Hype Cycle for Security Operations, 2023

Published 20 July 2023 - ID G00787018 - 91 min read

By Analyst(s): Jonathan Nunez, Andrew Davies

Initiatives: Security Operations

Security operations technologies and services defend IT/OT systems, cloud workloads, applications and other digital assets from attack by identifying threats and vulnerability exposures. Security and risk management leaders can use this research to strategize and deliver SecOps capability and functions.

More on This Topic

This is part of an in-depth collection of research. See the collection:

- 2023 Hype Cycles: Deglobalization, AI at the Cusp and Operational Sustainability

Analysis

What You Need to Know

Hybrid and remote work practices have matured rapidly, and security operations center (SOC) teams have evolved to support these transformations. The resulting expansion of attack surfaces has prompted organizations to become more agile and responsive in their approach to cyber defense, often taking on additional projects to bolster maturity. To keep up with the changing landscape, security and risk management (SRM) leaders must develop strategies centered on business risk instead of just adopting new ways to do the same things better.

The Hype Cycle

Security operations (SecOps) must find ways to adapt. To do so, SRM leaders should adopt an exposure-based approach to operations, promoting business relevance. As a primary function, SecOps is responsible for maintaining visibility across technology estates for the purposes of monitoring and responding to potential threat activity, and actively advising and reducing risk through careful orchestration of controls. To achieve its goals, it's equipped with technologies and services aimed at providing deep visibility of technology networks, assisting with diagnostic outcomes and, in some cases, control implementation.

However, even with previous advancements made in data science and analytical interventions, these tools and services have led to an inundation of data, disparity in tooling, and ultimately end users managing the complexities of triage and analysis across a multitude of platforms. While many of these capabilities champion increased visibility, they also highlight the need for a more unified approach that is centered on better prioritization for faster, risk-based outcomes.

Some key capability areas SRM leaders must include in their roadmap are:

- Implementing continuous threat exposure management (CTEM) concepts.
- Applying a business-relevant approach to improve the breadth and relevance of detection and response.
- Maximizing automation for the reduction of response times.
- Leveraging generative cybersecurity AI for operational efficiency gains and skill augmentation.

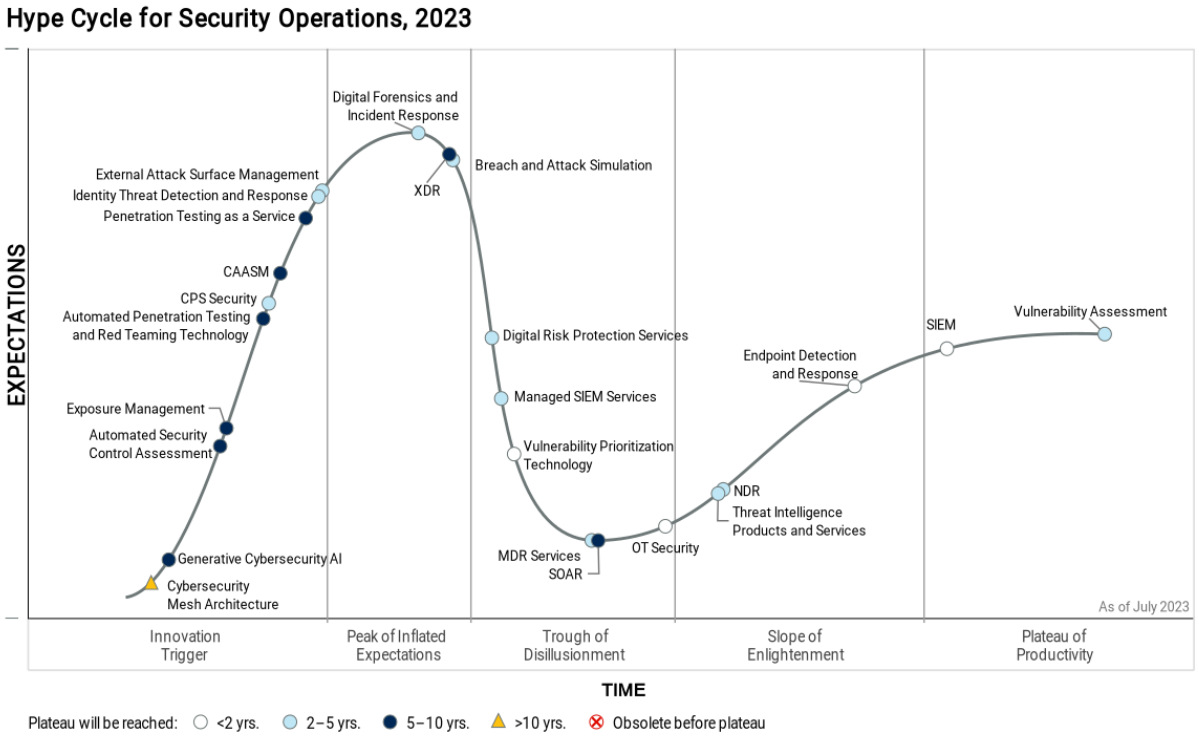
The complexity and volume of attacks directed at increasingly exposed technologies is echoed in this year's Hype Cycle, namely, by the technologies which have made the most significant movements: MDR, exposure management, external attack surface management (EASM), cyber asset attack surface management (CAASM), identity threat detection and response (ITDR), and XDR. These symbolize the increasing demand to know more, prioritize better, and act faster in proportion to the threat landscape and organizational risk.

An increasing number of technologies at the Innovation Trigger signify the demand to overcome attack surface complexities. Numerous categories continue to evolve, namely, exposure management, EASM, CAASM, penetration testing as a service (PTaaS), automated penetration testing and red teaming tools, automated security controls assessment (ASCA) and ITDR. These tools and services, in part, represent the need to continuously discover, assess, prioritize, validate and reduce exposure across digital estates.

At peak market interest are capabilities such as breach attack simulation (BAS) and digital risk protection services (DRPS), which aim to deliver continuous risk assessment and threat identification from within the estate and externally. Also at the peak are XDR and digital forensics and incident response (DFIR), signifying the demand for enhanced threat detection and response readiness.

Generative cybersecurity AI also emerges in the Hype Cycle with the potential to improve automated workflows, proxy existing analytics, generate security configurations and assemble realistic attack data. There are clear use cases, but mostly announcements and experimental features today, some of which are already tested for threat detection and response, threat intelligence, and even across the competencies of exposure management. SRM leaders looking to implement this technology should consider how their organization will consume or build such capabilities, and employ a mechanism to police its utilization.

Figure 1: Hype Cycle for Security Operations, 2023



The Priority Matrix

Organizations that evaluate the risks across the business before investing in any security operations service and capability will be more easily able to identify what to purchase and how much to spend. This will allow them to get the best risk reduction and respond effectively to issues that may be damaging to productivity, the brand, or both.

Technologies and services that align to security operations rarely provide immediate benefits. Such capabilities should be considered consumable. In other words, they require a process to fit in to become effective. Security risk should be managed in line with organizational priorities, but firmly anchored in addressing your specific organization's threat landscape.

When considering the technology and capability roadmap for security operations, you need to significantly focus on the prioritization of discovered issues to ensure that your security operations program aligns to your specific and dynamic attack surface. Concurrently, this all needs to align with modern IT architectures.

Adding complexity is neither of high priority, nor of high benefit. Long-term initiatives in areas such as CSMA adoption and exposure management are ways to model processes and the use of current technology, rather than using an entirely new tool. Security operations professionals must weigh up those strategic items that have a greater chance of effective and measurable positive impact on the risk profile of the business.

Table 1: Priority Matrix for Security Operations, 2023

(Enlarged table in Appendix)

Benefit	Years to Mainstream Adoption			
↓	Less Than 2 Years ↓	2 - 5 Years ↓	5 - 10 Years ↓	More Than 10 Years ↓
Transformational			Exposure Management Generative Cybersecurity AI	Cybersecurity Mesh Architecture
High	Endpoint Detection and Response OT Security Vulnerability Prioritization Technology	Breach and Attack Simulation CPS Security Identity Threat Detection and Response MDR Services Threat Intelligence Products and Services Vulnerability Assessment	SOAR XDR	
Moderate	SIEM	Digital Forensics and Incident Response Digital Risk Protection Services External Attack Surface Management Managed SIEM Services NDR	Automated Penetration Testing and Red Teaming Technology Automated Security Control Assessment CAASM Penetration Testing as a Service	
Low				

Source: Gartner (July 2023)

Off the Hype Cycle

This year, the Hype Cycle for Security Operations saw the retirement of one innovation, cloud access security broker (CASB). It has been ultimately consolidated into the security services edge (SSE) primarily due to its integration with secure web gateways (SWG) and zero trust network architectures (ZTNA), which are part of SSE.

On the Rise

Cybersecurity Mesh Architecture

Analysis By: Pete Shoard, Patrick Hevesi

Benefit Rating: Transformational

Market Penetration: Less than 1% of target audience

Maturity: Embryonic

Definition:

Cybersecurity mesh architecture (CSMA) is an emerging approach for architecting composable, distributed security controls that improve overall security effectiveness. It offers an approach to enabling secure, centralized security operations and oversight that emphasizes composable, independent security monitoring, predictive analytics and proactive enforcement, centralized intelligence and governance, and a common identity fabric.

Why This Is Important

CSMA aims to address the growing complexity of managing security tools, intelligence and identity solutions. Organizations must begin evolving toward a radically more flexible security architecture to prevent the impact of fast-emerging, evolving and retiring security tool categories and attack types. Planning to invest in composable, compatible and extensible security toolsets is essential to reduce cost and increase consistency.

Business Impact

CSMA offers a potential solution to problems currently suffered by defense-in-depth security architectures that most organizations employ. These are often made up of multiple point solutions that are poorly interconnected. CSMA addresses many challenges, including centralized exposure and security posture management, threat awareness, coordinated detection methodology and use cases, harmonized threat reporting and proactive response, and an increase in the efficiency of cross-tool collaboration.

Drivers

- Organizations increasingly require a broader perspective on the impact and likelihood of a threat or an exposure to a threat; it is this detail that is crucial in making better probusiness security decisions.

- IT security organizations can be overwhelmed when trying to stay ahead of new and more complex attacks, and when deploying the latest security tools to ever-expanding infrastructure. Teams are not able to implement the analytical capability required to be proactive and dynamic regarding their security enforcement and response decisions.
- Furthermore, these decisions are rarely fast enough to meet business needs.
- Effective security and identity management requires a layered and collaborative approach, but today's solutions are instead siloes that operate with insufficient knowledge of other tools and leave gaps. These silos are time-consuming to operate and monitor.
- Organizations understand and acknowledge the skills gaps and challenges in volumes of work, but do not have clear solutions to deal with these issues.
- Organizations are frustrated by the lack of integration and consistent visibility within their current security workbenches. Security and risk management leaders require an architecture that not only reacts to the current security issues (those that are visible in the organization), but provides a coordinated and holistic approach to complex security problems.
- Creating a collaborative ecosystem of security tools will address inconsistency and help understand and minimize the exposure that is consistent with business expectations.

Obstacles

- As CSMA emerges and vendors add support for the architecture principles to their products, vendor lock-in will likely be a concern. If a proprietary approach is employed, it may serve to block, rather than facilitate, cross-tool integration; then gaps in coverage will likely appear, and this inflexibility will drive up cost.
- Those organizations that choose to create their own CSMA construct will likely need significant engineering effort to integrate disparate products and may suffer if the security industry moves toward a set of standards for interoperability after significant custom integration work has been completed.
- Currently, there are no vendors that offer what might be described as a CSMA solution. Features and requirements of the reference architecture continue to evolve in response to consumer IT advancement and security technology consolidation as a result of vendor acquisitions and partnerships.

User Recommendations

- Position your organization for a future of rapid change. Add purchasing requirements that focus on integration and interoperability of multivendor tools.
- Mature your security infrastructure by selecting point product vendors that are aligning to the CSMA reference architecture, have fully developed advanced APIs, complete adherence to modern security standards and have integrations into security partner networks.
- Evolve your identity infrastructure to an identity fabric by removing silos to achieve dynamic real-time identity capabilities that incorporate a more complete set of context and risk signals (such as device proximity, posture, biometrics and location).
- Improve your responsiveness by centralizing your policy, posture and playbook management along with building an integrated “single starting pane of glass” view into your CSMA.

Gartner Recommended Reading

The Future of Security Architecture: Cybersecurity Mesh Architecture (CSMA)

How to Start Building a Cybersecurity Mesh Architecture

2023 Planning Guide for Security

Emerging Technology Horizon for Information Security, 2022

Automated Security Control Assessment

Analysis By: Evgeny Mirolyubov, Jeremy D'Hoinne

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

ASCA processes and technologies focus on the analysis and remediation of misconfigurations in security controls (e.g., endpoint protection, network firewall, identity, email security, and security information and event management), which improves enterprise security posture. ASCA can be a stand-alone tool or a capability of other security products, such as firewalls, identity threat detection and response, network security policy management, and cloud infrastructure entitlement management.

