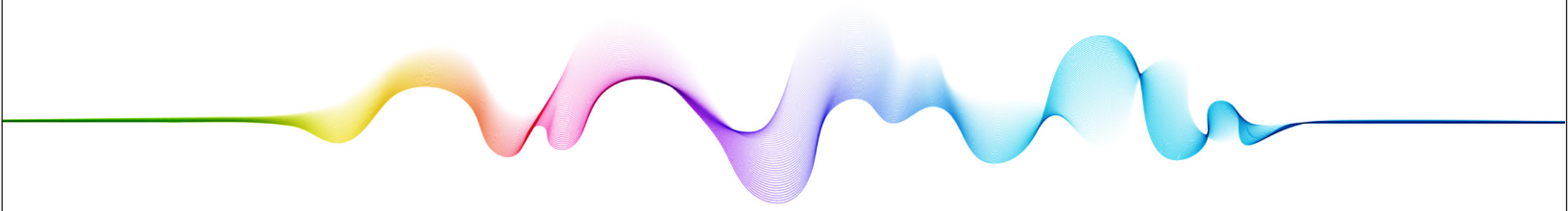
INSIGHT REPORT

OVERVIEW OF THE ATTACK SURFACE MANAGEMENT COMMERCIAL MARKET



TAG CYBERSECURITY

TAG Insights Report: Overview of the Attack Surface Management Commercial Market

Prepared by
Dr. Edward Amoroso
Chief Executive Officer, TAG Infosphere
Research Professor, NYU
eamoroso@tag-cyber.com

Version 1.0
February 10, 2024

Introduction

This TAG Insights Report on *Attack Surface Management (ASM)* is intended to help companies, managers, practitioners, researchers, investors, and commercial vendors better understand current trends, issues, and market opportunities in this area. A list of representative commercial vendors working in various areas of attack surface management is included. The five specific areas of covered in this report include:

1. Bug Bounty Services
2. External Attack Surface Management
3. Automated Pen Testing/Red Teams
4. Breach and Attack Simulation
5. Security Ratings Platforms

This report is intended for general and unrestricted use, but interested readers are encouraged to connect with the TAG research and advisory team for more information on the private TAG Research as a Service (RaaS) community that covers, discusses, and shares information on these topics in more depth and includes a wider range of startups, vendors, and companies.

TAG Taxonomy

We organize this TAG Insights Report as per our updated TAG Taxonomy which includes twenty categories of modern solution areas where stakeholders and buyers can find suitable commercial products and services for purchase and use. Each category has five subcategories

Copyright © 2024, TAG Infosphere, Inc.

that correspond to the main areas in which practitioners can focus. These subcategories are discussed below.

