PICUS

Reducing Risk in Banking, Financial Services and Insurance (BFSI) with Adversarial Exposure Validation

CTEM and DORA Guide for BFSI Organizations

Executive Summary

The **Banking, Financial Services, and Insurance (BFSI)** sector is increasingly under attack, and the attack surface has been expanding significantly, mainly driven by digital transformation initiatives.

Traditional vulnerability management and manual penetration testing practices can no longer withstand the scaling volume and complexity of cyber exposures. For this reason, BFSI organizations have started adopting **Exposure Management** programs, which work hand in hand with the collaboration of two main powerhouses: **Exposure Assessment Platforms (EAPs)** and **Adversarial Exposure Validation (AEV)** technologies. EAPs identify organizational exposures, along with providing a level of prioritization capability based on scoring models such as CVSS and EPSS. However, this sole reliance on these legacy scoring systems leaves a **significant gap in prioritization**, leaving organizations with an unmanageably large amount of issues remaining.

Adversarial Exposure Validation overcomes this challenge by simulating and emulating real-world attack scenarios to identify the most critical and exploitable vulnerabilities, factoring the effectiveness of existing security controls. Powered by automation technologies such as

- **Breach and Attack Simulation (BAS**),
- **Automated Penetration Testing** and **Red Teaming**,

AEV tools enable BFSI firms to adopt an “assume-breach” mindset. This approach allows security teams to focus on the most pressing risks, significantly reducing the number of vulnerabilities that require immediate attention.

By providing actionable and tailored mitigation suggestions for security controls, AEV technologies also streamline remediation efforts, helping organizations improve their security posture faster and more efficiently.

Without validation, what is today identified as an "unmanageably large issue" will become an "impossible task."

Gartner *2024 Strategic Roadmap for Managing Threat Exposure*

Introduction

The BFSI sector faces unique cybersecurity challenges due to its complex regulatory environment, the high value of the data it handles, and its critical role in the global economy. The sensitive nature of the data these firms manage—ranging from personal financial details to large-scale transaction records—makes them prime targets for cyberattacks. IBM's 2024 Cost of a Data Breach Report highlights that financial firms experienced the **second-highest** breach costs across all industries—surpassed only by healthcare—with the average breach costing $6.08 million, **22% higher** than the global average.

At the same time, the adoption of cloud technologies, increased reliance on third-party vendors, the growing use of mobile and online banking services, and the proliferation of interconnected systems with APIs are rapidly expanding the attack surface of BFSI firms. Consequently, Moody's survey reveals that organizations within the BFSI sector are becoming increasingly concerned about their capability to address the risks associated with the attack surface. 65% of the organizations admit that they have visibility gaps, 56% confirm that their approach to evaluating risk exposure lacks maturity, and 75% are concerned about the expanding scale of the attack surface.

This combination of factors creates a uniquely challenging cybersecurity landscape for BFSI firms, which are increasingly overwhelmed by the volume of exposures. As a result, traditional vulnerability management approaches are no longer sufficient. The solution lies in **Adversarial Exposure Validation (AEV)** technologies—tools designed to cut through the noise and focus on the exposures that pose the greatest risk to the business.

By adopting AEV technologies such as **Breach and Attack Simulation (BAS**) and **Automated Pentesting**, BFSI organizations can significantly reduce the operational burden on security teams, prioritize the most critical threats, and accelerate the remediation process. This approach helps organizations not only improve their security posture but also meet regulatory requirements and protect their bottom line.

In this whitepaper, we will explain the mechanics of AEV technologies and provide actionable guidance for BFSI organizations on selecting and implementing the right solutions to reduce risk and enhance cybersecurity. Additionally, we will demonstrate how to effectively run a Continuous Threat Exposure Management (CTEM) cycle, offering step-by-step examples to illustrate each phase of the process.

75% **of the IT and business leaders within financial services are concerned about the expanding scale of the attack surface.**

MOODY'S *2023 Cyber Survey*

Exposure Management and CTEM

Exposure management is the process of identifying, prioritizing, and mitigating security vulnerabilities that could be exploited by malicious actors. The goal is to reduce risk by aligning security efforts with the evolving threat landscape, ensuring that organizations are not only reactive but also proactive in their security posture. Exposure management encompasses not just vulnerability scanning, but a holistic view of all potential exposures, including misconfigurations, weak security policies, and gaps in security controls.

Continuous Threat Exposure Management (CTEM), on the other hand, is a structured and dynamic approach to exposure management. CTEM refines and enhances the exposure management process by making it continuous, data-driven, and more aligned with the tactics used by attackers.

By 2026, Gartner predicts that organizations using CTEM to guide their security investments will see a significant reduction in breaches—up to two-thirds—thanks to its emphasis on integration of advanced technologies like breach and attack simulation (BAS) and automated penetration testing to continuously validate both the organization's exposure and the effectiveness of its remediation efforts.

Exposure Management vs. Traditional Vulnerability Management

The table below highlights key differences between exposure and vulnerability management.