Why This Is Important

Automated security control assessment (ASCA) technologies reduce an organization's attack surface caused by security configuration drift, poor defaults, exessive tuning to reduce false positive rates, and high administration staff turnover. ASCA improves the security posture by verifying the proper, consistent configuration of security controls, rather than simply verifying the existence of controls.

Business Impact

Organizations implementing ASCA processes and technologies enhance staff efficiency, minimize the impact of human errors and improve resilience in the face of organizational churn. ASCA reduces security control configuration gaps that unnecessarily expose the organization to otherwise preventable attacks.

Drivers

- The volume of misconfigurations in security controls continues to grow with the increased complexity of environments, emerging threat vectors, the proliferation of new security tools and the high turnover of administration staff, leading to a more exposed attack surface.
- Specific organizational use cases and objectives require the preservation of complex heterogeneous infrastructure and security architectures, instead of pursuing simplification through vendor consolidation.
- The optimization of configurations of enterprise security controls cannot rely exclusively on manual periodic configuration reviews; siloed, tool-centric approaches; or occasional penetration tests.
- Continuously assessing and remediating security controls configurations in accordance with the highest-risk exposures is an effective risk mitigation strategy, ultimately reducing the attack surface.

Obstacles

- Lack of support for niche vendor and security control assessments makes ASCA tools less valuable for large, complex organizations with specialized point solutions.
- Overlaps with existing tools and vendors that are looking to accomplish similar goals in individual silos, such as tools for network firewall or cloud configuration assessments.
- The slow pace of remediation, paired with continuous assessments, may cause findings to pile up without proper automation and a triage process that considers business context.
- Lack of mature processes to optimize security controls configurations end to end.
- Budget increases to invest in people, technologies and, possibly, managed services needed to respond to an accelerated list of configuration issues discovered by ASCA tools.

User Recommendations

- Reduce complexity by pursuing security vendor consolidation or considering alternatives, such as “policy as code” to manage security configurations.
- Establish processes to evaluate enterprise security controls, including planning, assessing, remediating and validating expected configurations.
- Evaluate incumbent security providers for ASCA capabilities, including continuous configuration monitoring and alerting about the impact of configuration changes on security protection, operations and productivity.
- Assess ASCA providers’ capabilities, including the breadth of coverage for your enterprise security controls, cross-control configuration analysis quality and integration of input from cybersecurity validation tools, such as BAS and VA.

Sample Vendors

Absolute Software; CardinalOps; Veriti; XM Cyber

Generative Cybersecurity AI

Analysis By: Jeremy D'Hoinne, Avivah Litan, Mark Horvath, Wilco van Ginkel

Benefit Rating: Transformational

Market Penetration: Less than 1% of target audience

Maturity: Embryonic

Definition:

Generative cybersecurity AI technologies generate new derived versions of security-related and other relevant content, strategies, designs and methods by learning from large repositories of original source data. Generative cybersecurity AI can be delivered as a public or privately hosted cloud service or embedded with security management interfaces. It can also integrate with software agents to take action.

Why This Is Important

Enterprises witness many applications leveraging foundation models that can read multimodal objects (such as sensory data and images), following the first applications based on large language models (LLMs).

Cybersecurity technology providers can exploit generative cybersecurity AI to improve existing workflows, be a proxy of existing analytics, and generate security configuration or realistic attack data. Soon, applications will include autonomous agents, which can work using high-level guidance without a need for frequent prompting.

Business Impact

Existing vendors and new startups will add generative cybersecurity AI, expanding or replacing features. They will start implementing it with resource-intensive tasks, such as incident response, exposure or risk management, or code analysis.

Organizations will benefit from generative cybersecurity AI as it can improve efficiency and shorten response times to cybersecurity risks and threats. The pace of adoption will vary across industries and geographies due to security and privacy concerns.

Drivers

- ChatGPT is one of the most hyped and fastest-adopted AI technologies ever. It relies on generative AI foundation models, which are largely trained on massive internet datasets.
- Security operations center (SOC) teams cannot keep up with the deluge of security alerts they must constantly review, and are missing key threat indicators in the data.
- Risk analysts need to speed up risk assessments, and be more agile and adaptable through increased automation and prepopulation of risk data in context.
- Organizations continue to experience skill shortages and look for opportunities to automate resource-intensive cybersecurity tasks. Use cases for the application of generative AI include: synthesizing and analyzing threat intelligence; generating remediation suggestions for application security, cloud misconfigurations and configuration changes to adjust to threats; generating scripts and codes generation; implementing secure code agents; identifying and graphing key security events in logging systems; conducting risk and compliance identification and analysis; automating the first steps in incident response; tuning of security configuration adjustment; creating general best practice guidance.
- Generative cybersecurity AI augments existing continuous threat exposure management (CTEM) programs by better aggregating, analyzing and prioritizing inputs. It also generates realistic scenarios for validation.
- Generative AI offerings include the ability to fine-tune models, develop applications using prompt engineering and integrate with prepackaged tools and plugins through APIs. These possibilities open up a path for providers to add generative cybersecurity AI.
- Microsoft has already demonstrated a preview version of its security co-pilot feature, which is expected to drive competitors to embed similar approaches.
- Security program performance solutions and activities can solve their increasing demand for business alignment. Further, they can perform scenario planning for budget (re)allocation, and efficiency and effectiveness indicators and corrections.

Obstacles

- The cybersecurity industry is already plagued with false positives. Early examples of “hallucinations” and inaccurate responses will cause organizations to be cautious about adoption or limit the scope of their usage.
- Best practices and tooling to implement responsible AI, privacy, trust, security and safety for generative AI applications do not fully exist yet.
- Privacy and intellectual property concerns could prevent sharing and usage of business- and threat-related data, reducing the accuracy of generative cybersecurity AI outputs.
- As generative AI is still emerging, establishing the trust required for its wider adoption will take time. This is especially true for the skill augmentation use cases, as you would need the skills you are supposed to augment, in order to ensure the recommendations are good.
- Uncertainty on laws and regulations related to generative AI may slow down adoption in some industries, for example regulated industries in EU countries subject to GDPR compliance.

User Recommendations

- Pick initial use cases carefully. First implementations might have a higher error rate than more mature techniques already in place.
- Monitor the addition of generative AI features from your existing providers and beware of “generative AI washing.” Don’t pay a premium before obtaining measurable results.
- Choose fine-tuned models that align with the relevant security use case or fine-tune in-house models from base models offered by the providers.
- Refrain from sharing sensitive and confidential data with hosted models until verifiable privacy assurances are provided by the host.
- Apply AI security frameworks, such as AI TRiSM. Work with your legal team on data privacy and copyright issues.
- Implement a documented approval workflow for allowing new generative cybersecurity AI experiments.
- Make it mandatory from a policy standpoint that any content (that is, configuration or code) generated by an AI is fully documented, peer-reviewed by humans and tested before it is implemented. If not possible, consider any AI-generated content as “Draft Only” when used for critical use cases.

Gartner Recommended Reading

4 Ways Generative AI Will Impact CISOs and Their Teams

Innovation Insight for Generative AI

Market Guide for AI Trust, Risk and Security Management

Exposure Management

Analysis By: Pete Shoard, Mitchell Schneider, Jeremy D'Hoinne

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Exposure management (EM) encompasses a set of processes and technologies that allow enterprises to continually and consistently evaluate the visibility, and validate the accessibility and vulnerability of an enterprise's digital assets. EM is governed by an effective continuous threat exposure management (CTEM) program.

Why This Is Important

EM reduces the challenges organizations face inventorying, prioritizing and validating threat exposure that exist due to a rapidly expanding attack surface where traditional vulnerability management isn't enough. The volume of effort required and the diversity of potential issues lead to conflicting priorities and "dashboard fatigue." SRM leaders struggle to prioritize risk reduction actions, leaving gaps where they feel they have less control, such as SaaS platforms and social media.

Business Impact

Exposure management governs and prioritizes risk reduction for the modern enterprise and requires assessments of all systems, applications and subscriptions used.

- Likelihood of exploitation (visibility of the organizations attack surface).
- Inventory and prioritize (vulnerability, threat intel-based, digital assets).
- Validate the potential success of any attack and if security controls can assist with detecting or preventing them.
- CTEM is a program, not the outcome of a specific tool.

Drivers

- Most commonly, organizations are siloing exposure activities such as penetration testing, threat intelligence management and vulnerability scanning. These siloed views provide little or no awareness of the complete situation regarding the effective risks the organization has.
- The volume of discovered vulnerabilities and issues that testing surfaces continues to grow with the complexity of environments, the increased volumes of applications used and the increased use of cloud services.
- Lack of scope and understanding of prioritization and risk, in line with high volumes of findings is leaving organizations with far too much to do regarding their exposure and little guidance on what to action first.
- A programmatic and repeatable approach to answer the question “how exposed are we?” is necessary for organizations. This must have the aim of allowing reprioritisation of priority as environments change in a rapidly changeable IT landscape.
- Organizations must reorient their priorities, and segregate these priorities into three distinct questions: “what does my organization look like from an attacker’s point of view?,” “what configuration has my organization set that will make it vulnerable to attack?”; “how would our defensive controls cope and how would response processes perform?”

Obstacles

- The increased scope of CTEM programs over traditional VM introduces a number of new complexities often not previously considered or budgeted for.
- The concept of evaluating your attack surface is well-understood, continued security tool consolidation in this space, such as EASM with VA is beginning to simplify day-to-day operational processes, but formal integration of other technologies such as CAASM and CSPM technologies is still low.
- Processes to manage end-to-end awareness (from visibility of possible attack vectors to response to breaches) is virtually nonexistent in most organizations who often simply scan and test their networks for compliance reasons.
- The complex way an attack may manifest itself requires certain skill sets to understand, new markets such as BAS make it more simple to test the out-of-the-box scenarios. But to be more effective at using these technologies/services and develop custom-made simulations, new skills and understanding are required.

User Recommendations

- Embrace broader CTEM programs as security and risk management professionals, rather than simply processing vulnerabilities with VA tools.
- Mobilize various organizational stakeholders as success is dependent on it. Automated remediation from tools is unlikely to have a significant impact.
- Focus on visibility, end users must have an awareness of where risks are, and plan to respond to threats even if the organization has no way to reduce exposure to them.
- Prepare response and reaction plans. Monitoring and responding to issues and risks identified as a critical part of managing exposure, validating that exposures exist and controls are functioning is useful, but it is essential that organizations also prepare to react.
- Be sure to include assets that your organization doesn't directly own, such as social media accounts, SaaS applications and data held by supply chain partners, in your exposure management program.

Gartner Recommended Reading

Innovation Insight for Attack Surface Management

Implement a Continuous Threat Exposure Management (CTEM) Program

Predicts 2023: Enterprises Must Expand From Threat to Exposure Management

Top Trends in Cybersecurity 2023

Automated Penetration Testing and Red Teaming Technology

Analysis By: Mitchell Schneider, Jonathan Nunez, Jeremy D'Hoinne

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

The automation of penetration testing (pentesting) and red teaming activities has traditionally been difficult to commoditize. It is limited to a number of use cases and heavily based on custom tools from the teams operating the activity. Recent progress promises greater automation of full-spectrum cybersecurity validation activities.

Why This Is Important

Pentesting and red teaming engagements play an important role in an organization's ability to validate its exposure and attack surface. Many organizations only test when obligated by compliance requirements, on an annual, biannual or ad hoc basis. Increased automation leads to more frequent and reliable assessments, reducing the associated dwell time and creating efficiency and a more measurable outcome. It also augments the ability of red teams to focus on more advanced use cases.

Business Impact

- Frequent and consistent testing helps find and mitigate weaknesses, gaps and operational deficiencies not found by other security tools, in addition to reducing downtime and loss of revenue.
- Automated pentesting will not fully replace independent testing, but can reduce external costs and avoid paying expensive services only to discover "low-hanging" fruits.
- Continuous validation will help tune threat detection technologies and test response procedures, ensuring maximal breach readiness.

Drivers

- Forward-thinking organizations want to exceed compliance requirements and continuously validate their security posture.
- Security operations teams are looking for more automation in running attack scenarios, improved control of red team “stealthiness” and a reduction in operational execution risks when executing cybersecurity validation activities.
- Red teaming is still the purview of mature organizations that are prepared to benefit from these activities to validate and test technical and operational defenses.
- Human-led red teaming programs are difficult to initiate because they require a specific set of expertise, processes and tools that can be expensive to develop or procure. Adding automation to the red team’s toolkit can help initiate such a program.

Obstacles

- Adoption is low and there is limited feedback from buyers to validate the efficacy and value of these solutions.
- Acceptance of test results from automated pentesting and red teaming tools by auditors, assessors and third-party risk teams is rare — especially organizations in highly regulated industries. Organizations using automated testing solutions should confirm whether test results would be acceptable to applicable parties.
- Managing automated pentesting and red teaming solutions, along with consuming the output and taking follow-up actions, requires human effort and defined skill sets. Determining scope, gathering the necessary information (e.g., IP address ranges or excluded assets), configuring parameters of a test and monitoring the execution of the test until completion are rarely automatable.
- Current tools cannot address all variations of penetration tests that buyers may require, especially those that require people to be on site, like wireless and physical intrusion tests.