1 Application Security 1.1 API Security 1.2 Application Security Testing 1.3 Application Security Posture Mgmt. 1.4 Runtime Application Security 1.5 SBOM/SCA	**6 Email Security** 6.1 Anti-Phishing Tools 6.2 DMARC 6.3 Email Encryption 6.4 Phish Testing and Training 6.5 Secure Email Gateway	**11 Identity and Access Management** 11.1 Authorization 11.2 IAM Platforms 11.3 identity, Anti-Fraud, and KYC 11.4 Identity Governance and Admin. 11.5 Privileged Access Management	**16 Operational Technology Security** 16.1 ICS/OT Device Security 16.2 ICS/OT Visibility 16.3 Unidirectional Gateway 16.4 Vehicle Security 16.5 Zero Trust OT
2 Attack Surface Management 2.1 Bug Bounty Services 2.2 External Attack Surface Management 2.3 Automated Pen Testing/Red Teams 2.4 Breach and Attack Simulation 2.5 Security Ratings Platforms	**7 Encryption and PKI** 7.1 Certification Authority (CA) 7.2 Data Encryption 7.3 Key and Secret Management 7.4 Key and Certificate Protection 7.5 Post-Quantum Cryptography	**12 Security Operations and Response** 12.1 Data Forensics and eDiscovery 12.2 Incident Response 12.3 SIEM Platforms 12.4 SOC/SOAR Support 12.5 Threat Hunting	**17 Security Professional Services** 17.1 Penetration Testing 17.2 Security Assessments 17.3 Security Research and Advisory 17.4 Security Training 17.5 Value Added Resellers
3 Authentication 3.1 Biometrics 3.2 Multifactor Authentication 3.3 Passwordless Authentication 3.4 Password Management 3.5 Single Sign-On	**8 Endpoint Protection** 8.1 Antivirus Software 8.2 Browser Isolation 8.3 Content Disarm and Reconstruction 8.4 Endpoint Detection and Response 8.5 Security Enhanced Browser	**13 Managed Security Services** 13.1 DDOS Security 13.2 Managed Detection and Response 13.3 Managed Security Services Platform 13.4 Network Detection and Response 13.5 XDR Services	**18 Software Lifecycle Security** 18.1 AI/MLOps Security 18.2 Container/Kubernetes Security 18.3 Container Scanning 18.4 DevSecOps Platforms 18.5 Infrastructure-as-Code Security
4 Cloud Security 4.1 Cloud Data Fragmentation 4.2 Cloud Infrastructure Entitlement Mgmt. 4.3 Cloud Security Posture Management 4.4 Cloud Workload Protection Platform 4.5 Microsegmentation	**9 Enterprise IT Infrastructure** 9.1 Asset Inventory 9.2 Backup Platform 9.3 Infrastructure Resilience 9.4 Physical Security 9.5 Secure Sharing and Collaboration	**14 Mobility Security** 14.1 IOT Security 14.2 Mobile App Security 14.3 Mobile Device Management 14.4 Mobile Device Security 14.5 Mobility Infrastructure Security	**19 Threat and Vulnerability Management** 19.1 Digital Risk Protection 19.2 Security Scanning 19.3 Third Party Risk Management 19.4 Threat and Vulnerability Platform 19.5 Threat Intelligence
5 Data Security 5.1 Cloud Data Security Posture Mgmt. 5.2 Data Access Governance 5.3 Data Discovery and Classification 5.4 Data Leakage Protection 5.5 Data Privacy Platform	**10 Governance, Risk, and Compliance** 10.1 Continuous Compliance 10.2 Cyber Insurance 10.3 Incident Reporting 10.4 GRC Platform 10.5 Risk Management Platform	**15 Network Security** 15.1 Network Access Control 15.2 Next Generation Firewalls 15.3 Secure Access Service Edge (SSE) 15.4 Virtual Private Networks 15.5 Zero Trust Network Access	**20 Web Security** 20.1 Bot Management 20.2 Content Security 20.3 Secure Web Gateway 20.4 Web Application Firewall 20.5 Website Scanning

Figure 1. TAG Taxonomy for Cybersecurity

Overview of Attack Surface Management Solutions

The following emerging global commercial opportunities involving ASM solutions are covered in this report, including the listing of several viable commercial entities providing solutions on the market today:

- Bug Bounty programs allow organizations to crowdsource security testing by inviting external researchers to find and report vulnerabilities in their systems. These programs incentivize ethical hackers to discover and report issues, ultimately improving security. Technical teams collaborate with the reporting researchers to validate vulnerabilities and develop patches, promoting a cooperative approach to cybersecurity.
- Managing the external attack surface involves continuously monitoring all publicly accessible assets, including websites, APIs, and network infrastructure. This process employs tools and techniques such as web crawling, DNS enumeration, and port scanning. By mapping the external attack surface, organizations can identify weak points that malicious actors may exploit.
- Automated penetration testing tools simulate cyberattacks to identify vulnerabilities. These tools can be customized to mimic the tactics and techniques used by adversaries. Red teaming involves emulating attackers to assess an organization's defensive capabilities, while blue teaming focuses on monitoring and enhancing defenses. Purple

Copyright © 2024, TAG Infosphere, Inc.

teaming combines both approaches, facilitating communication and collaboration between red and blue teams to improve overall security posture.

- Breach and attack simulation (BAS) platforms emulate sophisticated cyberattacks to assess an organization's readiness and response capabilities. Teams use these simulations to identify vulnerabilities and measure the effectiveness of their detection and response mechanisms. By mimicking real-world attacks, organizations can continuously validate and fine-tune their security strategies.
- Security ratings platforms assess an organization's cybersecurity posture based on various data sources, including external attack surface analysis, breach history, and public records. These platforms provide an objective and data-driven view of an organization's security performance. Teams use these ratings to prioritize remediation efforts and gauge their security posture relative to industry benchmarks. Ratings are also commonly used in third-party risk management (TPRM) programs because the approach tends to scale well across large numbers of suppliers.