	CTEM	Traditional Vulnerability Management
Scope	Comprehensive (vulnerabilities, misconfigurations, weak policies, and third-party risks, etc.)	Focuses primarily on network, system and application vulnerabilities
Prioritization	Context-aware (considers business impact, threat intelligence, and effectiveness of compensating controls)	Generic (often relies on legacy scoring systems like CVSS and EPSS without business or asset context)
Validation	Simulates real-world adversarial attacks to validate exploitability	Limited validation, often theoretical risk assessment
Stakeholder Involvement	Involves cross-functional teams (security, IT, risk management, business units)	Primarily handled by IT or security teams
Remediation	Focused on the most critical, validated risks	Often overwhelming due to large volumes of unprioritized vulnerabilities

Why CTEM is Well Suited for BFSI

CTEM is a proactive cybersecurity approach that offers BFSI organizations continuous visibility, real-time threat validation, and prioritized risk management, making it especially effective in addressing the sector's unique security challenges.

Complex and Expanding Attack Surface:

BFSI organizations face an increasing number of vulnerabilities due to digital services like mobile banking, cloud infrastructure, and third-party integrations. CTEM provides continuous, real-time monitoring, ensuring vulnerabilities are quickly identified and addressed, unlike traditional periodic assessments.

High-Value Target for Cybercriminals:

Financial institutions are prime targets for advanced cyberattacks. CTEM uses adversarial exposure validation techniques to simulate real-world attacks, helping organizations focus on what matters the most and strengthen defenses.

Regulatory Compliance:

BFSI firms must adhere to strict regulations (e.g., PCI-DSS, CCPA, SOX, DORA). CTEM continuously validates security controls and helps meet compliance requirements by providing real-time insights and prioritizing vulnerabilities based on business impact.

Operational Efficiency:

Traditional vulnerability management tools often overwhelm security teams with non-contextual and low-priority alerts. CTEM filters non-critical vulnerabilities, allowing BFSI firms to focus resources on the most pressing risks, improving time to remediation and overall efficiency.

By 2026, organizations that prioritize their security investments based on a CTEM program will be three times less likely to suffer a breach.

Gartner *"How to Manage Cybersecurity Threats, Not Episodes"*
August 21, 2023

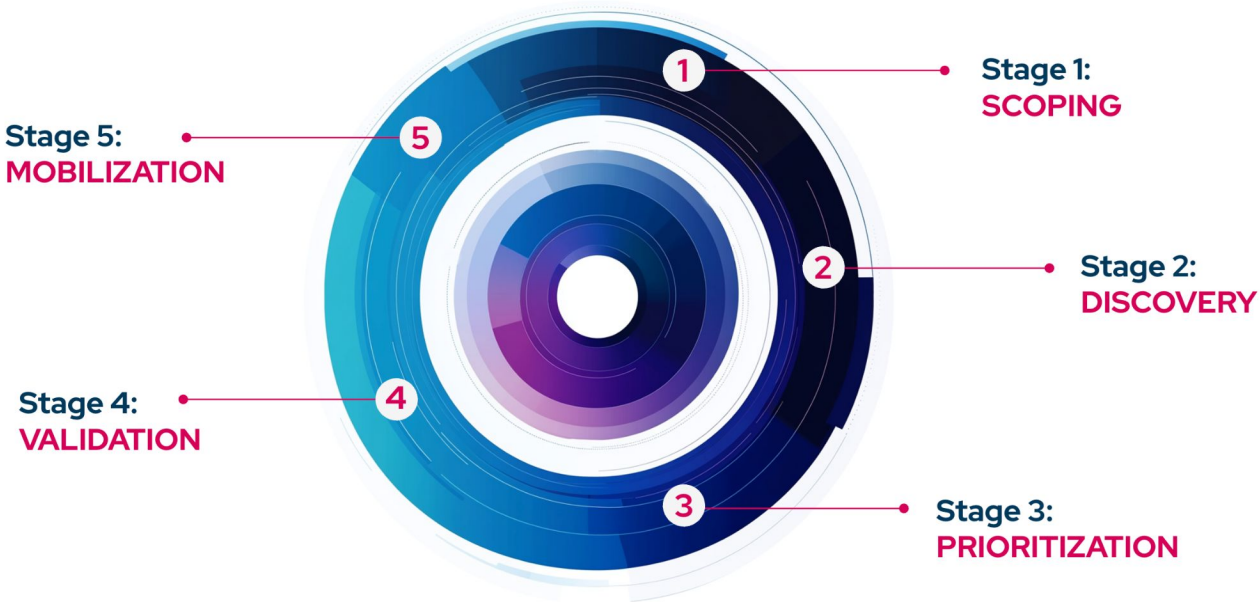
CTEM Implementation for BFSI

Continuous Threat Exposure Management follows a five-step lifecycle:

- **Scoping,**
- **Discovery,**
- **Prioritization,**
- **Validation, and**
- **Mobilization**

of the remediation efforts for identified exposures.

In the following sections, we will dissect each stage of the CTEM lifecycle, define the objectives and expected outputs, provide concrete examples, and highlight key activities that BFSI firms can undertake to proactively reduce their threat exposures, thereby improving their security posture.



