocus.com - Best Endpoint Protection Software of 2025, SentinelOne.com - Top 7 Endpoint Protection Products in 2025, TechRadar.com - Best endpoint protection software of 2025, Cynet.com - 10 Endpoint Security Solutions to Know in 2025, SoftwareWorld.co - Top Endpoint Protection Software 2025 Reviews, Palo Alto Networks, How to Measure Endpoint Security

Effectiveness, 2020, CrowdStrike, 2025 Gartner Critical Capabilities for EPP Report, Cynet, Endpoint Protection Platform (EPP) Security Guide, 2025, SentinelOne, 2025 Gartner Magic Quadrant for Endpoint Protection, 2025, NordLayer, SOCRadar, Gracker.AI, CYE Sec, SANS Institute, Red Canary, Coursera, Raef Meeuwisse, "Cybersecurity For Beginners", Clifford Stoll, "The Cuckoo's Egg", National Institute of Standards and Technology, NIST SP 800-207, "Zero Trust Architecture" (2020), TechTarget, CybersecurityGuide.org, EC-Council, StationX, Infosec Institute, How I Broke In: Real stories from Skillweed alumni and community members, INTERVIEW AN ALUMNI, Job Board: Curated list of current openings and internships,


SkillWeed