Focus Area: Bug Bounty Services

Bug Bounty services allow organizations to safely engage external security researchers, often referred to as "bug hunters" or "ethical hackers," to identify and report vulnerabilities within their software or digital infrastructure. This practice aims to improve security by leveraging the expertise of individuals who specialize in identifying and exploiting security flaws. The workflow of Bug Bounty services typically follows a structured process:

1. Scope Definition: The organization defines the scope of the bug bounty program, specifying which assets, applications, or systems are in scope for testing. This ensures that testing efforts are focused on the most critical components.
2. Engagement: Security researchers interested in participating in the bug bounty program register and agree to the program's terms and conditions. They are provided access to the designated testing environment.
3. Testing and Discovery: Researchers conduct thorough security assessments, including vulnerability scanning, code analysis, and penetration testing, within the defined scope. They aim to identify and exploit security vulnerabilities, such as code flaws, misconfigurations, or logical flaws.
4. Reporting: Researchers report identified vulnerabilities to the organization's security team or a designated point of contact. The reports typically include detailed descriptions of the vulnerabilities, proof of concept, and potential impact.
5. Verification: The organization's security team reviews the submitted reports to verify the validity of the identified vulnerabilities. They assess the impact and severity of each vulnerability based on established criteria.
6. Communication and Remediation: If a reported vulnerability is confirmed, the organization collaborates with the reporting researcher to understand the issue fully. Technical details and potential mitigations are discussed. The organization then proceeds with remediation efforts, which may include developing patches or implementing configuration changes.

Copyright © 2024, TAG Infosphere, Inc.

7. Reward Distribution: Researchers are rewarded based on a predefined monetary reward structure that considers the severity and impact of the identified vulnerabilities. Rewards are issued as a form of recognition and incentive.
8. Documentation: Throughout the process, all interactions, findings, and remediation actions are documented for future reference and compliance purposes.
9. Continuous Testing: Bug bounty programs often run continuously or periodically to ensure ongoing security assessment and vulnerability discovery as systems evolve.

Bug Bounty services provide organizations with an additional layer of security testing that complements internal security measures. They offer a proactive means of identifying and addressing security vulnerabilities, allowing organizations to enhance their cybersecurity posture while benefiting from the expertise of external security researchers.

Focus Area: External Attack Surface Management

External Attack Surface Management (EASM) is a technical approach to cybersecurity that involves monitoring and managing an organization's publicly accessible digital assets to identify potential security vulnerabilities and reduce the attack surface. EASM platforms are used to systematically track and assess the external attack surface of an organization, which includes web applications, websites, servers, APIs, DNS records, and network infrastructure. The primary goal is to gain comprehensive visibility into all exposed assets and potential entry points that could be exploited by malicious actors. Here's how EASM platforms work:

1. Asset Discovery: EASM platforms begin by scanning the internet to discover all publicly accessible assets associated with an organization. This process includes identifying IP addresses, domain names, subdomains, web applications, and open ports.
2. Enumeration and Profiling: Once assets are discovered, the platforms perform DNS enumeration and profiling. DNS enumeration identifies subdomains, while profiling provides detailed information about each asset, including technology stacks, server versions, and SSL/TLS configurations.
3. Vulnerability Scanning: EASM platforms conduct vulnerability scanning to identify known vulnerabilities associated with the discovered assets. These scans use databases of known vulnerabilities and common misconfigurations to assess the security of each asset.
4. Port Scanning: Port scanning is performed to identify open ports and services running on external assets. This helps in understanding the attack surface and potential entry points for attackers.
5. SSL/TLS Analysis: EASM platforms assess the security of SSL/TLS configurations on web assets. They check for vulnerabilities like weak ciphers, expired certificates, and misconfigurations that could lead to security breaches.
6. API Enumeration: The platforms enumerate and analyze public APIs, looking for potential security issues and vulnerabilities in the exposed API endpoints.
7. Reporting and Prioritization: After scanning and assessment, EASM platforms generate detailed reports that include a list of discovered assets, vulnerabilities, and their severity

Copyright © 2024, TAG Infosphere, Inc.

levels. These reports assist security teams in prioritizing remediation efforts based on the identified risks.
8. Integration: EASM platforms often offer integration with other security tools and workflows, enabling organizations to automate the remediation process and streamline vulnerability management.
9. Continuous Monitoring: EASM is an ongoing process. These platforms provide continuous monitoring capabilities, allowing organizations to keep track of changes in their external attack surface and respond to new threats promptly.