Moving away from "just" managing vulnerabilities and patching doesn't remove these issues from existence.

Technology we own and depend on will always have some sort of vulnerability, which must be prioritized alongside newly discovered exposure types.

Gartner. *Gartner, 2024 Strategic Roadmap for Managing Threat Exposure*

Stage 1:

Scoping

- **Objective:** Define and outline the scope of the exposure management program.
- **Output:** A clear, well-defined scope that prioritizes high-value targets and critical systems.
- **Stakeholders:** Security teams, Risk management, IT teams, Compliance officers, Business unit leaders.
- **Success Metrics:** Coverage of critical assets and systems, alignment with business priorities, clear understanding of the organization's threat landscape.

Key Activities for BFSI in the Scoping Stage

Identify Organization's Critical Assets:

A BFSI firm typically operates a complex network with critical components, including:

- Core banking systems, payment gateways (e.g., SWIFT, ACH), customer databases (containing Personally Identifiable Information, or PII), financial transaction systems, and mobile banking applications.
- Regulatory compliance systems (e.g., systems handling Anti-Money Laundering (AML) compliance, Know Your Customer (KYC) data).
- Third-party integrations (e.g., fintech partners, credit card processors, insurance claim systems).

Define Business Operations:

Defining business operations is crucial to aligning exposure management with the organization's core services and assets. For instance, in a retail bank, operations include Internet banking, ATM networks, and mobile apps, while in an insurance company, they focus on claim processing, underwriting platforms, and agent portals.

Identify Threat Actors Specifically Target BFSI Sector:

Financial institutions face a range of threat actors, each with different motivations and methods. These include:

- Advanced Persistent Threats (APTs) specifically targeting financial systems.
- Organized cybercriminal groups aiming for fraud or financial theft.
- Insider threats from disgruntled employees with access to sensitive data.

Set Your CTEM Goals:

Here are example goals that you would want to apply after running a CTEM program.

- Protect customer data and financial transactions.
- Ensure compliance with regulations including but not limited to PCI-DSS, CCPA, SOX.
- Secure third-party connections and APIs.

Stage 2:

Discovery

- **Objective:** Identify vulnerabilities, misconfigurations, and potential exposure points across the scoped environment.
- **Output:** A comprehensive list of exposures - vulnerabilities, weaknesses, and potential attack vectors.
- **Stakeholders:** Vulnerability management teams, Security operations, IT administrators.
- **Success Metrics:** Complete inventory of vulnerabilities and exposures across the attack surface, identification of all potential entry points.
- **Tools:** Vulnerability Scanners, Threat Intelligence Platforms, Cyber Asset Attack Surface Management (CAASM), External Attack Surface Management (EASM), Digital Risk Protection Tools & Services (DRPT/S), SaaS Security Posture Management (SSPM)

Key Activities for BFSI in the Discovery Stage

Vulnerability Scanning:

- Regularly scan web applications, such as internet banking portals, for OWASP Top 10 vulnerabilities, including SQL injection, cross-site scripting (XSS), insecure deserialization, weak authentication mechanisms, and insufficient security misconfigurations. Ensure these scans also cover API endpoints, session management flaws, and any unprotected sensitive data exposure.
- Conduct internal scans of core banking systems for outdated software, unpatched vulnerabilities, or misconfigurations using solutions.

Asset Discovery:

- Use tools like CAASM solutions to map all connected assets across the network, including ATMs, point-of-sale (POS) systems, branch office workstations, cloud-based services, and third-party integrations.
- Discover shadow IT systems, like unapproved cloud storage or SaaS apps, that employees may use to handle sensitive data.

Threat Intelligence:

- Leverage threat intelligence feeds to identify emerging threats targeting financial institutions, such as malware variants like **Nexus**, **Xenomorph**, or **GoatRAT**, which are commonly used in banking Trojans.

Attack Surface Mapping:

- Map out potential attack paths, such as phishing attacks that could lead to credential theft or vulnerabilities in third-party payment processors that could expose transaction data.

Stage 3:

Prioritization

- **Objective:** Rank exposures based on risk, business impact, regulations, and likelihood of exploitation, accounting for the effectiveness of security controls
- **Output:** A prioritized list of exposures
- **Stakeholders:** Risk management, Security teams, and Business unit leaders.
- **Success Metrics:** Clear prioritization of exposures based on risk, business impact, and exploitation likelihood, reduced list of critical vulnerabilities.
- **Tools:** Vulnerability prioritization technologies, adversarial exposure validation tools, risk assessment frameworks, threat modeling tools, and business impact analysis tools.

Key Activities for BFSI in the Prioritization Stage

Prioritization should be carried out by considering the following factors:

Risk Scoring:

While frameworks like CVSS and EPSS provide valuable vulnerability scoring, they often lack the necessary context for accurate prioritization. For instance, a critical Log4j vulnerability in a customer-facing online banking app should be prioritized much higher than the same vulnerability in an internal HR system, but both may receive the same CVSS score. This highlights a major flaw in legacy prioritization systems—they don't account for business-critical assets, compensating security controls, or real-world impact. Although EPSS factors in active exploitation, it still doesn't consider whether compensating controls are effectively mitigating the risk or how the vulnerability affects business operations.