User Recommendations

- Perform proofs of concept (POCs) and other due diligence to confirm that the solutions being considered are fit for purpose and will meet the buyer's requirements. This is because the market is nascent and there is limited end-user experience with these tools.
- Ensure that the tools will be considered equivalent to the activities performed, and findings and results provided, by testing services providers. It is important in case you are planning to use these tools to address any audit or regulatory compliance requirements.
- Create relationships with vendors in this space to help them refine and improve their solutions, identify and prioritize new features and functionality, and drive more custom requirements to become a standard part of their solutions.

Sample Vendors

FireCompass; Horizon3.ai; IBM (Randori); Pentera; Prancer; Ridge Security; SCYTHE; Vonahi Security

CPS Security

Analysis By: Katell Thielemann

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Cyber-physical systems (CPS) are engineered systems that orchestrate sensing, computation, control, networking and analytics to interact with the physical world (including humans). They are created as physical assets become connected to each other or enterprise IT systems, and as drones and robots are deployed. CPS security is the overall discipline to ensure that CPS remain safe, reliable and resilient in the face of growing threats.

Why This Is Important

CPS includes the industrial control systems (ICS)/supervisory control and data acquisition (SCADA), operational technology (OT), Internet of Things (IoT), and industrial IoT umbrellas. This includes everything from utilities, smart cities and grids, to autonomous vehicles and smart manufacturing. They connect physical processes with digital technology, and underpin all critical infrastructure. CPS are increasingly targeted by attackers through stealing data, demanding ransom or derailing production.

Business Impact

Unlike IT systems that create, store, transact or transform data, CPS connect both the cyber and the physical worlds. They are usually deployed in production or mission-critical environments, which means that CPS security efforts need to focus on human safety and operational resilience, above and beyond traditional data-centric security efforts. These efforts need to consider all cybersecurity best practices, as well as laws of physics and industry-specific engineering decisions.

Drivers

- Focusing on CPS security is a pressing need due to rapidly increasing initiatives from governments and companies alike, in domains such as smart cities, utilities, healthcare, food, agriculture, public safety, and transportation.
- As risks extend to the physical world, concerns over physical perimeter breaches, USB insertion, controller area network (CAN) bus injections, GPS jamming, hacking, spoofing, tampering, command intrusion, or malware implanted in physical assets, also need to be addressed above and beyond cybersecurity.
- The last few years have seen a marked increase in attacks in enterprise IT systems, impact operations, and production environments in manufacturing and critical infrastructure. Because these areas are where value is usually created or essential services for societies are performed, CPS will continue to be targeted.
- The consequences of a successful attack on CPS go beyond cybersecurity-centric data loss to include operational shutdowns, environmental impacts, damage and destruction of property and equipment, and even personal and public safety risks.
- The generic OT security market has evolved into specific CPS security categories, such as protection platforms, cyber risk quantification platforms, unidirectional data flow solutions, secure remote access solutions, content disarm and reconstruction solutions, security services, network-centric solutions (e.g., cloaking, microsegmentation), onboard diagnostics solutions, embedded systems security, and supply chain security solutions.

Obstacles

- CPS are often deployed by business units without consultation with the security team.
- Most organizations still focus mainly on IT-security-centric risk management.
- The lack of collaboration across siloed teams running systems such as IT, OT and IoT, hamper CPS security efforts that require cross-functional collaboration.
- Many organizations do not have structured security programs or skills that sufficiently cover the scope of CPS, especially for those high-value/mission-critical assets.
- Because of standards in CPS products that guide security design and usage are still evolving, many manufacturers value “speed to market” over “secure to market”.
- Many devices lack storage and compute power to facilitate security mechanisms.
- The omnipresence of CPS devices in buildings, cities, homes and vehicles means that traditional security methods may not be scalable to address the risks in devices, areas or the entire value chain.

User Recommendations

- Prioritize security controls and “secure by design” practices in new procurements, such as for drones and robots.
- Discover all connected assets, whether born out of IT/OT connectivity or new IoT/industrial IoT/smart “X” programs.
- Evaluate which CPS assets are high-value or mission-critical, identify specific CPS security controls already in place, and determine whether any gaps need to be prioritized based on potential organizational impact.
- Create an investment plan to update security and risk management strategies and programs in relation to CPS, starting with those high-value and mission-critical assets.
- Engage functional business leaders to establish clear risk ownership and define domain-specific controls for CPS, to balance between growing the business and improving security.
- Evaluate the growing list of CPS security solutions, as there are more options than ever before.

Sample Vendors

Armis Security; Claroty; Dragos; Microsoft; Nozomi Networks

Gartner Recommended Reading

3 Initial Steps to Address Unsecure Cyber-Physical Systems

Predicts 2023: Cyber-Physical Systems Security — Beyond Asset Discovery

CPS Security Governance — Best Practices From the Front Lines

Innovation Insight for Cyber-Physical Systems Protection Platforms

CAASM

Analysis By: John Watts, Mitchell Schneider, Neil MacDonald

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Cyber asset attack surface management (CAASM) is focused on enabling security teams to overcome asset visibility and exposure challenges. It enables organizations to see all assets (internal and external), primarily through API integrations with existing tools, query consolidated data, identify the scope of vulnerabilities and gaps in security controls, and remediate issues.

Why This Is Important

CAASM aggregates asset visibility from other products that collect a subset of assets, such as endpoints, servers and devices. By consolidating internal and external cyberassets, users can query to find coverage gaps and misconfigurations for security tools such as vulnerability assessment and endpoint detection and response (EDR) tools. CAASM provides mostly passive data collection via API integrations, replacing time-consuming manual processes to collect and reconcile asset information.

Business Impact

CAASM enables security teams to improve basic security hygiene by finding security controls gaps, security posture, and asset exposures across all digital assets. Organizations that deploy CAASM reduce dependencies on homegrown systems and manual collection processes, and remediate gaps either manually or via automated workflows. Organizations visualize security tool coverage, support attack surface management (ASM) processes, and correct systems of record that may have stale or missing data.

Drivers

- Full visibility into any asset owned by the organization collected through existing tools to improve the understanding of an organization's potential attack surface and existing security control gaps.
- Quicker audit compliance reporting through more accurate, current, and comprehensive asset and security control reports.
- Consolidation of existing products that collect asset and exposure information into a single normalized view, to reduce operational overhead of manual processes and dependencies on homegrown applications.
- Access to consolidated asset views for multiple individuals and teams across an organization and integrations with other systems of record for current state visibility.
- Lower resistance to data collection from, and better security visibility into, "shadow IT" organizations, installed third-party systems and line-of-business applications over which the IT department lacks governance and control. Security teams need visibility in these places, whereas the IT department may not.
- Help IT teams improve the accuracy of their existing CMDB through periodic updates of assets and attributes missed by CMDB reconciliation processes.

Obstacles

- Resistance to “yet another” tool — there are increasing overlaps with CAASM vendors and adjacent tools that provide some asset inventory and reporting.
- Not all vendors have capabilities to identify and integrate with every required system for visibility and vulnerability information.
- Vendor response actions to prioritized issues may be limited to opening tickets or invoking a script.
- Products licensed per asset consumed become cost-prohibitive for very large organizations.
- The scalability of a single instance may be limited for extremely large environments, in terms of both data collection and usability.
- Tools that can be integrated with a CAASM product either do not exist (due, for example, to the lack of an API) or may be prevented from integrating by the teams that own them.
- Reconciliation processes that conflict with source systems may not be resolved easily within CAASM vendor tooling.

User Recommendations

- Take advantage of proof-of-concept opportunities, and free versions of products and subscriptions, in order to “try before you buy,” as CAASM products are nondisruptive and easy to deploy.
- Given the immaturity of the market, sign no more than a one year contract.
- Favor vendors that can combine inside-out and outside-in asset visibility capabilities or partner with EASM providers.
- Favor vendors that understand all asset types beyond traditional asset categories such as granular software assets, users, and IoT/OT systems to extend to more use cases.
- Inventory all available APIs that can be integrated with the CAASM product you are considering, and ensure you have read-only or low-privilege user accounts available to integrate.
- Ask your incumbent security vendors if they have a roadmap to provide CAASM functionality in future.

Sample Vendors

Armis; Axonius; Brinqa; Encore; JupiterOne; Noetic Cyber; Northstar.io; Ordr; Panaseer; Sevco Security

Gartner Recommended Reading

Innovation Insight for Attack Surface Management

Implement a Continuous Threat Exposure Management (CTEM) Program

Competitive Landscape: External Attack Surface Management

Emerging Tech: Security — The Future of Attack Surface Management Supports Exposure Management

Penetration Testing as a Service

Analysis By: Mitchell Schneider, Jeremy D'Hoinne, Carlos De Sola Caraballo, William Dupre

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Penetration testing as a service (PTaaS) provides technology-led, point-in-time and continuous application and infrastructure testing aligned with penetration testing (pentesting) standards, which have traditionally relied heavily on human pentesters using commercial/proprietary tools. The service is delivered via a SaaS platform, leveraging a hybrid approach of automation and human pentesters (crowdsourced or vendors' in-house team) to increase the efficiency and effectiveness of the results.

Why This Is Important

Pentesting is foundational in a security program and mandated by various compliance standards (e.g., PCI). PTaaS delivers a platform that enables faster scheduling and execution of pentests, and real-time communications with testers and visibility of test results. It provides API access to enable integration with existing DevOps and ticketing solutions for workflow automation. It also provides the ability to document and track pentesting results to demonstrate progress over time to leadership/auditors.

Business Impact

PTaaS complements vulnerability scanning and application security testing, and provides cost-optimization and quality improvement of pentesting output and validation of vulnerability status. PTaaS enables organizations to elevate their security posture through continual assessment. It integrates validation earlier in the software development life cycle compared with traditional pentesting phases by giving access to real-time findings delivered through the platform, therefore enabling faster reduction of exposure.

Drivers

- Organizations are turning to PTaaS to deal with the increase of attack surfaces due to accelerating use of public cloud and expansion of public-facing digital assets. PTaaS allows developers to talk to and receive guidance from pentesters instead of arguing with scanners, such as dynamic application security testing/static application security testing (DAST/SAST) scanners.
- Organizations with limited in-house security expertise must meet their compliance and risk management objectives, in addition to improving their security posture, and therefore look to pentesting services to meet these initiatives.
- In order to meet fast production deadlines, security-aware organizations must integrate a more agile way of conducting pentesting into their continuous integration/continuous delivery (CI/CD) pipelines for their DevSecOps practices.
- Gartner clients have expressed an appetite to test on a more frequent basis; however, manual pentesting is cost-prohibitive in modern infrastructure (e.g., IaaS, SaaS and third-party subscriptions).

Obstacles

- Selecting a suitable PTaaS vendor in the market will be difficult, as their capabilities vary. Vendors use one or a combination of automation and human testers, which are in-house or community-led — typically vetted freelancers — to perform penetration testing for the client organization.
- Most of the PTaaS vendors in the market focus on the internet-facing digital assets, like web and mobile applications, which may only partially fulfill client requirements.
- There is confusion between PTaaS and bug bounty programs, as many bug bounty vendors also now offer PTaaS.
- Heavily regulated industries may still be required to contract a third party to perform a traditional, consulting type of pentest due to compliance requirements; therefore, PTaaS may not be an acceptable alternative.

User Recommendations

- Determine which option/mix of penetration testing programs is best for your organization: compliance-driven service engagement; PTaaS; in-house red team leveraging an automated pentesting tool; or bug bounty.
- Identify and evaluate the pentesting scope and requirements that PTaaS vendors will be able to fulfill before engaging with vendors. PTaaS is well-aligned to both application testing and external infrastructure testing. Not all of the vendors will be able to replace internal infrastructure pentests, wireless, social engineering and physical assessments.
- Favor hybrid scanning models that combine human analysis and automation to increase both effectiveness and efficiency.
- Select a PTaaS vendor that aligns with relevant compliance requirements, and not just focused on internet-facing infrastructure and applications.
- Seek PTaaS vendors that provide customized and tailored guidance throughout the life cycle of their service to alleviate the security skills gap.

Sample Vendors

Bishop Fox; BreachLock; Bugcrowd; Cobalt Labs; Evolve Security; HackerOne; NetSPI; OccamSec; Raxis; Synack

Gartner Recommended Reading

How to Select a Penetration Testing Provider

Understand the Types, Scope and Objectives of Penetration Testing

External Attack Surface Management

Analysis By: Ruggero Contu, Elizabeth Kim, Mitchell Schneider, Franz Hinner

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

External attack surface management (EASM) refers to the processes, technology and managed services deployed to discover internet-facing enterprise assets and systems and associated exposures. Examples include exposed servers, public cloud service misconfigurations and third-party partner software code vulnerabilities that could be exploited by adversaries.

Why This Is Important

Digital transformation initiatives have accelerated the expansion of enterprises' external attack surfaces. Cloud adoption, remote/hybrid working and IT/OT/IoT convergence are some key changes increasing exposure to external threats. EASM helps identify internet-facing assets while also prioritizing discovered vulnerabilities and related threats. It aims to provide risk information relevant to digital assets in the public domain, exposed to threat actors.