External Attack Surface Management platforms play a crucial role in helping organizations maintain a proactive cybersecurity posture. They offer technical capabilities to discover, assess, and monitor publicly accessible assets, helping organizations reduce the potential attack surface and mitigate security risks effectively. Artificial intelligence will certainly be an important component of this control in the future and buyers are advised to keep an eye on which vendors make the best progress in this area.

Focus Area: Automated Penetration Testing and Red/Blue/Purple Teaming

Automated penetration testing and Red/Blue/Purple teaming platforms and services are technical solutions employed in cybersecurity to assess an organization's defenses and readiness against cyber threats. They provide a complement or replacement for manual penetration testing which is limited in its ability to provide continuous validation of security – or, more likely, presence of security issues.

Automated penetration testing platforms perform systematic testing of an organization's systems, networks, and applications to identify vulnerabilities and assess their exploitability. These platforms use predefined scenarios and techniques to simulate real-world attacks. In practice, automated penetration testing involves:

1. Target Identification: The platform identifies the target systems, networks, and applications to be tested.
2. Vulnerability Scanning: Automated scans are conducted to identify known vulnerabilities, misconfigurations, and weaknesses in the target environment.
3. Exploitation: The platform attempts to exploit identified vulnerabilities to verify their severity and potential impact.
4. Reporting: A detailed report is generated, listing all identified vulnerabilities, their criticality, and potential mitigations.

Red/Blue/Purple teaming exercises assess an organization's security defenses and responses through simulated attacks and defense scenarios. The red team simulates attackers, attempting to infiltrate the organization's systems and achieve specific goals, such as data breaches or system compromises. They use advanced attack techniques to assess vulnerabilities and bypass defenses.

Copyright © 2024, TAG Infosphere, Inc.

The blue team represents the organization's defenders. They monitor the red team's activities, detect intrusion attempts, and respond to incidents in real-time. The blue team's goal is to defend against the red team's attacks effectively. Purple teaming combines both red and blue teams. The red team conducts attacks, and the blue team responds. The collaboration allows for real-time learning and improvement in the organization's security posture. In practice, Red/Blue/Purple teaming involves the following major process steps and components:

1. Scenario Definition: Teams define specific attack scenarios, objectives, and rules of engagement.
2. Attack Execution: The red team executes the defined attack scenarios, using a range of tactics, techniques, and procedures (TTPs) to test the organization's defenses.
3. Defense and Response: The blue team monitors and defends against the red team's attacks, applying incident response procedures to mitigate potential breaches.
4. Learning and Improvement: During the exercise, the teams collaborate to identify vulnerabilities and weaknesses in the organization's security posture. Lessons learned are used to improve security defenses and response procedures.
5. Reporting: A comprehensive report is generated, highlighting vulnerabilities, successful attack vectors, and recommended security enhancements.

Automated penetration testing and Red/Blue/Purple teaming platforms and services provide organizations with the technical means to evaluate their security posture, identify vulnerabilities, and enhance their defenses. These assessments help organizations proactively address security weaknesses and prepare for real-world cyber threats.

Focus Area: Breach and Attack Simulation

Breach and Attack Simulation (BAS) platforms are technical tools used in cybersecurity to simulate cyberattacks and assess an organization's readiness and response capabilities. These platforms replicate various attack scenarios to identify vulnerabilities, test detection and response mechanisms, and measure an organization's ability to defend against cyber threats. Here's how BAS platforms work:

1. Attack Scenario Definition: The BAS platform starts by defining specific attack scenarios and objectives. These scenarios are based on known attack vectors, threat intelligence, and real-world cyber threats. They may include scenarios like phishing attacks, malware infections, or lateral movement within a network.
2. Attack Simulation: The platform simulates cyberattacks by mimicking the tactics, techniques, and procedures (TTPs) commonly used by real adversaries. This involves sending simulated phishing emails, attempting to exploit known vulnerabilities, or executing malware payloads.
3. Payload Execution: In some cases, BAS platforms may execute harmless payloads to mimic the behavior of real malware without causing any actual harm. This allows organizations to observe how their systems and security controls respond to such threats.

Copyright © 2024, TAG Infosphere, Inc.