Business Context:

Business context is crucial for prioritization. For example, a vulnerability in the SWIFT payment system would rank higher than one in a non-critical internal system, as SWIFT processes high-value international transactions, posing greater business risk.

Regulatory Considerations:

Prioritize vulnerabilities that could lead to non-compliance with regulations. For instance, a vulnerability that exposes customer PII could lead to PCI-DSS violations and hefty fines.

Threat Likelihood:

If threat intelligence indicates that a certain type of malware is actively targeting financial institutions, prioritize this threat. For example, if a new ransomware variant is targeting outdated Windows servers, prioritize patching those systems to prevent a potential breach.

Compensating Security Controls:

If your security controls block different variants of a threat, its priority can be reduced. For example, if all exploit methods of a vulnerability are blocked by network security controls, the priority of that vulnerability can be lowered. You can verify this using BAS tools.

EXAMPLE

Prioritization Example for BFSI
Using Adversarial Exposure Validation

Here's a real-life example of how adversarial exposure validation helps a BFSI firm prioritize vulnerabilities, enabling the security team to focus on critical threats, saving time and resources, and strengthening overall security.

Scenario Overview

A BFSI organization conducts a vulnerability assessment and identifies over 1,000 distinct vulnerabilities within its network. Addressing all these vulnerabilities simultaneously is not feasible, even for a large security team. To prioritize effectively, the organization utilizes adversarial exposure validation to simulate attack scenarios, determining which vulnerabilities are genuinely exploitable and pose the greatest risk to critical assets.

1. Initial Discovery of Exposures

A thousand vulnerabilities are identified across multiple systems:

- Core banking systems,
- Payment gateways (e.g., SWIFT),
- Customer databases containing PII,
- Mobile banking applications
- Third-party integrations (e.g., fintech APIs)
- Identity and access management (IAM) systems
- Regulatory compliance management tools

2. Filtering Based on Security Controls via Adversarial Exposure Validation

- The organization conducts adversarial exposure validation by simulating attack scenarios to determine which vulnerabilities are actively exploitable.
- The security team uses tools like **Breach and Attack Simulation (BAS**), and **Automated Penetration Testing, and Red Teaming** technologies for validation.
- The validation process reveals that 90% of the vulnerabilities (900 vulnerabilities) are blocked by existing security controls such as NGFW, IPS, EDR, and WAF, meaning they are not immediately exploitable by attackers. Therefore, they are de-prioritized for immediate remediation.

Fixing 100 validated vulnerabilities can be far more impactful than scrambling to fix 1,000 potential issues. The key to that is knowing where to focus.

3. Risk Scoring and Prioritization

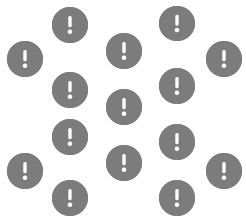
- The remaining 100 vulnerabilities are found to be immediately exploitable and pose a high risk to critical assets. These vulnerabilities affect:
  - Customer databases: Exposing sensitive PII, which could lead to identity theft or regulatory fines.
  - Payment systems: Vulnerabilities in systems like SWIFT or ACH that could result in financial fraud or unauthorized transactions.
  - Mobile banking applications: Vulnerabilities that could allow attackers to compromise customer accounts or intercept financial data.
  - Third-party integrations: APIs that handle sensitive payment or customer data.

- Risk scoring is applied to the 100 exploitable vulnerabilities based on:
  - Business impact: Vulnerabilities affecting customer data or payment systems are prioritized higher due to the potential for financial loss, regulatory penalties, and reputational damage.
  - Likelihood of exploitation: Vulnerabilities that are actively being targeted in the wild (based on threat intelligence) are prioritized higher.
  - Regulatory implications: Vulnerabilities that could result in non-compliance with regulations like PCI-DSS, CCPA, DORA or SOX are given top priority.

- A risk-based prioritization matrix is created:
  - Critical vulnerabilities (e.g., a SQL injection vulnerability in the customer database that could expose millions of records) are given the highest priority.
  - High-risk vulnerabilities (e.g., a vulnerability in the payment gateway that could allow unauthorized transactions) are next in line.
  - Moderate-risk vulnerabilities (e.g., vulnerabilities in internal systems that are less likely to be targeted but still pose a risk) are addressed later.

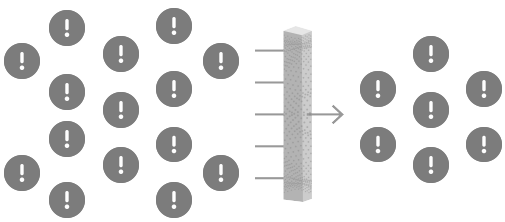
1 Discovery

A growing **attack surface** results in an growing list of exposures, including vulnerabilities, assets, devices, and misconfigurations.



2 Exposure Validation

Prioritization establishes high-risk exposures based on business context. Then, **Exposure Validation** works as a filter to prove which exposures pose an actual risk to your org.