Business Impact

EASM provides valuable risk context and actionable information to SRM leaders. EASM delivers visibility through five primary capabilities:

- Asset discovery/inventory for external-facing assets and systems.
- Monitoring for internet-facing enterprise exposures (cloud services, IPs, domains, certificates and IoT devices).
- Analysis to assess and prioritize the risks and vulnerabilities discovered.
- Indirect remediation, mitigation and incident response through prebuilt integrations with ticketing systems and SOAR tools.

Drivers

- Interest in understanding what organizations are exposed to from an attacker's point of view.
- Digital business initiatives such as cloud adoption, application development, hybrid working and IT/OT/IoT convergence present new enterprise risks.
- Demand to quantify third-party risks arising from activities such as merger and acquisition (M&A) and integration of supply chain infrastructure.
- EASM's adoption across different security platforms, offering EASM capabilities as part of a broader solution set to support better actionability.

Obstacles

- Low-value perception, with EASM leveraged for single-use cases rather than multiple areas.
- Confusion with the availability of EASM as a feature from various platforms, such as DRPS and VA.
- Already overburdened vulnerability management (VM) capabilities and teams concerned about adding to workloads.

User Recommendations

- Review available EASM capabilities arising from converging markets, in areas such as threat intelligence (TI), security testing/validation, vulnerability assessment or providers with broader platforms, such as Palo Alto Networks and Microsoft. You may have an existing commercial relationship in place with a provider, and its functionalities may be good enough.
- Review providers' capabilities such as breadth of coverage (discovery), accuracy, prioritization efficacy and level of automation in supporting remediation activities as they vary considerably from vendor to vendor.
- Select an EASM technology or service provider based on the recognized use-case priority, but also plan for longer-term requirements potentially stretching into DRPS, TI, threat hunting and/or security testing/validation use cases.
- Ensure your EASM investment fits into the larger ASM strategy where external and internal exposure management is combined together.
- Consider EASM a key capability if primary business revenue is driven by externally facing web services.

Sample Vendors

Bishop Fox; Censys; CrowdStrike; CyCognito; FireCompass Technologies; IBM; Palo Alto Networks; Pentera; SOCRadar; ZeroFox

Gartner Recommended Reading

Market Guide for Security Threat Intelligence Products and Services

Emerging Tech: Security — The Future of Attack Surface Management Supports Exposure Management

Competitive Landscape: External Attack Surface Management

Quick Answer: What Is the Difference Between EASM, DRPS and SRS?

Innovation Insight for Attack Surface Management

Identity Threat Detection and Response

Analysis By: Mary Ruddy

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Identity threat detection and response (ITDR) is a discipline that includes tools and best practices that protect identity infrastructure itself from attacks. ITDR can block and detect threats, confirm administrator posture, respond to various types of attacks and restore normal operation as needed.

Why This Is Important

Identity is foundational for security operations (identity-first security). Only authorized end users, devices and services should have access to your systems. As identity becomes more important, threat actors are increasingly targeting the identity infrastructure itself. Organizations must focus more on protecting their IAM infrastructure. ITDR adds an additional layer of security to identity and access management (IAM) and cybersecurity deployments.

Business Impact

Securing your identity infrastructure is mission-critical for security operations. If your accounts are compromised, permissions set incorrectly or your identity infrastructure itself is compromised, attackers can take control of your systems. Protecting your identity infrastructure must be a top priority. “Business-as-usual” processes that seemed adequate before attackers began targeting identity tools directly are no longer sufficient.

Drivers

More sophisticated attackers are actively targeting the IAM infrastructure itself. For instance:

- Administrator credential misuse is now a primary vector for attacks against the identity infrastructure.
- Attackers can use administrative permissions to gain access to the organization’s global administrator account or trusted Security Assertion Markup Language (SAML) token signing certificate to forge SAML tokens for lateral movement.

- Modern attacks have shown that conventional identity hygiene is not enough. There is no such thing as perfect prevention. Multifactor authentication and entitlement management processes can be circumvented, and these tools generally lack mechanisms for detection and response if something goes wrong.
- ITDR is needed in addition to IGA, PAM, a security information and event management (SIEM) solution and an in-house security operations center (SOC) or outsourced managed detection solution. There are major detection gaps between IAM and infrastructure security controls. IAM is traditionally used as a preventive control, whereas infrastructure security is used broadly but has limited depth when detecting identity-specific threats. ITDR mechanisms are more specific and operate with lower latency than general purpose configuration management, detection and response systems.

Obstacles

- ITDR requires coordination between IAM and security teams, which some organizations find difficult to establish.
- Lack of awareness of IAM administrator hygiene, detection and response best practices means that many organizations are not adequately protecting their identity infrastructure. More is needed than just traditional AD TDR.
- IAM teams often spend too much effort protecting other group's digital assets and not enough protecting their own IAM infrastructure.
- Multiple capabilities are required to fully protect identity infrastructure, including more closely monitoring configuration changes to root IAM administrator accounts, detecting when identity tools are compromised, enabling rapid investigations and efficient remediation and the ability to quickly revert to a known good state.
- The "R" part of ITDR is still nascent. Automated responses are still relatively basic.
- Even though there are many different ITDR capabilities, specific vendors provide only some of them.

User Recommendations

- Include ITDR strategy in your formal IAM program. ITDR requires a sponsor who can identify stakeholders and spearhead this collaborative initiative.
- Prioritize securing identity infrastructure with tools to monitor identity attack techniques; protect identity and access controls; detect when attacks are occurring; and enable fast remediation.
- Use the MITRE ATT&CK framework to correlate ITDR techniques with attack scenarios to ensure that at least well-known attack vectors are addressed.
- Combine foundational IAM infrastructure hygiene, such as PAM and IGA, with ITDR. Manage security posture and configuration of user directories and token generators. This will help to achieve identity fabric immunity.
- Prevent administrator accounts from being compromised (e.g., by forcing proper termination of RDP sessions).
- Modernize IAM infrastructure using current and emerging standards (e.g., OAuth 2.0, CAEP).

Sample Vendors

Authomize; CrowdStrike; Gurucul; Microsoft; Netwrix; Oort; Proofpoint (Illusive); Semperis; SentinelOne (Attivo Networks); Silverfort

Gartner Recommended Reading

Top Trends in Cybersecurity 2022

Implement IAM Best Practices for Your Active Directory

At the Peak

Digital Forensics and Incident Response

Analysis By: Eric Ahlm, Mitchell Schneider, Craig Lawson, Andrew Davies

Benefit Rating: Moderate

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Digital forensics and incident response (DFIR) is offered as a multifaceted service that enables clients to respond to a potential security breach. DFIR services can offer postbreach assistance for incident response (IR) in evaluating a security incident, and a service that enables structure planning and training in the creation of security playbooks for IR.

Why This Is Important

DFIR services are a strategic investment to strengthen an organization's incident response capabilities, both proactively and reactively. Advanced attacks, such as ransomware, require specialized skills in investigation, negotiation, forensics and response. For most organizations, having highly specialized experts on payroll for limited usage doesn't make sense. DFIR providers can help augment response capabilities through contracted services.

Business Impact

DFIR services are increasingly critical to an organization's strategic IR plan. Improper handling of response postbreach can lead to extended impacts and losses. Regulatory fines, legal fees, lawsuits, brand devaluation and customer attrition can all be affected by how a breach is handled. Having a robust DFIR capability in place will elevate the response capabilities of the organization, allowing for proportional responses aligned to avoid real impacts.

Drivers

- The increased risk of cyberattacks against organizations has reflected the need to invest in a DFIR provider to react, remediate and recover the business infrastructure.

- DFIR has had a strong increase in popularity within North America, EMEA and the Asia/Pacific region. This highlights the strategic importance of DFIR, but also the value attributed to the brand and reputation of an organization.
- Businesses want rapid response to incidents with a highly detailed investigation and accuracy so that they will be able to minimize the impact of a breach — reducing any downtime and meeting any regulatory or insurance-driven needs.
- DFIR providers offer the expertise required to help organizations recover from security incidents quickly. They provide guidance on security control reconfiguration and granular details regarding the true impact of a breach, without the overhead of directly attracting, compensating and retaining specialist staff.
- Certain clients need assistance in the chain of custody. This is a process that proves that evidence used to prosecute a cybercriminal is legitimate and not edited fraudulently. Most DFIR suppliers can help deliver this if requested, while some even provide litigation support.
- Cyberinsurance carriers often require clients to engage with a DFIR provider to reduce the risk, and thus the cost, to the insurance company. Insurance companies may offer reduced premiums if their preferred DFIR provider is used.

Obstacles

- DFIR vendors have different approaches to providing response and forensics capabilities. Vendors can use a combination of human and technology approaches and identify which approach best suits the needs of the buyer.
- Understanding the DFIR roles and responsibilities when responding to incidents is critical to the success of the program. Organizations must understand what constitutes a call out and what does not.
- The buyer must understand the engagement with the DFIR supplier on a retainer, a zero-hour retainer or a pay-for-retention contract, which is usually assigned against the buyer's organization.
- A DFIR contact won't solve the problem of the internal cross-team collaboration required for response. Business decisions about an incident, as well as internal coordination of the response, can be an obstacle.

User Recommendations

- Evaluate purchasing a prepaid IR retainer if the budget allows this. DFIR buying options can be confusing. Prepurchasing retainers can maximize investment, and increase priority and access to services to support your DFIR requirements in case of an incident.
- Evaluate the DFIR services for breach planning and avoidance services in addition to postbreach response services. The best option is always to avoid a breach if possible.
- Involve your DFIR provider in your cybersecurity maturity. This can enhance an organization's other security investments. DFIR providers' business deals with breaches. The lessons learned from breaches can enhance your cybersecurity defense with more-sophisticated use cases, threat detection and even playbooks.
- An agreement with a DFIR provider is not a replacement for the buying organization having its own incident response process in place.

Sample Vendors

Accenture; BlueVoyant; Booz Allen Hamilton; CrowdStrike; Deloitte; IBM; Mandiant; NCC Group; PwC; Verizon

Gartner Recommended Reading

Market Guide for Digital Forensics and Incident Response Retainer Services

Breach and Attack Simulation

Analysis By: Jeremy D'Hoinne, Eric Ahlm, Mitchell Schneider, Pete Shoard

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

Breach and attack simulation (BAS) technologies allow enterprises to gain better visibility on their security posture weak spots by automating the continuous testing of threat vectors such as lateral movement and data exfiltration. BAS complements, but cannot fully replace, red teaming or penetration testing. BAS validates the security posture of organizations by testing its ability to detect a portfolio of simulated attacks run from SaaS platforms, software agents and virtual machines.

Why This Is Important

The key advantage of BAS technology is to provide automated and consistent assessment of an enterprise's threat vectors. Many BAS products have innovated to include external attack surface capabilities to maintain an up-to-date assessment list, and cover more of the attack kill chain. Frequent automated BAS assessments also enable organizations to detect gaps in their security posture due to configuration errors, or reevaluate priorities of upcoming security investments.

Business Impact

BAS allows organizations to validate the impact of what attack surface assessments and security posture management tools indicate as potential exposure to a specific threat. Organizations can continuously execute these assessments to gain more frequent visibility on a larger percentage of their assets. They can evaluate the efficacy of their security controls and discover attack paths leading to their most critical assets, allowing them to prioritize remediation.

Drivers

BAS is relevant for multiple exposure validation use cases, including, but not limited to:

- Threat exposure confirmation: Organizations with establishing cybersecurity validation programs use BAS technology primarily to ensure consistent, yet improved, security posture over time and across multiple locations.
- Security control validation: BAS tools might integrate with security control technologies, through management APIs or by reading alert logs, enabling security configuration management and improving the visibility of defense gaps.
- Compliance optimization: BAS provides "safer" and more automated assessments that organizations value to prepare for mandatory penetration testing, or to refocus red team activity on more advanced scenarios.

IT and business stakeholders often sponsor deployment of BAS technologies as they perceive it as a safer way to assess the competency of current security controls, their configuration and the incident response processes for the organization. BAS also supports continuous threat exposure management (CTEM) programs by enabling deeper automation of the “validation” step.

Obstacles

- Only higher maturity organizations are successfully implementing an exposure management initiative, or try to go beyond what the minimal compliance requirements are.
- BAS vendors need extensive internal sponsorship, not only from the security team, but from other infrastructure teams, such as networks or applications. Issues that BAS tools discover create complex remediation pathways.
- BAS tools need to expand beyond the diagnostic and basic remediation guidance through standard frameworks.
- The skill set required to deploy, maintain and operate a BAS tool is extensive and includes technical competences; threat actor and technique understanding as well as infrastructure and application architecture insights.
- BAS technology suffers from increased competition with more adjacent tools adding attack simulation, and need to expand and cover more environments, such as cloud infrastructure and SaaS.

