Deloitte.

Attack Surface Management (ASM)

Identify. Assess. Strengthen.

Deloitte's ASM offering delivers comprehensive services to help you identify, assess, and strengthen your tech environment. From advanced, AI-powered testing to exposure management programs, our global team of ethical hacking professionals combines cyber and business insights to help you proactively protect your organization and boost resilience.

The challenge

Threats from cyber adversaries are growing as business complexity and vulnerability chaos increases. With each new technology stack component and third-party connection, as well as the recent, rapid proliferation of Gen AI, an organization's attack surface expands and creates more entry points. Whie many organizations have testing capabilities and security tools, they often lack end-to-end visibility and struggle with effective remediation due to large, complex technology landscapes. Without a unified approach to integrating key data sources and prioritizing extensive vulnerability backlogs, addressing exposures in a risk-based, cost-effective manner remains a challenge

End-to-end Attack Surface Management

Our ASM offering enables you to take charge of your tech environment, from strategy to implementation to ongoing operations—so you can have peace of mind as your critical assets are protected.

Identify

Build actionable intelligence and understand real-world threats by identifying threat actors, attack vectors, tactics, techniques, and procedures (TTPs), leaked credentials, and brand abuse specific to your industry and organization. Analyze how threats could materialize within your attack surface, which will be validated in the Assess phase.

Assess

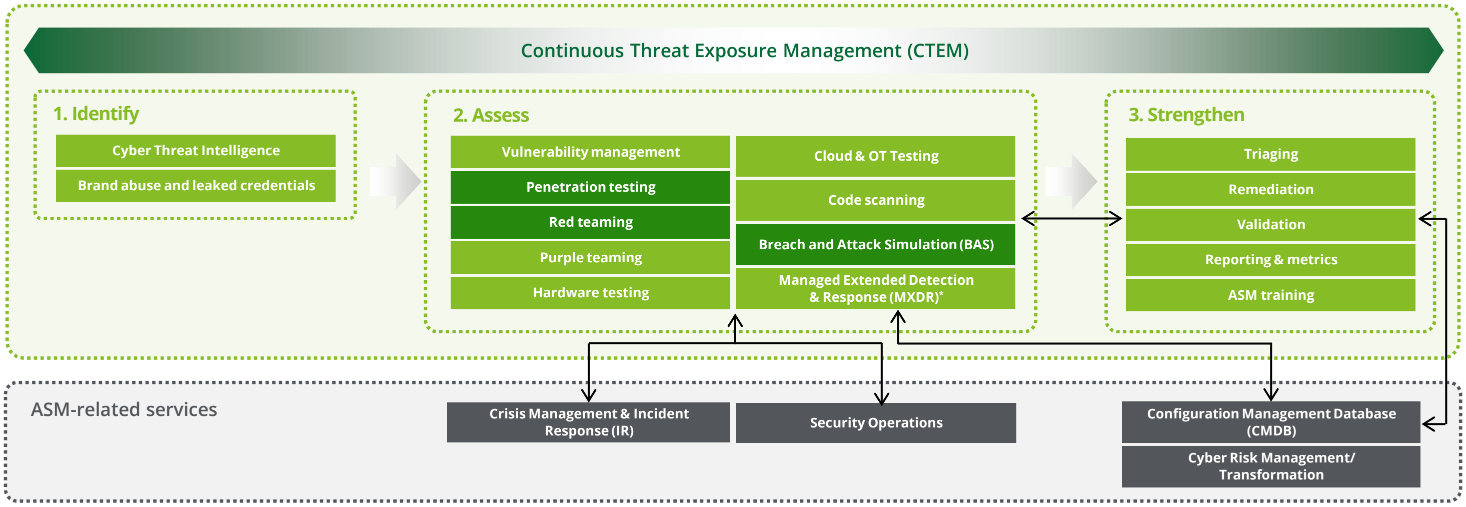
Thoroughly examine and obtain information about your tech environment by identifying potential vulnerabilities and attack paths—through effective combination of capabilities like vulnerability scanning, (manual and automated) penetration testing, breach and attack simulation, red teaming.

Strengthen

Fuse all information regarding your attack surface, obtained in the Assess phase, to effectively prioritize and remediate critical vulnerabilities, validate the effectiveness of controls, and provide comprehensive insights to enhance organizational readiness.

Continuous Threat Exposure Management (CTEM)

Continuously assess and prioritize threat exposure through a programmatic approach for end-to-end ASM. Our cyclical process of scoping, discovery, prioritization, validation, and mobilization strengthens security posture and minimizes breach risks.



Continuous Threat Exposure Management (CTEM)

1. Identify
- Cyber Threat Intelligence
- Brand abuse and leaked credentials

2. Assess
- Vulnerability management
- Penetration testing
- Red teaming
- Purple teaming
- Hardware testing
- Cloud & OT Testing
- Code scanning
- Breach and Attack Simulation (BAS)
- Managed Extended Detection & Response (MXDR)*

3. Strengthen
- Triaging
- Remediation
- Validation
- Reporting & metrics
- ASM training

ASM-related services
- Crisis Management & Incident Response (IR)
- Security Operations
- Configuration Management Database (CMDB)
- Cyber Risk Management/ Transformation

Deloitte can support clients with a wide range of capabilities. Three of our core offensive security testing services are highlighted below:

Penetration Testing

Evaluate specific scope of systems, applications, and networks for vulnerabilities and validate exploit possibilities, leveraging automation and AI for optimization (e.g., 50% reduction of manual efforts for web app penetration testing).