3 Risk Scoring and Prioritization

Validated exposures are prioritized based on their security impact. This helps you tackle your organization's most pressing exposures first.

Stage 4:

Validation

- **Objective**: Evaluate the real-world impact of identified exposures, demonstrate the feasibility of various attack scenarios, and convert exposure data into a prioritized and validated list of actionable exposures.
- **Output:** Verified understanding of the organization's exposure to real-world threats in the presence of compensating security controls.
- **Stakeholders:** Red teams, Blue teams, Security operations, IT administrators.
- **Success Metrics**: Successful validation of security controls, reduced false positives, and confirmation of critical vulnerabilities' exploitability
- **Tools:** Adversarial Exposure Validation tools (Breach and Attack Simulation (BAS) platforms, automated penetration, and red teaming technologies)

Key Activities for BFSI in the Validation Stage

Attack Simulation:

- Leverage Breach and Attack Simulation platforms to simulate attacks within your environment continuously. For instance, BAS tools can simulate attacks to assess the effectiveness of your email gateway, web application firewall, endpoint detection and prevention solutions, firewall, and other security controls.

Penetration Testing:

- Conduct regular penetration tests on critical financial networks and systems. For example, a penetration test could simulate a lateral movement attack within the organization's network to assess whether an attacker could move from a compromised system to other critical assets, such as customer databases or transaction systems. Leverage automated penetration testing tools to enable continuous testing, swiftly identify real-time vulnerabilities, and minimize manual effort, ensuring a secure and resilient environment for sensitive financial data.

Red Team Exercises:

- Perform red teaming exercises to simulate real-world attacks on high-value targets like the core banking system or customer databases. For instance, a red team might attempt to exfiltrate sensitive PCI and PII data. Use automated red team tools to continuously simulate advanced persistent threats (APTs) and adversary behavior to test the resilience of your defenses without the need for constant manual intervention.

Remediation Validation:

- After applying a new signature or rule on a security control, validate that the fix has been properly applied. For example, if a new IPS rule is implemented to block exploitation of a specific vulnerability, simulate the attack by attempting to exploit the vulnerability to verify that the IPS blocks the malicious traffic.

Adversarial Exposure Validation for BFSI

Adversarial Exposure Validation (AEV) is a proactive approach to assessing and mitigating cyber risks by simulating real-world attack scenarios. This method is crucial for industries like BFSI, which manage vast amounts of sensitive data and are prime targets for financially motivated cyberattacks. By simulating and emulating the tactics, techniques, and procedures (TTPs) used by real threat actors, AEV enables security teams to evaluate both the feasibility of an exposure being exploited and its potential impact.

AEV helps organizations defend against persistent threats by automating the identification and validation of vulnerabilities. It reduces the manual burden of adversarial engagements, ensuring that security controls are continuously tested in real-time. This allows BFSI organizations to prioritize risks based on both the likelihood of an attack's success and the severity of its impact, improving decision-making and resource allocation.

AEV tools simulate and automate attack scenarios to verify whether identified vulnerabilities can be exploited by adversaries, assess the effectiveness of current security controls, and measure the organization's ability to detect and respond to threats in real-time. These insights provide crucial context for prioritizing risks.

Key Adversarial Exposure Validation tools include:

- **Breach and Attack Simulation (BAS)**: Automates continuous simulations of known attack vectors.
- **Automated Penetration Testing**: Identifies and attempts to exploit seemingly isolated security vulnerabilities.
- **Automated Red Teaming**: Simulates full-scale adversarial attacks, testing defenses and response readiness.

In this section, we will explore how these three technologies contribute to the Validation stage of the CTEM lifecycle, with a specific focus on their critical role in enhancing cybersecurity for the BFSI sector.

Adversarial Exposure Validation delivers data-driven clarity on attack feasibility in BFSI—turning theoretical risks into actionable insights by stress-testing defenses against real-world adversarial behaviours, identifying weaknesses before they can be exploited.

Breach and Attack Simulation (BAS) for BFSI

BAS solutions are excellent examples of Adversarial Exposure Validation tools that run a wide range of attack simulations, helping organizations continuously assess their cybersecurity posture. In BFSI sector, where the stakes are particularly high due to the sensitive nature of financial data and regulatory requirements, BAS tools play a crucial role in validating security controls and identifying vulnerabilities before they can be exploited.

To ensure a strong return on investment, BAS vendors are expected to provide a variety of attack vectors, including:

- **Malware and ransomware download attacks**, which are particularly relevant given the increasing frequency of ransomware targeting financial institutions.
- **Atomic attacks**, such as credential dumping scenarios, which are critical in environments where unauthorized access to financial systems can lead to significant data breaches or fraud.
- **Advanced Persistent Threat (APT)** scenarios, which simulate the sophisticated, long-term attacks often targeting financial institutions.
- **Data exfiltration attacks**, which mimic the theft of sensitive financial data, including customer information and transaction records.
- **Web application and email attacks**, which are common attack vectors in BFSI, given the reliance on online banking, customer portals, and email communication.
- **Vulnerability exploitation attacks,** which test the organization's ability to defend against vulnerabilities in critical financial systems.
- **Ready-to-run and dynamic attack templates** specifically curated for BFSI organizations

BAS is the financial sector's virtual stress test —continuously probing defenses to identify threat exposures before cybercriminals can exploit them, safeguarding the resilience of BFSI organizations in an environment of constant risk.