User Recommendations

- Prioritize your company's use case(s) and then assess the BAS vendors' capabilities to deliver value continually by regularly adding new capabilities, such as EASM, but also highlighting changes in the security posture and providing reports in a form that minimizes diagnostic fatigue.
- Integrate BAS in a cybersecurity validation roadmap, as part of a continuous threat exposure management (CTEM) program. Don't run BAS in isolation.
- Evaluate the number of threat vectors and attack scenarios BAS tools can deliver and the frequency to which these simulations are updated to reflect real-world attacks.
- Understand the benefits and challenges resulting from the deployment options for BAS technologies. BAS products might leverage software agents, virtual machines and SaaS components.
- Work with your auditors to determine whether BAS technology can be used to validate the efficacy of existing security controls.
- Ensure that the results delivered by the BAS products are actionable.

Sample Vendors

AttackIQ; Cymulate; Google; Keysight; Pentera; Picus Security; Ridge Security; SafeBreach; SCYTHE

Gartner Recommended Reading

Quick Answer: What Are the Top and Niche Use Cases for Breach and Attack Simulation Technology?

Implement a Continuous Threat Exposure Management (CTEM) Program

Top Trends in Cybersecurity 2023

Using Security Testing to Grow and Evolve Your Security Operations

XDR

Analysis By: Eric Ahlm, Thomas Lintemuth, Franz Hinner

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Extended detection and response (XDR) delivers unified security incident detection and automated response capabilities. XDRs integrate threat intelligence and telemetry data from multiple sources, with security analytics to provide contextualization and correlation of security alerts. XDR must include native sensors. XDR can be delivered on-premises or as a SaaS offering, and is typically deployed by organizations with smaller security teams.

Why This Is Important

XDR offers a less complex approach for threat detection and response by using a systematic, rather than an integration, approach to building a detection stack. XDR vendors can include a variety of security controls, usually natively integrated by the vendor via APIs. The vendor provides prebuilt playbooks that enable collaboration in their stack, and coherence in the detection of common threats.

Business Impact

The simplicity of XDR to detect common threats reduces the need for internal skill sets and could reduce the staff needed to operate a more complex solution, such as security information and event management (SIEM). XDR can also help reduce the time and complexity associated with security operations tasks through a single centralized investigation and response system.

Drivers

- XDR platforms appeal to organizations with modest maturity needs due to the detection logic, mostly vendor-provided, that generally requires less customization and maintenance.
- XDRs appeal to organizations looking for improved visibility across the security stack, as well as those looking to lower the administration requirements of more complex incident response (IR) solutions.
- Midsize organizations that struggle to correlate and respond to alerts generated from disparate security controls appreciate the productivity gain from centralized XDR interfaces.
- Staff with the required skills to maintain and operate an extensible detection stack are hard to recruit and retrain.
- Purchasing a systemic detection stack in the form of XDR can simplify product selection and acquisition.

Obstacles

- Single-vendor systemic XDR solutions may take years to replace in the case of effectiveness or efficiency issues.
- XDR's lack of extensibility for custom detections and other use cases could cause some clients to need both an XDR and a classic SIEM solution to meet multiple needs.
- Expanding an XDR detection stack's capabilities through the addition or replacement of security controls may be limited by the vendor.
- An XDR product alone does not always meet all needs for long-term log storage for use cases other than incident response, such as compliance, application monitoring and performance monitoring. XDR may also be a poor choice for a forensically sound system of record for things such as access data.

User Recommendations

- Work with security operations stakeholders to determine if the XDR strategy is right for your organization.
- Base decision criteria on staffing and productivity levels, level of IT federation, risk tolerance, and security budget, as well as consolidation aims and the presence of existing XDR component tools.
- Develop an internal architecture and purchasing policy that is in line with your XDR strategy, one that explains when and why exceptions might be permissible.
- Plan security purchases and technology retirements in relation to a long-term XDR architecture strategy.
- Favor security products that provide APIs for information sharing, and that allow automated actions to be sent from an XDR solution.

Sample Vendors

CrowdStrike; Fortinet; Microsoft; Palo Alto Networks; SentinelOne; Sophos; Stellar Cyber; Trend Micro; Trellix

Gartner Recommended Reading

Market Guide for Security Orchestration, Automation and Response Solutions

Sliding into the Trough

Digital Risk Protection Services

Analysis By: Mitchell Schneider, Jonathan Nunez

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Digital risk protection services (DRPS) are a set of technology-led services which enable brand protection, third-party risk assessment and discovery of external-facing threats, and provide technical response to identified risks. These solutions provide visibility into the surface web, social media, dark web and deep web sources to identify potential threats to critical assets and provide contextual information on threat actors, their tactics and processes for conducting malicious activities.

Why This Is Important

Modern attacks, from commodity exploits to highly curated and sophisticated fraud schemes, have become increasingly prevalent and effective as threat actor delivery modalities have been commensurately commoditized (clear, deep and dark web). DRPS leverages these modalities to discover and mitigate the risks which may directly impact business operations or reputation. These services typically require specialized skill sets to operate and are most often consumed as an outsourced function.

Business Impact

DRPS proactively identifies external-facing risks from social media-related artifacts, provides dark web findings, and even supports third-party risk initiatives to determine corrective courses of actions, with the purpose of protecting your organization's brand. Their services aim to associate all malign activity on the public internet related to your organization, enrich those findings with threat context, and perform technical responses to evict certain threats when possible (takedowns).

Drivers

- DRPS has been driven by its ability to support a range of use cases and user roles. Example use cases include digital footprinting (e.g., mapping internal/external assets and identifying shadow IT); brand protection (e.g., impersonations, doxing and misinformation); account takeover (e.g., credential theft, lookalike domains and phishing sites); data leakage detection (e.g., detection of intellectual property, personally identifiable information [PII], credit card data, credentials); and high-value target monitoring (e.g., VIP/executive monitoring).
- Complexities in the management of risks are key reasons why organizations can benefit from DRPS. These complexities include an expanding attack surface, a more hybrid workforce, higher reliance on e-commerce, regulatory compliance, cloud assets, digital business transformation, and the magnitude of information derived from monitored risk and security activities (e.g., preextortion related to ransomware).
- Demand for DRPS is also driven by the accessibility of such an offering for small or midsize businesses (SMBs) that originally couldn't benefit from threat intelligence (TI), due to the lack of specialized skills and resources for security, including the time needed to perform follow-up actions. This is because of the less technical and more accessible nature of the intelligence made available by many DRPS providers, as well as the availability of a managed service type of offering.

Obstacles

- The DRPS market is starting to get crowded with more than 50 vendors, which makes it difficult for vendors to differentiate themselves from one another. Furthermore, the vendor capabilities vary and may be limited in their ability to provide a comprehensive solution. Some vendors have a best-of-breed approach, whereby they focus heavily on single DRPS use cases (e.g., VIP/executive monitoring), whereas many vendors have expanded to support more than one use case, including external attack surface management (EASM) — the latter natively or via acquisition.
- Market consolidation is accelerating and increasingly overlaps with complementary markets, such as TI, managed security service providers (MSSPs)/managed detection and response (MDR) providers, as well as EASM. These markets are experiencing increased competition.

User Recommendations

- Evaluate the capabilities and features of DRPS offerings and match them to the needs of your organization's security programs and business risks. Ask vendors what threats they cover and whether they focus on a specific use case or many (e.g., phishing, dark/deep web monitoring, data leakage and/or social media protection).
- Prioritize best-of-breed solutions to meet specific urgent needs, depending on the urgency and importance of the core use case. One example would be threats arising from consistent look-alike domains and phishing domains requiring takedown services. Assess vendors based on takedown success rates and ability to work with internet service providers (ISPs) and registrars in foreign locations.
- Prioritize solutions that include managed services in their offerings (especially if there are resource constraints), that can predict and prevent issues from occurring in the first place, and have service-level agreements (SLAs) that ensure the fastest remediation time.

Sample Vendors

Allure Security; Bolster Inc.; CloudSEK; CybelAngel; Cyberint; Cybersixgill; GroupSense; ReliaQuest; SOCRadar; ZeroFox

Gartner Recommended Reading

Market Guide for Security Threat Intelligence Products and Services

Tool: Vendor Identification for Security Threat Intelligence Products and Services

Emerging Tech: Adoption Growth Insights in Digital Risk Protection Services

Emerging Tech: Security — The Future of Attack Surface Management Supports Exposure Management

Innovation Insight for Attack Surface Management

Managed SIEM Services

Analysis By: Pete Shoard

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

Managed security information and event management (MSIEM) services provide remote management and/or monitoring of a client-owned SIEM solution. Services ensure availability and performance, and assist with the creation of a wide range of SIEM use cases, data acquisition, and reporting content.

Why This Is Important

Organizations of all sizes are making strategic investments in SIEM. Flexibility, customization and service requirements are at the center of a decision to utilize managed SIEM. The lack of available skills for deployment and maintenance means that buyers require the assistance from a managed service. The challenge that faces organizations is not the investment in technology, but the ongoing complexity, staffing and cost of supporting SIEM deployments.

Business Impact

Organizations make SIEM purchases, but often struggle to operate them effectively. Detection and response is critical to the success of any security strategy. SIEMs are becoming more accessible, as more midsecurity and midmaturity buyers are entering the market by adopting cloud-based IT. Managed SIEM provides value in overlooked areas, such as creation and tuning of detection content/reporting, maintenance, and lightweight investigation of security issues.

Drivers

- The complexity of SIEM deployments and configuration requirements means that many buyers do not have the in-house expertise to build, configure, and maintain SIEM.
- Buyers require the ability to continuously build and update the detection content and reporting within the SIEM. This requires expert knowledge of the threat landscape and other data manipulation skills, which are hard to acquire and retain.
- Different to turnkey services, such as managed detection and response (MDR) managed SIEM, provides buyers greater flexibility and customization in configuring a dedicated detection and response capability. Managed SIEM is often a follow-up pathway to MDR, which is chosen as an organization's security maturity increases and internal skill sets grow.
- Managed SIEM provides resources to triage the large volume of alerts and threats discovered by SIEM deployments in a cost-effective manner. It also provides resources outside of normal business hours.
- Buyers may already have a services provider or systems integrator, where this partner has implemented a SIEM for threat detection and incident response on behalf of the buyer.
- Many buyers have adopted, or plan to adopt, SaaS SIEM offerings in line with other infrastructure investments, migrating from legacy on-premises deployments or existing SaaS SIEM platforms. The requirements of these migrations are complex and can benefit from assistance from experienced managed SIEM vendors.

Obstacles

- Direct requirements setting is imperative for engagement with a managed SIEM provider, as most services focus on technology implementation rather than scoping.
- The flexibility of managed SIEM engagements means several elements are customizable, including technology choice and implementation. While it is important to have a clear vision, understanding what is of value for the organization is troublesome.
- Managed SIEM providers operate on a consultative basis regarding requirements, which could increase cost if not correctly worded before engaging with the provider.
- Managed SIEM services augment security staffing and operational internal capabilities, but internal staff will still be needed to consume the raw outputs.
- Sharing operational responsibilities between an internal team and an external partner can be challenging, with segmentation of responsibility being hard to define effectively, often leading to dissatisfaction with services.

User Recommendations

- Identify details of use cases early to establish requirements for log data, threat detection and incident response, and any compliance reporting needs to ensure the project costs are well-controlled.
- Evaluate the use of SaaS SIEM to identify whether a managed SIEM provider is required. SaaS SIEM offers lower overheads for technology maintenance.
- Document the organization's network architecture, including deployed security controls, SaaS and IaaS investments, and details of other high-priority integrations, such as identity services, before engaging with managed SIEM vendors. If they are not available, invest in a consultative engagement before purchasing a service.
- Separate requirements aligned to the management of the technology, the creation of content to run on the SIEM, and the operational tasks associated with running and maintaining the platform. Decide which components are best aligned with the support you seek from a service.

Sample Vendors

AT&T; BlueVoyant; Capgemini; NCC Group; ReliaQuest; Talion; Vodafone; Wipro

Gartner Recommended Reading

Magic Quadrant for Security Information and Event Management

Critical Capabilities for Security Information and Event Management

Market Guide for Managed SIEM Services

A Guidance Framework for Architecting and Deploying a Modern SIEM Solution

Vulnerability Prioritization Technology

Analysis By: Mitchell Schneider, Craig Lawson

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Vulnerability prioritization technology (VPT) streamlines a range of vulnerability telemetry sources into a single location — using intelligence sources, analytics and visualizations and to efficiently provide prioritized, pragmatic recommendations on how best to perform critical remediation/mitigation activities. The approach considers the exploitability of a vulnerability, asset or business-criticality, the severity of a vulnerability and compensating controls in place.

Why This Is Important

VPT supports a risk-based vulnerability management (RBVM) approach. These products and services provide a consolidated view of exposures by leveraging the telemetry from sources, including vulnerability assessment (VA) tools, configuration management databases (CMDBs), endpoint detection and response (EDR), penetration testing results and application security testing (AST). VPT adds intelligence and efficiency by leveraging analytics and various threat and vulnerability intelligence sources.

Business Impact

VPT is a form of automation that leverages data science, advanced analytics and vulnerability intelligence to improve VA and prioritization, and rapidly identify the highest-risk exposures for remediation. Moreover, VPT provides the ability to track the VM life cycle via a centralized view. The increase of security incidents and breaches drives many organizations to adopt VPT solutions to implement an effective VM program. This has also caused VA vendors to align more to the RBVM methodology.