Red Teaming

Validate the effectiveness of protective and detective controls by mimicking threat actors via real-life threat scenarios. Frequently, our red teams are able to stay undetected even in mature client organizations and achieve their predefined objectives.

Breach and Attack Simulation

Continuously simulate cyberattacks and validate control effectiveness/optimize compliance efforts by using an automated and quantitative security testing approach against MITRE ATT&CK Framework-mapped threats.

* Managed Extended Detection & Response (MXDR) by Deloitte is a managed service offering that operates 24x7x365 cyber threat hunting, detection, response, and remediation capabilities. Because detect and respond tooling is typically installed across the entire IT/OT environment, MXDR can be used to obtain data on the attack surface (e.g., vulnerabilities).

Deloitte's ASM in action: A global chemicals company

Issue

A leading chemicals organization, dealing with an increase in sophisticated cyberattacks, aimed to better understand and manage its expanding attack surface with a focus on physical vulnerabilities and reliance on third-parties.

Solution

Working with Deloitte, the client developed a comprehensive ASM program to set up the required governance and assess its attack surface. Deloitte deployed ASM specialists, ethical hackers, and proprietary ASM tools to identify a very large number of vulnerabilities, effectively prioritizing and remediating these vulnerabilities.

Impact

Enhanced ASM visibility and governance has allowed the organization to actively reduce risks and costs—through detailed reporting and proactive insights that guide activities and investments (e.g., increased visibility of attack surface by 152%, reduced vulnerabilities by 41% and overall risk by 41%). The program has helped the organization improve its business resilience and ability to innovate.

Focusing on bottom-line benefits

Working with Deloitte to transform your attack surface management allows you to initiate real change and empower your business to make a greater impact.

Increase visibility of existing attack paths as well as relevant threats

Understand your attack surface through integrating key data sources – enabling proactive remediation of risks

Safeguard critical systems and data, helping protect customer trust and brand reputation, and enabling a more resilient organization

Boost regulatory compliance in a cost-effective manner

Innovate faster – thanks to seamless security testing and remediation, and confidence in your level of resilience

The Deloitte difference

HOLISTIC APPROACH

Help proactively manage your tech environment—integrating key data sources (threats, vulnerabilities, attack paths, etc.), and prioritizing issues—from strategy to implementation to ongoing operations.

operations

Deliver crucial **cyber remediation capabilities beyond ASM**—such as cyber strategy and transformation, detection and response—for small- and large-scale remediation and transformation, to cost- effectively improve resilience and reduce cost of compliance.

GLOBAL NETWORK OF PROFESSIONALS AND RESOURCES

Our professionals can serve your business wherever you operate—with **100+ local offices** and satellite centers worldwide. **Certified in Offensive Security**: Certified Professional (OSCP), Certified Red Team Professional (CRTP), Certified Ethical Hacker (CEH), and many more.

In addition to **1,000+ offensive security practitioners**, we can draw on more than 40,000 global cyber professionals who can provide support across Deloitte's global network.

DEEP EXPERIENCE AND ACCELERATORS

20+ years of ASM experience, with automated testing and artificial intelligence (AI) reporting tools, research (e.g., undetectable payloads/malware), **and accelerators** (e.g., checklists to ensure quality and completeness of vulnerability identification, MITRE control mapping for Governance, Risk and Compliance (GRC)), that allow us to accelerate the reduction of your attack surface.

Ethical hacking specialists with **extensive technical experience** perform **advanced offensive security testing** capabilities on all types of technology (e.g. IT, operational technology (OT), GenAI/LLMs, hardware such as cars and medical devices) to discover vulnerabilities and validate control effectiveness.

Industry Recognition

#1

Ranked No. 1 in Security Services Worldwide by revenue in Gartner® Market Share Report, 2024.[1]

Named a **leader in Worldwide Cybersecurity Incident Readiness Services** by IDC MarketScape[2]

Named a **leader in Worldwide Managed Detection and Response Services** by IDC MarketScape[3]

Take the next step to become more resilient

To learn more, contact our team today: globalasmcyber@deloitte.com

Endnotes

[1] Gartner, Market Share: Security Services, Worldwide, 2024, By Rahul Yadav, Shailendra Upadhyay, Akshita Joshi, Tarun Rohilla, Bryan Haley, 25 April 2025. Gartner is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

[2] IDC MarketScape: Worldwide Incident Readiness Services 2021 Vendor Assessment, by Craig Robinson and Christina Richmond, November 2021, IDC #US46741420

[3] IDC MarketScape: Worldwide Managed Detection and Response (MDR) Services 2024 Vendor Assessment by Craig Robinson, April 2024, IDC #US49006922e

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/aboutto learn more.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms or their related entities (collectively, the "Deloitte organization") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.