Breach and Attack Simulation (BAS) for BFSI

Advanced BAS tools like Picus Security Control Validation (SCV) offer BFSI organizations the ability to:

1. **Comprehensive Testing of Preventive and Detective Controls:**

BAS solutions test both preventive controls (e.g., NGFWs, WAFs, and IPS and detection measures like SIEM and EDR solutions). For BFSI organizations, this is particularly important because attackers often attempt to bypass preventive controls to gain access to high-value assets, such as core banking systems, payment processing platforms, and customer databases. By testing these controls, BAS helps organizations understand:

- Whether preventive measures are effectively stopping attacks at different kill chain stages
- How quickly and accurately detection systems identify malicious activity
- Whether alerts are generated and logged

2. **End-to-End Cyber Kill Chain Simulation:**

BAS tools simulate the entire cyber kill chain, from initial access to privilege escalation and data exfiltration. This end-to-end approach helps BFSI organizations validate their security posture against the most advanced attack scenarios.

3. **Data-Driven Visibility and Actionable Insights:**

Automated Red Teaming tools provide data-driven visibility into an organization's security posture by measuring key metrics such as, **time to detection which means** how quickly an attack is detected after it begins.

4. **Regulatory Compliance and Reporting:**

In the highly regulated BFSI sector, Automated Red Teaming helps organizations demonstrate compliance with industry standards and regulations, such as: PCI-DSS, DORA, SOX, CCPA/CPRA.

Advanced BAS tools give BFSI organizations a critical edge by testing both preventive controls and defensive measures—delivering data-driven results on whether threats are blocked or, if not, detected, logged, and alerted.

With real-world attack simulations and actionable insights, they enable faster detection and ensure regulatory compliance.

Automated Penetration Testing for BFSI

Automated Penetration Testing is an Adversarial Exposure Validation technology that targets specific systems, applications, or networks of an organization. The primary objective of these technologies is to identify and exploit security vulnerabilities within a pre-established scope, simulating how real-world attackers would infiltrate an organization's environment. This has become especially critical for the Banking, Financial Services, and Insurance (BFSI) sector, where the protection of sensitive financial data, customer information, and compliance with stringent regulations are paramount.

The demand for penetration testing has surged in recent years as BFSI organizations recognize the importance of maintaining a strong security posture. With increasing regulatory requirements such as PCI DSS, SOX, CCPA/CPRA as well as industry-specific standards like FFIEC and NIST, Automated Penetration Testing software has become a preferred choice due to its efficiency, scalability, and ability to simulate complex attack scenarios.

Automated Penetration Testing tools are designed to uncover and exploit seemingly isolated security vulnerabilities, such as:

- **Kerberoastable accounts**, which can expose service accounts with weak encryption, a common issue in large financial institutions.
- **Weak passwords** with easily crackable hashes, which are a significant risk in environments where privileged accounts are used to access critical financial systems.
- **Privilege escalation vulnerabilities**, which can allow attackers to move laterally within the network and gain access to sensitive financial data or core banking systems.

Automated Penetration Testing allows BFSI organizations to uncover and chain together seemingly isolated vulnerabilities, *revealing attack paths that lead to critical assets.*

By simulating real-world threats, it helps strengthen security postures and ensures compliance with regulations like PCI DSS and GDPR.

Automated Penetration Testing for BFSI

For example, solutions like Picus Attack Path Validation (APV) run attack vectors within an organization's internal network using an "assumed breach" mindset, which assumes that attackers have already bypassed perimeter defenses. This approach mimics the attack techniques of real-life advanced adversaries, such as APT groups targeting financial institutions.

By chaining together seemingly isolated vulnerabilities, Automated Penetration Testing technologies can simulate how attackers might navigate through an organization's network to access "crown jewel" assets—such as core banking systems, payment gateways, customer databases, and financial transaction systems. This provides BFSI organizations with comprehensive visibility into their attack surface and highlights critical vulnerabilities.

Automated Penetration Testing tools offer BFSI organizations the ability to:

- **Identify complex attack paths** that may not be immediately apparent through isolated vulnerability assessments.
- **Validate the effectiveness of security controls** in preventing lateral movement and privilege escalation within the network.
- **Prioritize remediation efforts** by focusing on vulnerabilities that pose the greatest risk to business-critical assets and operations.
- **Ensure compliance with regulatory requirements** by demonstrating proactive security measures to auditors and regulators.

In conclusion, penetration testing automation is crucial for BFSI organizations looking to strengthen their security posture, protect sensitive financial assets, and meet industry-specific regulatory requirements. These tools provide a realistic assessment of an organization's cyber exposures, helping to mitigate risks before they can be exploited by adversaries. In addition to automated pentesting, in-depth manual penetration testing may be required in certain scenarios.

Automated penetration testing tools simulate advanced attacker behaviors, using an "assumed breach" mindset to map potential routes to critical assets like core banking systems.