Drivers

- Organizations are inundated with vulnerability findings prioritized solely by Common Vulnerability Scoring System (CVSS) scores. VPT solutions contextualize these findings with active threat information, resulting in increased actionability. For example, a vulnerability that is a low risk today might be a high-impact vulnerability tomorrow due to the dynamic changes driven by attackers, while the CVSS score would remain relatively static.
- Interest in the VPT market has accelerated within the last 12 months, according to Gartner research and client inquiries. VPT identifies more pragmatic risks to the organization and helps prioritize actions for vulnerability treatment — whether via remediation (e.g., patching) and/or compensating controls (e.g., intrusion prevention system [IPS] and web application firewalls [WAFs]) — to avoid potential compromise or beginnings of a breach.
- VPT can provide savings in terms of operational full-time employee (FTE) costs due to the automation of vulnerability prioritization, which facilitates attack surface reduction efforts, and results in improved continuity of operations. This is especially beneficial for organizations looking to retain talent by focusing them on more value-added activities.
- The need to take more proactive security actions is offered through other forms of vulnerability prioritization, such as attack path mapping. Attack path mapping is understanding if and how the attacker targets your organization, and what path they could potentially take to get in — uncovering paths to high value assets and contextualizing vulnerabilities risks.

Obstacles

- VPT solutions require a more mature vulnerability management program to be effective. If there are broken processes in the exposure management program, the value of VPT will be limited.
- Organizations that are fixated on CVSS severity as the defining characteristic of how serious a vulnerability is will not be able to get full value from VPT approaches since that metric-driven output is rarely based on risk — as factors like threat activity, asset context and existing security controls are not considered.
- There are overlapping capabilities between VPT and cyber asset attack surface management (CAASM), leading to buyer confusion. CAASM is focused on aggregation of data and visibility, while VPT is focused on improving an organization's RBVM operational processes.
- Attack path mapping is an output of vulnerability prioritization and breach and attack simulation (BAS) to support cybersecurity validation initiatives, but is different from testing security controls. Your organization may already have this capability via another tool.

User Recommendations

- Implement a risk-based approach that correlates asset value and business impact to calculate a risk rating, and automate this through a VPT.
- Augment VA tools with stand-alone VPT solutions for better prioritization, or use existing VPT capabilities that assist with the effective methodology for real risk reduction. This enables vendor consolidation and places less effort on new training and tool deployment.
- Identify vendors with patching and SOAR integrations. This puts the security team in control of workflows. Evaluate if this approach is appropriate. If so, leverage remediation workflow automation and avoid using two different tools.
- Deploy VPT that takes into account the presence (and configuration) of existing security controls to enhance prioritization efforts. This capability is increasing across the market.
- Identify vendors with CAASM capabilities, or who have connectors with your CAASM to better integrate the two products to solve both visibility and improve operational processes.

Sample Vendors

Brinqa; Cisco; Flashpoint; HivePro; Ivanti; NopSec; NorthStar; Nucleus Security; ServiceNow; Skybox Security

Gartner Recommended Reading

How To Implement a Risk-Based Vulnerability Management Methodology

Tracking the Right Vulnerability Management Metrics

Quick Answer: What Are the Top and Niche Use Cases for Breach and Attack Simulation Technology?

Innovation Insight for Attack Surface Management

MDR Services

Analysis By: Andrew Davies

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Definition:

Managed detection and response (MDR) services provide customers with remotely delivered security operations center (SOC) functions. These allow organizations to rapidly detect, analyze, investigate and actively respond through threat disruption and containment. MDR providers offer turnkey experience, using a technology stack that commonly covers endpoint, network, logs and cloud. This telemetry is analyzed in the provider's platform by experts skilled in threat hunting and incident management.

Why This Is Important

The cyberthreat landscape is in constant movement, and the complexity of attacks are escalating against organizations. Most organizations lack the resources, budget or appetite to build and run their own 24/7 SOC function, which is required to help them protect and defend against attacks that increasingly cause more impact and damage to operations. MDR services enable organizations to mature their threat detection and response coverage.

Business Impact

Organizations that have not invested in threat detection and response capabilities are at greater risk from the impact of cyber incidents. The challenge of finding, acquiring and retaining the necessary expertise and tools makes building an adequate internal capability unappealing. MDR services combine people, process and technology, translating security issues into business-focused risks, impacts and outcomes, reducing complexity, and allowing increased security maturity through turnkey adoption.

Drivers

- MDR services enable organizations to focus on business-risk-driven outcomes, as they provide the expertise to interpret and deliver against a set of requirements in a turnkey format. Ultimately, this delivers relevant and actionable business outcomes.
- The expansion of an organization's IT infrastructure and digital footprint, moving into a broader set of providers and technologies, puts pressure on organizations to maintain visibility across an ever broader set of attack surfaces. MDR providers offer high-fidelity threat detection and coverage of a wide range of data sources, technologies and SaaS platforms.
- MDR providers allow for remotely delivered response actions, enabling buyers to respond and mitigate issues faster with lower impact to their business. However, the level of autonomy granted to vendors varies according to the trust level. With the improved access to MDR service providers' portals, clients can validate the response for a scenario, and possibly execute it.
- With the variety of risk-based issues that organizations are paying attention to, MDR providers are expanding their capabilities to include exposure management and risk management. The combination of these, with a traditional detection and response capability, are helping clients with the visibility they require.
- Buyers increasingly require fast adoption of mature capabilities that would have taken a long time to build or buy, and have been prohibitively expensive to operate. MDR delivers a turnkey solution for those who have no desire to build and maintain internal capability, or require capability quickly.

Obstacles

- The high diversity of vastly different approaches to offering MDR services often causes buyers to question how strategically to engage a provider.
- Technology vendors with detection and response solutions offer closely named, but often more light-touch overlay services, such as managed endpoint detection and response (MEDR), managed security information and event management (MSIEM), and managed extended detection and response (MXDR). This ends up increasing buyers' confusion.
- Performance issues with MDR service providers and failed engagements are often due to misaligned expectations. Buyers should clearly outline what they require the services to deliver, rather than focus on the technology or data that they want monitored.
- Not assigning staff as the point of contact to the service can cause challenges. Segmentation of operational responsibilities between internal contacts and an external partner, if not defined effectively, usually leads to dissatisfaction with services.

User Recommendations

- Focus on outcomes, not technologies, for MDR buyers. Organizations underinvested in technologies such as EDR and network detection and response (NDR) should favor an approach in which a vendor provides the tools and delivers the desired outcomes, and ensures it is in the contract language.
- Assess MDR services if buyers are lacking staff and expertise to handle incident response activities once a threat has been identified, or want to add threat-hunting capabilities.
- Examine compatibility as a requirement if there are existing investments in threat detection technologies, such as EDR and SIEM.
- Buy MDR services that offer a migration path to more self-service in the future. Looking for vendors that have open communication channels with analysts and delivery teams can support that goal.
- Choose broader managed security service (MSS) capability providers if technology management, compliance monitoring and other MSSs are required — especially those that offer MDR-type services.

Sample Vendors

Arctic Wolf Networks; BlueVoyant; eSentire; Expel; Optiv Security; Pondurance; Rapid7; Red Canary; ReliaQuest; Secureworks

Gartner Recommended Reading

Market Guide for Managed Detection and Response Services

Quick Answer: Key Questions to Ask When Selecting a Managed Detection and Response (MDR) Provider

The Top 3 Technology Priorities in Midsize Enterprises

SOAR

Analysis By: Eric Ahlm, Craig Lawson

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Gartner defines security orchestration, automation and response (SOAR) as solutions that combine incident response, orchestration and automation, and threat intelligence (TI) management capabilities in a single solution. SOAR tools can be leveraged for many security operations tasks, such as documenting and implementing processes, supporting security incident management, applying machine-based assistance to human security analysts and operators, and better operationalizing the use of TI.

Why This Is Important

SOAR tools are flexible and can be applied to various security operations centers (SOCs) and broader SecOps use cases. Current buyers tend to be end-user organizations and security services providers with a SOC function that are looking to optimize the efficiency, consistency and effectiveness of their threat monitoring, detection and incident response activities. Threat management use cases for SOAR are still emerging.

Business Impact

SOAR solutions can help clients:

- Reduce errors in handling incidents by codifying activities.
- Scale security operations by adding efficiency in handling various tasks and activities.
- Improve SOC team morale and reduce analyst turn over by removing repetitive tasks from humans.

Drivers

- SOAR can improve the process and execution speed of repetitive tasks that often torment SOCs, especially tasks that consume time and require little human expertise. This frees teams to spend more time on critical tasks and activities.
- SOAR can increase alert fidelity and actionability by adding more context and data enrichment. This helps reduce noise due to the high volume of alerts that needs to be handled by the SOC team.
- Security orchestration and automation (SOA) as a capability is increasingly needed by security operations. SOAR solutions offer flexible SOA in the platform. However, SOA is also becoming more available as canned, baked-in functionality in other security technologies, such as email security solutions, to help improve both analysis and triage, and automate responses to threats.

Obstacles

- SOAR requires both development and ongoing operational cycles to maintain, similar to other coding development practices. As such, not all activities will warrant the investment in SOAR development and maintenance.
- SOAR and automation is best applied to existing practice and activities. Clients wanting to use SOAR for building new activities in the SOC may find the time to value is much longer than expected.
- Justifying the expense of automation and a SOAR purchase remains an obstacle for clients. The value of automation is best described in the language of gains into existing areas of operations.

User Recommendations

- Assess the availability of development skill sets internally to develop SOAR's required functionality. Security leaders should also review the time and cost this may add to the total cost of owning an SOAR toolset.
- Involve the entire security organization when scoping requirements for SOAR. Organizations must look beyond simply plugging a new technology into security information and event management (SIEM), and engage with wider security.
- Select an appropriate product based on buyer understanding and its applicable use cases, such as SOC optimization, threat monitoring and response, threat investigation and hunting, and TI management.
- Implement well-defined processes and playbooks before acquiring SOAR. Although SOAR promotes lots of benefits, not every security organization is ready for SOAR tools, and a considerable amount of time is required to develop playbooks.

Sample Vendors

Cyware; D3 Security; Google; Palo Alto Networks; Rapid7; ServiceNow; Splunk; Swimlane; Tines; Torq

Gartner Recommended Reading

SOAR Will Not Make You Better at Running SIEM

Market Guide for Security Orchestration, Automation and Response Solutions

OT Security

Analysis By: Katell Thielemann

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Definition:

Operational technology (OT) includes hardware and software that detect or cause a change, through the direct monitoring and/or control of industrial equipment, assets, processes, and events. OT security focuses on protecting them. As threats and security solutions multiply, a generic category of OT security that was once dominated by network-centric tools is now evolving into multiple categories.

Why This Is Important

Once disconnected from IT networks, the increased connectivity of OT and IT systems has created new security risks. As operational systems are the centers of value creation, OT security has major relevance to organizations in national critical infrastructure, and to any other industrial verticals with operations and asset-centric environments. Network-centric security, with a focus on segmentation and firewalls, traditionally anchored OT security approaches, but new categories have emerged.

Business Impact

Whether it be nation-states targeting critical infrastructure and intellectual property (manufacturing is often targeted for cyber espionage), or financially motivated hackers deploying ransomware, the number of attacks on systems in production or mission-critical environments has increased over the past five years. The impact of operational disruption can range from mere annoyance to hundreds of millions of dollars, along with reliability, life and safety impacts.

Drivers

- Digital transformation initiatives are multiplying in asset-intensive organizations, in turn creating new risks that security teams may have no visibility into.
- Due to a rapidly changing threat landscape, asset-centric organizations are increasingly focusing their attention on the security risks they face outside of enterprise IT. They realize they are surrounded by cyber-physical systems (CPS) that underpin all their production, distribution and value creation efforts.
- International standards, such as IEC 62443, NIS2 and NIST 800 series, are emerging to provide guidance. In some industry verticals, security mandates, such as NERC CIP or TSA directives, are already in place. Given the close relationship between critical infrastructure and national security, and the growing concerns of targeted attacks, government-led efforts are on the rise, adding to the growing list of existing national legislations.
- One of the initial focus areas was network-based security, which has underpinned most OT security efforts for the last decade. But, many specific categories have emerged to deal with the fast-evolving threat landscape and introduce innovation in security operations. As a result, a singular OT security market is evolving.
- Some of the emerging new categories for CPS include protection platforms, cyber risk quantification platforms, secure remote access solutions, security services, network-centric solutions, or onboard diagnostics solutions.

Obstacles

- Organizations face cultural, governance and security controls challenges that prevent a one-size-fits-all approach to security. For instance, production assets often run 24/7 and cannot be stopped at will.
- Manufacturers often connect remotely to production assets to maintain and update them. If not done securely with consistent policies, this creates additional risks. They also often control deployment of updates on the basis of contracts and warranties, which can hamper security efforts.
- Shortages of OT security skills remain acute and growing.
- The age of systems and devices (up to 20 years) means no security updates are available anymore.
- OT security is evolving into CPS asset-centric security, enabled by platforms that support not only OT, but also IoT, industrial IoT, or smart building assets. This is changing OT security from focusing on segmentation and firewalls to placing the assets at the center of security, and layering defense-in-depth approaches around them.