4. Monitoring and Detection: During the simulation, the platform monitors the organization's network, endpoints, and security infrastructure for signs of suspicious or malicious activity. It tracks how security measures like intrusion detection systems and antivirus software respond to the simulated threats.
5. Incident Response Evaluation: BAS platforms assess how the organization's incident response teams react to the simulated attacks. This includes measuring response times, the effectiveness of containment efforts, and communication among response teams.
6. Reporting and Analysis: After completing the simulation, the BAS platform generates comprehensive reports detailing the results of the tests. These reports highlight vulnerabilities discovered, successful attack vectors, detection rates, and the overall readiness of the organization to defend against cyber threats.
7. Remediation Guidance: BAS reports often include recommendations and guidance on mitigating vulnerabilities and improving incident response processes. This information assists organizations in prioritizing remediation efforts and enhancing their security posture.
8. Continuous Testing: BAS is not a one-time exercise. Organizations use these platforms for continuous testing and improvement of their security defenses. Regular BAS assessments help organizations stay prepared for evolving threats.

Breach and Attack Simulation platforms provide a technical means for organizations to proactively evaluate their cybersecurity readiness. By simulating various cyberattacks and assessing detection and response capabilities, these platforms help identify vulnerabilities, measure the effectiveness of security controls, and guide organizations in improving their overall cybersecurity posture.

Focus Area: Security Ratings Platforms

Security Ratings Platforms are technical tools used to assess and quantify an organization's cybersecurity posture and risk by aggregating and analyzing data from various sources. These platforms provide a quantitative measure of an organization's security performance, allowing for data-driven security assessments. Here's how Security Ratings Platforms work:

1. Data Aggregation: Security Ratings Platforms gather data from multiple sources, including public data, internet scanning, and external assessments. These sources provide information about an organization's external attack surface, historical breaches, vulnerabilities, and security practices.
2. Asset Profiling: The platform identifies and profiles an organization's digital assets, including IP addresses, domain names, subdomains, and web applications. This asset discovery process helps create a comprehensive view of the organization's attack surface.
3. Data Correlation: The platform correlates data from various sources to assess an organization's security posture. It looks for patterns and trends in the data to identify potential security risks.

Copyright © 2024, TAG Infosphere, Inc.

4. Risk Scoring: Using predefined algorithms and risk models, Security Ratings Platforms assign quantitative security scores to organizations. These scores reflect the level of risk associated with the organization's digital assets and security practices.
5. Vulnerability Assessment: The platforms analyze data related to vulnerabilities, misconfigurations, and security weaknesses. They consider factors such as the severity of vulnerabilities and their potential impact on the organization's security score.
6. Historical Breach Data: Security Ratings Platforms review historical breach data to assess an organization's past security incidents and their impact. This information contributes to the overall risk assessment.
7. Security Practices Evaluation: The platforms assess an organization's security practices, such as the use of encryption, secure certificate management, and adherence to security best practices.
8. Benchmarking: Security Ratings Platforms often provide benchmarking capabilities, allowing organizations to compare their security scores to industry peers or established benchmarks. This helps organizations gauge their security posture relative to their peers.
9. Reporting and Remediation: The platforms generate detailed reports that highlight vulnerabilities, weaknesses, and recommended remediation actions. These reports enable organizations to prioritize security improvements effectively.
10. Continuous Monitoring: Security Ratings Platforms offer continuous monitoring of an organization's security posture, allowing for real-time assessment and adaptation to emerging threats and vulnerabilities.

Security Ratings Platforms provide organizations with a quantitative assessment of their cybersecurity posture and risk. By aggregating and analyzing data from various sources, these platforms offer a data-driven approach to security assessment, helping organizations identify vulnerabilities, prioritize remediation efforts, and improve their overall security practices.

Companies and Contributions

The companies listed below emerged as part of our research at TAG. Our goal in listing these fine firms is to provide a starting point for buyers, advocates, stakeholders, and researchers trying to make sense of the commercial landscape for attack surface management as a means for driving toward a more secure global ecosystem.

Bug Bounty Services Vendors

1. Bugcrowd: Bugcrowd offers crowdsourced security testing and vulnerability disclosure programs for companies.
2. FireBounty: FireBounty is a bug bounty platform that connects researchers with companies looking for security testing.
3. HackerOne: HackerOne connects organizations with a global community of ethical hackers to identify and remediate security vulnerabilities.
4. Intigriti: Intigriti is a European crowdsourced security platform for ethical hacking and bug bounty programs.

Copyright © 2024, TAG Infosphere, Inc.