By uncovering hidden vulnerabilities and attack paths, they help BFSI organizations strengthen defenses and prioritize high-risk areas for remediation.

Automated Red Teaming with BFSI

Automated Red Teaming is an advanced Adversarial Exposure Validation technology that continuously assesses an organization's security posture by simulating real-world attack scenarios. In the Banking, Financial Services, and Insurance (BFSI) sector, where the protection of sensitive financial data and compliance with stringent regulatory requirements are critical, Automated Red Teaming plays a crucial role in ensuring that an organization's security measures are both resilient and responsive to sophisticated attacks.

Unlike traditional security assessments, Automated Red Teaming focuses on testing compensating controls—both preventive and detective. These technologies simulate the TTPs of Advanced Persistent Threats (APTs) and other sophisticated adversaries, providing a realistic evaluation of how well an organization's security controls react under a full-scale attack.

Automated Red Teaming for BFSI:

Automated Red Teaming tools are designed to mimic the TTPs used by threat actors and malware campaigns that frequently target the BFSI sector, such as BlueNoroff (part of the Lazarus group) and the ALPHV/BlackCat ransomware group, which often employ complex attack chains, including:

- Initial access through phishing or exploiting vulnerabilities in web applications.
- Privilege escalation to gain higher-level access to critical systems.
- Lateral movement to access sensitive data or financial systems.
- Data exfiltration of customer data, payment information, or intellectual property.

By simulating these types of attacks, Automated Red Teaming tools allow BFSI organizations to assess how well their defenses hold up against real-world threats.

Automated Red Teaming simulates every step of the attack kill chain, from initial access to data exfiltration, in a safe and controlled manner.

It helps BFSI organizations test their defenses against real-world threats, ensuring robust security across the entire attack lifecycle.

Key Factors in Choosing The Right Validation Tool For BFSI

To successfully adopt exposure validation, organizations are advised to choose an automated platform that supports various use cases and integrates easily with their implemented security controls. The following criteria can help identify ideal technologies:

Threat Simulation Capability

Threat simulation is a vital capability of exposure validation. Determine the types of threats a tool can simulate and its coverage against the MITRE ATT&CK® framework.

Frequency of Threat Library Updates

To keep pace with the latest threats, a validation tool needs to be regularly updated. Check a vendor's SLA for emerging threat support and releases.

Exposure Assessment Support

To facilitate CTEM, some Exposure Validation tools integrate with Attack Surface Management and Vulnerability Management solutions. Others offer their own native EA capabilities, which can streamline your workflow even further.

Integration with Security Controls

Understand the extent to which a tool can validate your choice of security controls, plus ingest attack surface, vulnerability, and cyber threat intelligence data.

Mitigation Support

A tool should not only be capable of identifying and prioritizing exposures. It should also supply one-click fixes to help you mitigate them quickly.

Ease of Deployment & Automation

To realize a swift time to value equation, look for an exposure validation tool that can be set up and configured in hours, not days.

Use in Production

Identify a tool that can perform validation testing in your environments without disrupting workloads or creating noise for your security operations center.

Training Requirements

Complex tools create a steep learning curve. Evaluate how easy a tool is to use and the security expertise required to manage it.

Stage 5:

Mobilization

- **Objective:** Implement and track remediation efforts, ensuring timely and effective resolution of critical vulnerabilities.
- **Output:** Remediated vulnerabilities, improved security posture, and reduced attack surface.
- **Stakeholders:** IT teams, Security teams, Risk management, Compliance officers.
- **Success Metrics:** Reduction in the number of critical vulnerabilities, improved security posture, compliance with industry standards and regulations.

Key Activities for BFSI in the Mobilization Stage

Improve Security Controls:

- Based on insights gained from validation, refine your security controls to prevent the exploitation of identified exposures. Platforms such as Picus offer both generic and vendor-specific mitigation recommendations, helping to streamline the remediation process and alleviate the operational burden on security teams.

Improve Security Policies:

- Leverage findings from validation to update and improve security policies. For example, if weak password protocols were exploited during a red team exercise, adjust the policy to mandate stronger passwords and implement multi-factor authentication (MFA) for all employees.

Employee Training:

- Conduct regular security awareness training for employees, focusing on phishing, social engineering, and how to handle sensitive financial data. For example, train employees to recognize phishing emails that impersonate executives requesting wire transfers.

Continuous Monitoring:

- Implement Security Information and Event Management (SIEM) solutions to continuously monitor for suspicious activity. For example, monitor for unusual login patterns in the core banking system that could indicate an account takeover attempt. Validate SIEM rules using AEV tools to ensure that alerts are accurately triggered and aligned with the latest threat patterns, allowing for timely detection and response to potential security incidents.

Incident Response Preparation:

- Update the incident response plan based on the findings from validation exercises. For instance, if an automated red team exercise revealed gaps in the response to a ransomware attack, update the playbook to ensure faster containment and recovery.