User Recommendations

- Initiate risk discussions between IT security and production/engineering teams, and determine the current extent of OT security efforts.
- Deploy CPS asset discovery, inventory and network mapping security platforms.
- Determine immediate gaps, such as flat networks and missing or misconfigured firewalls.
- Accelerate security awareness and skills training for converging IT and OT infrastructures.
- Focus on organizational and cultural trust challenges between IT and OT personnel.
- Collaborate with your procurement team to demand that OEMs of OT systems ensure that systems are secure by design.
- Prepare for the new reality of CPS security as a centralizing discipline for securing the ever-growing list of IT, OT, IoT and industrial IoT systems, and for bringing together an asset-centric cybersecurity discipline.

Sample Vendors

Blue Ridge Networks; Booz Allen Hamilton; Optiv Security; Waterfall Security Solutions

Gartner Recommended Reading

3 Initial Steps to Address Unsecure Cyber-Physical Systems

Predicts 2023: Cyber-Physical Systems Security — Beyond Asset Discovery

CPS Security Governance — Best Practices From the Front Lines

Innovation Insight for Cyber-Physical Systems Protection Platforms

Climbing the Slope

NDR

Analysis By: Jeremy D'Hoinne, Nat Smith, Thomas Lintemuth

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Network detection and response (NDR) products detect abnormal system behaviors by applying behavioral analytics to network traffic. They continuously analyze raw network packets or traffic metadata for both internal (east-west) and “public” (north-south) networks. NDR can be delivered as hardware and software sensor, and software or increasingly SaaS management console. Organizations rely on NDR to detect and contain postbreach activity, such as ransomware, or insider’s malicious activity.

Why This Is Important

NDR focuses on detecting abnormal behaviors, with less emphasis on signature-based controls detecting known threats. NDR is effective in detecting weak signals and previously unknown behavior from traffic on networks such as lateral movement or data exfiltration. NDR solutions expand to hybrid networks, adding new detections. Automated response capabilities, provided natively or through integration remain important, but incident response workflow automation becomes an increasing area of focus.

Business Impact

NDR solutions provide visibility into network activities to spot anomalies. The machine learning algorithms that are at the core of many NDR products help to detect anomalies in traffic that are often missed by other detection techniques. The automated response capabilities help to offload some of the workload for incident responders. NDR products also help incident responders with their threat hunting by providing useful context and drill-down capabilities.

Drivers

- Detecting postbreach activity: NDR complements traditional preventative controls by detecting activities based on deviations from baseline. This allows the security team to investigate insider's activities resulting from breaches without relying on having observed a previous occurrence of the same activity.
- Low risk — high reward: Implementing NDR products is a low-risk project because the sensors are positioned out-of-band, so they don't represent a point of failure or a "speed bump" for network traffic. Enterprises that implement NDR products as a proof of concept (POC) often report high degrees of satisfaction because the tools provide much-needed visibility into network traffic and enable even small teams to spot anomalies.
- Monitoring cloud traffic: A growing number of NDR vendors offer the ability to monitor IaaS traffic and M365 by leveraging available APIs from the cloud providers. Organizations expanding their cloud presence use NDR to avoid creating gaps in their ability to monitor interactions between their systems.

Obstacles

- Enterprises with a lower maturity security operation program might struggle to justify the expense for a technology that cannot simply be evaluated by counting the number of alerts it triggers.
- The response features of the NDR products are more rarely deployed or narrowed down to specific use cases, such as ransomware, due to a risk of false positives. Many organizations postpone their implementation until they understand how to use the NDR tool better.
- NDR is expanding to support more detections in the cloud but have yet to prove they are the right tool for the use case.
- False positives are inevitable with any behavioral-based detection tool. NDR tools might require fine-tuning of the configuration to reduce the amount of false positives, especially in early days of the deployment. This explains why response capabilities are more rarely deployed initially.
- NDR increasingly competes for budget with consolidated platforms such as SIEM and extended detection and response (XDR).

User Recommendations

- Develop a strong understanding of the overall traffic patterns and specific traffic patterns in your enterprise network to gain maximum value from NDR.
- Carefully plan sensor types and deployment locations so that the most relevant network traffic can be analyzed. Proper positioning of the NDR sensors is critically important to limit the number of false positives and control the cost of the deployment.
- Tune out false positives in the implementation phase (false positives may be triggered by vulnerability scanners, shadow IT applications and other factors that may be specific to your environment).
- Plan for ongoing tuning as new detection models are deployed from the vendor.
- Select sensor capturing capacity that is sized appropriately for your network.

Sample Vendors

Cisco; Corelight; Darktrace; ExtraHop; Fortinet; IronNet; MixMode; Plixer; Trend Micro; Vectra

Gartner Recommended Reading

Market Guide for Network Detection and Response

Emerging Tech: Top Use Cases for Network Detection and Response

Threat Intelligence Products and Services

Analysis By: Jonathan Nunez

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Threat intelligence (TI) services provide buyers with knowledge about the cyberthreat landscape by documenting tactics, techniques and procedures; and by profiling threats and threat actors. TI products deliver tools to assist organizations in aggregating, collecting, curating and operationalizing their own TI and potentially sharing it with outside entities.

Why This Is Important

Security leaders have an obligation to understand the organization's threat landscape. They must ensure their security solutions are updated with the latest threat content and provide contextual information to their teams as it helps inform overall risk. TI provides the means for an organization to maintain visibility of their threat landscape, build timely, accurate and actionable insights that can be applied before, during and after threats present themselves to your organization.

Business Impact

- TI products and services are applicable in every industry, across security functions and controls, because every organization has a unique threat landscape.
- TI informs the business about current and potential future threats that pose risks to organizations.
- TI solutions can be applied as machine- or human-readable to enhance security technologies and an understanding of adversarial intentions and motivations.

Drivers

- Security platform vendors are investing in TI products and services either through organic development or acquisitions. These vendors are delivering an increasing amount of threat intelligence platform (TIP) functionality to aggregate TI and manage it within a single platform offering, accelerating the adoption and utilization of TI in the market.
- Organizations continue to look for security solutions that address multiple use cases. This has pushed TIP vendors to extend beyond the security orchestration, analytics and reporting (SOAR) functionality they have been advertising, to now offering threat detection and enhanced analytic platform features.
- TI service providers are now expanding their core use cases and features to include digital risk protection services (DRPS), offering organizations a single-vendor way to deliver highly curated external threat and risk information. Gartner continues to see an interest in DRPS capabilities and features, driving TI solution providers to add the capability to their portfolios.
- Organizations are putting more effort toward understanding their risk by aligning digital exposures with malign threats. Often informed by TI, these vendors are now starting to offer external attack surface management (EASM) in an effort to heighten curation and increase actionability.
- Curation is key for organizations as they grapple with increased volumes of data. Customers will continue to demand a deep understanding of the threat landscape as they work to synthesize TI into actionable insights.

Obstacles

- Many organizations have no formal TI program or dedicated analysts to use TI solutions, like a TIP, or interpret the value from bespoke TI reports. They rather focus on indicators like IP addresses, domains and hash values, and allocate too few resources to human-readable or advanced TI solutions.
- Organizations struggle to measure and justify the value of TI solutions. Lack of TI performance reporting will increase the likelihood of TI budget cuts or prohibition of program maturation.
- Many organizations lack well-defined priority intelligence requirements (PIRs), which can lead to overinvestment in or underutilization of TI solutions.
- A saturated and seemingly undifferentiated TI marketplace creates buyer confusion and fatigue, especially in light of not having well-defined PIRs, which can aid in the vendor-selection process.

User Recommendations

- Incorporate TI solutions and services into your overall security program. Define detailed requirements and expectations for TI service providers to deliver outcomes aligned to organizational threat concerns.
- Ensure PIRs are defined to drive TI solution needs before TI vendor engagement. This is a foundational requirement as it informs what to focus on, what to collect, who to track, and what it means to the business in terms of risk and exposure.
- Develop operational delivery metrics (ODMs) for the defensible maturation of your TI Program. These ODMs should focus on metrics and outcomes that drive faster detection and response, increased efficacy in security tools, and improved efficiency in incident response.
- Consider leveraging TI services through your existing managed security services or managed detection and response providers. These providers can decrease time-to-value while simultaneously scaling your TI program by providing technical collection, curation, analysis and reporting.

Sample Vendors

Bfore.Ai; Cybersixgill; Cyware; DuskRise; GroupSense; Security Alliance; Silobreaker; ThreatConnect; ZeroFox

Gartner Recommended Reading

Market Guide for Security Threat Intelligence Products and Services

Tool: Vendor Identification for Security Threat Intelligence Products and Services

Emerging Technologies: Adoption Growth Insights in Digital Risk Protection Services

Innovation Insight for Attack Surface Management

Emerging Technologies: Critical Insights for Threat Intelligence Demand

Endpoint Detection and Response

Analysis By: Franz Hinner, Satarupa Patnaik, Eric Grenier

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Endpoint detection and response (EDR) analyzes system, process, and user activity to detect security threats. It provides remedial guidance for threats that bypass prevention controls and enables endpoint threat investigations. EDR capabilities are often included in endpoint protection platforms and delivered as software agents connected to centralized cloud-based security analytics and management software.

Why This Is Important

EDR is an essential defense component for most enterprise endpoints. It requires the installation of an agent to assist in the discovery and reporting of suspicious and malicious behaviors, visualization of attack propagation, and remediation guidance. EDR can stop known malware and ransomware families, and it can also help discover and remediate more stealthy and unknown threats.

Business Impact

- All devices and servers that connect to corporate networks or handle data need EDR protection.
- New threats and covert exploits require early identification and quick reaction.
- Cyber insurers and regulators demand EDR, and some EDR solutions provide low-cost ransomware insurance.

Drivers

- The nature of threats has changed. It is no longer practical to achieve 100% prevention, and older endpoint protection platform (EPP) tools should be updated to also contain EDR functionality.
- Stealthy malware and ransomware campaigns, state-sponsored adversaries and supply chain attacks use advanced techniques to remain undetected and to bypass older security controls.
- Remote work has accelerated the adoption of cloud-managed solutions, which now represent 80% of the installed bases and most new deployments.
- Detection of user- and machine-identity-related exploits and credential misuse is an emerging must-have feature.
- Rapid real-time response, as incidents unfold, is critical to contain a threat and stop it from spreading.
- Augmenting existing vulnerability management programs and providing a means to reduce the attack surface are increasingly needed to ensure systems are not misconfigured and have no unpatched vulnerabilities.
- The collection of logs and events from EDR agents forms the basis for retrospective threat detection and threat hunting.
- Sophisticated attacks require a new breed of EDR tools that work holistically together with other security tools as a composable security ecosystem to maximize protection and minimize exposure.

Obstacles

- Many businesses lack and underestimate the knowledge and resources to install and employ EDR tools successfully. EDR adoption requires responder training, including “range” training that mimics assaults.
- Traditional endpoint security technologies and agents don’t function with cloud-hosted workloads’ “agile” deployment pipelines. This splits agile deployed workloads from containers or serverless computing.
- Non-Microsoft-Windows systems may lack feature parity. Endpoint security solutions for these systems lack EDR detection and response capabilities.
- In hybrid and remote working models, older on-premises technologies are difficult to adopt and maintain.

User Recommendations

- Choose solutions with a single unified agent and fast remote deployment.
- Prioritize technologies with ease of use and prebuilt automated playbooks.
- Favor cloud-hosted solutions with flexible deployment options.
- Assess the organization’s ability to monitor and manage detection and response services to identify gaps and determine if a managed service is required for your organization. Ensure appropriate data retention and fulfill regulatory compliance.

Sample Vendors

Cisco; CrowdStrike; Cybereason; Fortinet; Microsoft; Palo Alto Networks; SentinelOne; Sophos; Trellix; Trend Micro

Gartner Recommended Reading

Magic Quadrant for Endpoint Protection Platforms

Critical Capabilities for Endpoint Protection Platforms

Entering the Plateau

SIEM

Analysis By: Eric Ahlm, Mitchell Schneider

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Definition:

Security information and event management (SIEM) is a configurable security system of record that aggregates and analyzes security event data from on-premises and cloud environments. SIEM assists with response actions to mitigate issues that cause harm to the organization, and satisfy compliance and reporting requirements.

Why This Is Important

Aggregating and normalizing data from various environments to centralize visibility is a core element of effective security programs. SIEM supports an organization's ability to identify, prioritize and investigate security events of interest, execute response actions and report on current and historical security events.

Business Impact

SIEM solutions can impact the business by:

- Allowing organizations to identify and respond to critical security events earlier in their life cycle to reduce risk.
- Creating overall situational awareness for security issues and events, providing an efficient and trusted system of record, which can be used for operational security and compliance reporting.
- Aligning disparate technology investments and reducing the operational staffing overhead of managing security issues and incidents.