5. Open Bug Bounty: Open Bug Bounty is a nonprofit platform that enables security researchers to responsibly report vulnerabilities.
6. Synack: Synack provides a platform that combines human intelligence and machine learning for security testing and bug hunting.
7. Vulnerability Lab: Vulnerability Lab offers security research and responsible disclosure services for businesses.
8. YesWeHack: YesWeHack is a European bug bounty platform that connects organizations with ethical hackers.
9. Zerocopter: Zerocopter provides a platform for continuous security testing, monitoring, and bug bounty programs.

External Attack Surface Management (EASM) Vendors

1. Balbix: Balbix uses deep learning and other specialized AI algorithms to continuously analyze your attack surface and business context and produce relevant insights
2. BinaryEdge: BinaryEdge offers external attack surface monitoring and threat intelligence services.
3. BishopFox: Achieve real-time visibility with continuous mapping of your entire external perimeter with their Cosmos platform.
4. Bitsight: Stay on top of your exposure and solve immediate problems so only the people you want in your inner circle access your data.
5. BreachLock: BreachLock's platform, allows customers to automate security assessments and measure their attack surface.
6. Bugcrowd: Bugcrowd Attack Surface Management matches the efforts of attackers with the ingenuity and impact of trust attack-minded defenders for an assessment of risk.
7. Census: Census Cyber Threat Intel Services provides data on the external attack surface of the internet.
8. Censys: Censys provides a platform for discovering and managing a company's external assets and vulnerabilities.
9. CloudFlare: Cloudflare unifies security everywhere across the Internet, employees, and corporate network, so you can accelerate growth.
10. Coalfire: the Hexeon platform combines manual and automated testing services to present a holistic picture of your perimeter and network as well as recommendations to harden each part.
11. CybelAngel: CybelAngel provides digital risk protection services, including monitoring of the external attack surface.
12. CyCognito: CyCognito offers an EASM platform that helps organizations discover and managed their external attack surface.
13. Foretifydata: Fortify ASM has capabilities to discover and inventory external assets, internal networks, cloud services and third party external attack surface.
14. GreyNoise: GreyNoise is a threat intelligence platform that helps organizations filter out noise and focus on relevant external threats.
15. IBM: Randori Security Recon monitors external attack surfaces for unexpected changes.

Copyright © 2024, TAG Infosphere, Inc.

16. ImmuniWeb: Illuminate your entire external attack surface with ImmuniWeb® Discovery attack surface management just by entering your company name
17. Intel 471: Intel 471's Attack Surface Protection is a suite of three solutions that enable you to visualize your organization's management of its attack surface and see yourself as an attacker would.
18. Ivanti: With the RiskSense platform, achieve end-to-end comprehensive oversight of vulnerability exposure tracking and remediation validation.
19. JupiterOne: View and monitor all your assets. 200+ security and IT integrations. Devices, users, servers, apps, and more.
20. Microsoft: Microsoft's Defender Threat Intelligence (Acquisition of Risk IQ) is a threat investigation platform that includes external attack surface monitoring capabilities.
21. Palo Alto Networks: Palo Alto's acquisition of Expanse Cortex offers a platform for external attack surface management, providing visibility into internet-connected assets.
22. Pentera: Pentera offers an EASM platform, enabling customers to automate security ass essments and continuously measure their attack surface.
23. Scans.io: Scans.io, hosted by Stanford Internet Research, is a repository of internet-wi de scan data, useful for understanding the external attack surface.
24. SecurityTrails: SecurityTrails offers an API-driven platform for external attack surface reconnaissance and asset management.
25. Shodan: Shodan is a search engine that scans and indexes devices and services on the i nternet, helping organizations manage their external attack surface.
26. Telos: Telos Ghost®, a cloud-based virtual obfuscation network as-a-service, enables organizations to hide their most critical assets, data, devices, and personnel from adversaries.
27. Tenable: Tenable Attack Surface Management (formerly Tenable.asm) continuously maps the entire internet and discovers connections to your internet-facing assets.
28. UpGuard: UpGuard helps organizations discover and assess their external attack surface and cyber risk.
29. Vicarius: Vicarius provides a platform for vulnerability prioritization and patch management for an organization's external attack surface.
30. Zercurity: (Recently acquired by Jumpcloud) Zercurity provides asset discovery and management for external attack surface monitoring.

Automated Penetration Testing and Red/Blue/Purple Teaming Vendors

1. AttackForge: AttackForge is a platform for managing and automating the entire security testing lifecycle.
2. AttackIQ: AttackIQ offers a platform for continuous automated penetration testing and security validation.
3. Breachlock: Breachlock offers managed penetration testing services
4. Cyberbit: Cyberbit provides cybersecurity training and simulation solutions, including purple teaming.
5. Cymulate: Cymulate offers a SaaS-based platform for continuous security validation through automated red and blue teaming.

Copyright © 2024, TAG Infosphere, Inc.

6. NopSec: NopSec provides vulnerability risk management and remediation solutions, including red and blue teaming.
7. Pentera: Pentera offers a cloud-based attack simulation platform, enabling customers to automate security assessments and continuously measure their attack surface.
8. Qualys: Qualys offers an attack surface management solution that includes red and blue teaming capabilities.
9. Randori: Now a part of and a product service for IBM, Randori offers an automated platform that supports penetration testing and red/blue team engagements.
10. Rapid7: Rapid7 provides a variety of cybersecurity solutions, including automated penetration testing and purple teaming.
11. SafeBreach: SafeBreach provides a popular platform for simulating and testing security breaches.
12. SCYTHE: SCYTHE offers an advanced platform for continuous red teaming and breach simulation.
13. XM Cyber: XM Cyber offers a platform for automated red teaming and simulation of advanced threats.

Breach and Attack Simulation (BAS) Vendors

1. AttackForge: AttackForge offers a breach and attack simulation management and reporting platform that helps manage projects, reduce vulnerability remediation times and increases go-to-market speed.
2. AttackIQ: AttackIQ offers a platform for continuous automated penetration testing and security validation, including breach simulation.
3. Cyberbit: Cyberbit provides cybersecurity training and simulation solutions, including breach and attack simulation.
4. Cycognito: CyCognito provides uses a SaaS-based global bot network to use attack methods that identify assets and define an enterprise attack surface.
5. Cymulate: Cymulate offers a SaaS-based platform for continuous security validation, including breach and attack simulation.
6. Guardicore: Guardicore (part of Akamai) offers a breach and attack simulation platform to help organizations assess and improve their security posture.
7. Picus Security: Picus Security provides a breach and attack simulation platform for continuous security validation.
8. Rapid7: Rapid7 provides a variety of cybersecurity solutions, including breach and attack simulation.
9. SafeBreach: SafeBreach offers an advanced platform for simulating and testing security breaches.
10. SCYLLA: SCYLLA provides an AI-powered platform for automating breach and attack simulation exercises.
11. SCYTHE: SCYTHE offers a platform for continuous breach and attack simulation and red teaming.
12. Trellix: provides a platform for security validation and automated breach simulation.

Copyright © 2024, TAG Infosphere, Inc.

13. XM Cyber: XM Cyber offers a platform for automated breach and attack simulation, testing security posture against advanced threats.

Security Ratings Platforms Vendors

1. BitSight: BitSight offers a security ratings platform that assesses the cybersecurity posture of organizations and their vendors.
2. FortifyData: FortifyData provides automated threat assessments resulting in a quantification of cyber risk.
3. Panorays: Panorays offers a security ratings platform for assessing and managing third-party vendor risk.
4. Prevalent: Prevalent provides solutions for third-party risk management and vendor assessment.
5. ProcessUnity: (Formerly CyberGRX) ProcessUnity offers a platform for managing and assessing third-party cyber risk.
6. riskrecon: riskrecon (by Mastercard), offers a platform for assessing and monitoring the security posture of third-party vendors.
7. SecurityScorecard: SecurityScorecard provides cybersecurity ratings and risk assessment services for organizations.
8. UpGuard: UpGuard provides a security ratings platform that assesses and monitors cybersecurity risk.

About TAG

TAG is a trusted next generation research and advisory company that utilizes an AI-powered SaaS platform to deliver on-demand insights, guidance, and recommendations in cybersecurity, artificial intelligence, and sustainability to enterprise teams, government agencies, and commercial vendors.

Copyright © 2024 TAG Infosphere, Inc. This report may not be reproduced, distributed, or shared without TAG Infosphere's written permission. The material in this report is comprised of the opinions of the TAG Infosphere analysts and is not to be interpreted as consisting of factual assertions. All warranties regarding the correctness, usefulness, accuracy, or completeness of this report are disclaimed herein.