Drivers

- Central monitoring of threats, as reported by multiple sources, is a primary driver for SIEM. A SIEM offers a central place to monitor and investigate security alerts, as well as supporting contextual information required to make an alert actionable.
- A SIEM can turn raw alert data into actionable intelligence, through whatever analysis method works best for a given monitoring objective.
- The need to expand detection workflow to include response activities with capabilities such as security orchestration, automation and response (SOAR).
- SaaS SIEM solutions in the cloud transfer the platform and infrastructure maintenance to the vendor and allow for more predictable linear budgeting for growth.
- As more assets move to cloud-centric environments, such as Microsoft Azure, Amazon Web Services (AWS), Google Cloud Platform (GCP), Oracle and many others, a SIEM must have awareness of the underlying environment to perform well.
- Organizations have a large quantity of both streaming and nonstreaming data, which is useful for security monitoring, and SIEM platforms provide a centralized place to store and interrogate this data.

Obstacles

- Getting a SIEM to perform well against detecting attacks requires dedication and sufficient staffing. Undermanaged SIEMs continue to plague many organizations.
- SIEM budgets and resources are constrained; however, the types of threats to monitor tend to be rather endless. As such, deciding what to best monitor with the SIEM resources you have is concession engineering at best.
- SIEM threat detection performance is dependent on not only SIEM and its configuration, but also the detection stack and all supporting telemetry chosen to be sent to the SIEM.
- Gartner is tracking a number of non-SIEM solutions that provide value for a limited function of a traditional SIEM. This can cause increased buyer confusion or make the justification of a complete SIEM more challenging

User Recommendations

- Preplan what monitoring objectives best meet your organization's security needs. Use those as design requirements to correctly identify important selection criteria such as analysis methods, performance, sizing and retention.
- Allow for a learning period of alerting to determine how best to operationalize detection and response as planning operational support of alert pipeline management without knowing how many alerts and how much work is required can be difficult.
- Ensure your cloud SIEM is aware of the underlying infrastructure which it monitors. A SIEM must understand the nuances of its native environment, such as AWS, Google Cloud or Microsoft Azure.

Sample Vendors

Elastic; Exabeam; IBM; LogRhythm; Microsoft; NetWitness; Rapid7; Securonix; Splunk

Gartner Recommended Reading

Magic Quadrant for Security Information and Event Management

Critical Capabilities for Security Information and Event Management

Vulnerability Assessment

Analysis By: Mitchell Schneider, Jonathan Nunez

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Vulnerability assessment (VA) tools operate across on-premises, cloud and/or virtual environments to help reduce exposure. They discover, identify and report on vulnerabilities of IT, cloud, IoT and/or OT devices OSs and software. They also establish a baseline of connected assets and vulnerabilities; identify and report on security configuration of assets; and support compliance reporting and control frameworks, risk assessment and remediation prioritization, and remediation activities.

Why This Is Important

VA is a foundational component of the vulnerability management (VM) process, supporting infrastructure hardening, security posture management, proactive prevention of threats, and conformity with regulations and compliance regimes. VA is a fundamental process for the discovery and enumeration of digital assets and their associated security weaknesses, helping to reduce the risk to IT.

Business Impact

Security exposures in infrastructure, apps and other assets can be abused by attackers for malicious purposes. When used in conjunction with a well implemented VM program, VA solutions can be used to effectively reduce the risks associated with security breaches, such as malware infections and ransomware. Also, many regulatory bodies and standards require organizations to perform VM for compliance mandates.

Drivers

The VA market is mature; however, advancement and innovation continues to be applied to VA tools and services in the areas of discovery, prioritization and remediation/mitigation (such as tracking vulnerability remediation progress and workflow automation) to meet buyers' evolving requirements and needs — including newer capabilities such as external attack surface management (EASM).

Although compliance use cases are still strong drivers for leveraging VA tools, many organizations are implementing these solutions to help understand, prioritize and reduce the risk of exposure from threats (see How to Implement a Risk-Based Vulnerability Management Methodology).

Depending on their maturity level, organizations typically pick one of three delivery models for VA:

- Buying, deploying and operating the product with internal staff. VA application and network scanners are both deployed on-premises or increasingly delivered as SaaS. SaaS (cloud)-delivered VA products have components on-premises, but are managed from the cloud.
- Buying and deploying the tool, then having it operated by a third party, such as a managed security service provider (MSSP) or managed detection and response (MDR) service provider.
- Outsourcing to a third party that provides managed VM services and uses its own proprietary technology or licensed commercial tools.

Obstacles

- Although VA solutions are relatively easy to deploy, if extensive agent deployment is not required, organizations will need resources and expertise that they may not have. Therefore, outsourcing VM to a security service provider is a credible option that many pursue.
- Risk-based prioritization of vulnerabilities is still not the norm for many VM programs, as the tools are still evolving this capability.
- The VA market is fragmented and characterized by a small number of large, pure-play vendors — along with startups and other vendors from various security markets offering VA as part of their overall product portfolio.
- VA used to be simple, with a big scanner deployment covering the entire environment, but factors are different now. Organizations may have multiple tools for cloud, another for containers, traditional vulnerability scanners, a solution to assess OT assets and one for endpoint detection and response (EDR), which can sometimes provide VA capabilities for the end-user systems.

User Recommendations

- Evaluate vendors offering a combined solution if your organization is resource-constrained or wants to consolidate vendors. Most VA vendors have added prioritization and EASM capabilities to their products.
- Evaluate and distinguish between the various deployment options available in the VA market, and understand how the technology fits your requirements.
- Network scanning involves remote scans of network-connected devices, but will not work when devices are off the network; give preference to authenticated scanning.
- Agent-based scanning assists with getting vulnerability data from assets that are not connected to the enterprise LAN. Agent-based scanning is best for remote workers or a DMZ.
- API-based scanning is often delivered from the cloud, but does not preclude scanning from on-premises appliances or software.
- Evaluate VA vendors that have strong built-in integrations with patch management and IT service management tools, which are aimed at streamlining the overall VM process.

Sample Vendors

Balbix; CrowdStrike; Intruder Systems; Microsoft; Outpost24; Qualys; Rapid7; Secureworks; Tenable; WithSecure

Gartner Recommended Reading

Market Guide for Vulnerability Assessment

Decoding Vulnerability Management: A Stand-Alone Tool vs. a Technique in Endpoint Protection

The Top 5 Elements of Effective Vulnerability Management

A Guidance Framework for Developing and Implementing Vulnerability Management

Appendixes

See the previous Hype Cycle: Hype Cycle for Security Operations, 2022

Hype Cycle Phases, Benefit Ratings and Maturity Levels

Table 2: Hype Cycle Phases

(Enlarged table in Appendix)

Phase	Definition
Innovation Trigger	A breakthrough, public demonstration, product launch or other event generates significant media and industry interest.
Peak of Inflated Expectations	During this phase of overenthusiasm and unrealistic projections, a flurry of well-publicized activity by technology leaders results in some successes, but more failures, as the innovation is pushed to its limits. The only enterprises making money are conference organizers and content publishers.
Trough of Disillusionment	Because the innovation does not live up to its overinflated expectations, it rapidly becomes unfashionable. Media interest wanes, except for a few cautionary tales.
Slope of Enlightenment	Focused experimentation and solid hard work by an increasingly diverse range of organizations lead to a true understanding of the innovation's applicability, risks and benefits. Commercial off-the-shelf methodologies and tools ease the development process.
Plateau of Productivity	The real-world benefits of the innovation are demonstrated and accepted. Tools and methodologies are increasingly stable as they enter their second and third generations. Growing numbers of organizations feel comfortable with the reduced level of risk; the rapid growth phase of adoption begins. Approximately 20% of the technology's target audience has adopted or is adopting the technology as it enters this phase.
Years to Mainstream Adoption	The time required for the innovation to reach the Plateau of Productivity.

Source: Gartner (July 2023)

Table 3: Benefit Ratings

Benefit Rating ↓	*Definition* ↓
Transformational	Enables new ways of doing business across industries that will result in major shifts in industry dynamics
High	Enables new ways of performing horizontal or vertical processes that will result in significantly increased revenue or cost savings for an enterprise
Moderate	Provides incremental improvements to established processes that will result in increased revenue or cost savings for an enterprise
Low	Slightly improves processes (for example, improved user experience) that will be difficult to translate into increased revenue or cost savings

Source: Gartner (July 2023)

Table 4: Maturity Levels

(Enlarged table in Appendix)

Maturity Levels	Status	Products/Vendors
Embryonic	In labs	None
Emerging	Commercialization by vendors Pilots and deployments by industry leaders	First generation High price Much customization
Adolescent	Maturing technology capabilities and process understanding Uptake beyond early adopters	Second generation Less customization
Early mainstream	Proven technology Vendors, technology and adoption rapidly evolving	Third generation More out-of-box methodologies
Mature mainstream	Robust technology Not much evolution in vendors or technology	Several dominant vendors
Legacy	Not appropriate for new developments Cost of migration constrains replacement	Maintenance revenue focus
Obsolete	Rarely used	Used/resale market only

Source: Gartner (July 2023)

Document Revision History

Hype Cycle for Security Operations, 2022 - 5 July 2022

Hype Cycle for Security Operations, 2021 - 23 July 2021

Hype Cycle for Security Operations, 2020 - 23 June 2020

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Understanding Gartner's Hype Cycles

Tool: Create Your Own Hype Cycle With Gartner's Hype Cycle Builder

Emerging Technologies: Top Trends in Security for 2022

Security Operations Primer for 2023

Top Trends in Cybersecurity 2022

SOC Model Guide

Table 1: Priority Matrix for Security Operations, 2023

Benefit	*Years to Mainstream Adoption*			
↓	*Less Than 2 Years* ↓	*2 - 5 Years* ↓	*5 - 10 Years* ↓	*More Than 10 Years* ↓
Transformational			Exposure Management Generative Cybersecurity AI	Cybersecurity Mesh Architecture
High	Endpoint Detection and Response OT Security Vulnerability Prioritization Technology	Breach and Attack Simulation CPS Security Identity Threat Detection and Response MDR Services Threat Intelligence Products and Services Vulnerability Assessment	SOAR XDR	
Moderate	SIEM	Digital Forensics and Incident Response Digital Risk Protection Services External Attack Surface Management Managed SIEM Services NDR	Automated Penetration Testing and Red Teaming Technology Automated Security Control Assessment CAASM Penetration Testing as a Service	
Low				

Benefit	Years to Mainstream Adoption			
↓	Less Than 2 Years ↓	2 - 5 Years ↓	5 - 10 Years ↓	More Than 10 Years ↓

Source: Gartner (July 2023)

Table 2: Hype Cycle Phases

Phase	*Definition*
Innovation Trigger	A breakthrough, public demonstration, product launch or other event generates significant media and industry interest.
Peak of Inflated Expectations	During this phase of overenthusiasm and unrealistic projections, a flurry of well-publicized activity by technology leaders results in some successes, but more failures, as the innovation is pushed to its limits. The only enterprises making money are conference organizers and content publishers.
Trough of Disillusionment	Because the innovation does not live up to its overinflated expectations, it rapidly becomes unfashionable. Media interest wanes, except for a few cautionary tales.
Slope of Enlightenment	Focused experimentation and solid hard work by an increasingly diverse range of organizations lead to a true understanding of the innovation's applicability, risks and benefits. Commercial off-the-shelf methodologies and tools ease the development process.
Plateau of Productivity	The real-world benefits of the innovation are demonstrated and accepted. Tools and methodologies are increasingly stable as they enter their second and third generations. Growing numbers of organizations feel comfortable with the reduced level of risk; the rapid growth phase of adoption begins. Approximately 20% of the technology's target audience has adopted or is adopting the technology as it enters this phase.
Years to Mainstream Adoption	The time required for the innovation to reach the Plateau of Productivity.

Phase ↓	Definition ↓

Source: Gartner (July 2023)

Table 3: Benefit Ratings

Benefit Rating ↓	Definition ↓
Transformational	Enables new ways of doing business across industries that will result in major shifts in industry dynamics
High	Enables new ways of performing horizontal or vertical processes that will result in significantly increased revenue or cost savings for an enterprise
Moderate	Provides incremental improvements to established processes that will result in increased revenue or cost savings for an enterprise
Low	Slightly improves processes (for example, improved user experience) that will be difficult to translate into increased revenue or cost savings

Source: Gartner (July 2023)

Table 4: Maturity Levels

Maturity Levels ↓	*Status* ↓	*Products/Vendors* ↓
Embryonic	In labs	None
Emerging	Commercialization by vendors Pilots and deployments by industry leaders	First generation High price Much customization
Adolescent	Maturing technology capabilities and process understanding Uptake beyond early adopters	Second generation Less customization
Early mainstream	Proven technology Vendors, technology and adoption rapidly evolving	Third generation More out-of-box methodologies
Mature mainstream	Robust technology Not much evolution in vendors or technology	Several dominant vendors
Legacy	Not appropriate for new developments Cost of migration constrains replacement	Maintenance revenue focus
Obsolete	Rarely used	Used/resale market only

Source: Gartner (July 2023)