How Adversary Exposure Validation (AEV) Technologies Support DORA Compliance

In response to risk of cyber threats for financial sector, the Digital Operational Resilience Act (DORA) was introduced by the European Union to ensure that financial entities can withstand, respond to, and recover from ICT-related incidents. DORA sets out a comprehensive framework for managing ICT risks, covering everything from risk management and operational resilience testing to incident reporting and third-party risk management.

One of the most critical aspects of DORA is its emphasis on continuous testing and validation of ICT systems to ensure their resilience against evolving cyber threats. This is where Adversary Exposure Validation (AEV) technologies—such as Breach and Attack Simulation (BAS), Automated Penetration Testing, and Red Teaming—come into play. In the table below, we explore how AEV technologies directly support compliance with key DORA requirements.

Explanation of DORA Requirement	Adversarial Exposure Validation (AEV) Relevance
Chapter II Article 6: Financial entities are required to establish and maintain an ICT risk management framework to manage and mitigate risks related to ICT systems. This framework must cover risk identification, protection, detection, response, and recovery.	AEV technologies help implement and validate the ICT risk management framework by identifying defensive gaps in real-time.
Chapter II Article 7: Financial entities must ensure that their ICT systems, protocols, and tools are secure, resilient, and capable of handling cyber threats. This includes implementing security controls, regular patching, and system upgrades.	AEV tools ensure that ICT systems are resilient, scalable, and capable of handling real-world cyber threats by continuously testing protocols and tools.
Chapter II Article 9: Financial entities must implement adequate protection and prevention measures to safeguard their ICT systems from cyber threats. This includes deploying security controls, firewalls, encryption, and intrusion detection systems.	AEV tools continuously test detection systems measures work as intended. This automated validation helps identify security gaps. Advanced AEV tools also provides detection rules to address these gaps.

How Adversary Exposure Validation (AEV) Technologies Support DORA Compliance

Explanation of DORA Requirement	Adversarial Exposure Validation (AEV) Relevance
Chapter II Article 10: Financial entities are required to have systems in place to detect ICT-related incidents in real time. This includes monitoring for anomalies, vulnerabilities, and potential security breaches that could affect ICT systems.	BAS and Automated Red Teaming test the effectiveness of detection mechanisms by simulating cyberattacks and anomalies in ICT systems.
Chapter II Article 11: Financial entities must establish and test response and recovery plans to ensure that they can quickly recover from ICT-related incidents. These plans should cover business continuity, data recovery, and restoration of operations after an incident.	AEV technologies test the effectiveness of ICT response and recovery plans by simulating real-world cyber incidents and measuring the organization's reaction.
Chapter II Article 13: Financial entities must have processes in place to learn from ICT-related incidents and continuously improve their ICT risk management framework. This includes analyzing incidents to identify root causes and implementing preventive measures.	AEV tools help gather intelligence from simulated incidents to improve the ICT risk management framework and enhance resilience against future threats.
Chapter III Article 17: Financial entities must have a robust incident management process to handle ICT-related incidents. This process should include detection, classification, reporting, and resolution of incidents, with a focus on minimizing the impact on operations.	AEV tools simulate incidents, helping financial entities refine their incident management processes and improve response times. They provide data-driven results into where prevention solutions fail, and in this case, if the attack was logged and alerted.

How Adversary Exposure Validation (AEV) Technologies Support DORA Compliance

Explanation of DORA Requirement	Adversarial Exposure Validation (AEV) Relevance
Chapter III Article 18: Financial entities are required to classify ICT-related incidents and cyber threats based on their severity and potential impact on operations. This classification helps prioritize response efforts and ensures that critical incidents receive attention.	AEV tools help classify vulnerabilities and incidents based on their severity and potential impact, supporting a prioritized response.
Chapter IV Article 24: Financial entities must perform ongoing digital operational resilience testing, ensuring that their ICT systems can withstand cyber threats and disruptions. This includes vulnerability assessments and testing of critical functions.	BAS and Automated Penetration Testing continuously assess cyber defense, ensuring that ICT systems are resilient to attacks and disruptions.
Chapter IV Article 25: Financial entities must ensure that their ICT systems, tools, and processes are tested regularly to identify vulnerabilities and weaknesses. Testing should cover both internal and external systems, including those provided by third parties.	AEV tools conduct penetration testing and scenario-based attack simulations to identify weaknesses in cyber defense of ICT systems.
Chapter IV Article 26: Financial entities are required to conduct Threat-Led Penetration Testing (TLPT) to simulate real-world cyberattacks. This testing must mimic the tactics, techniques, and procedures of genuine threat actors to assess the resilience of critical systems.	AEV tools, especially Automated Penetration Testing and BAS are central to TLPT. They simulate real-world cyberattacks on critical systems to test operational resilience.

Conclusion

The Banking, Financial Services, and Insurance (BFSI) sector faces an increasing volume of cybersecurity risks, making traditional vulnerability management methods inadequate. To address this challenge, BFSI organizations are now adopting Exposure Management programs, which consist of five key stages: scoping, discovering, prioritizing, validation, and mobilization of remediation efforts.

A key component of a CTEM program is Adversarial Exposure Validation (AEV), which provides visibility into how attackers can exploit vulnerabilities. AEV technologies—such as Breach and Attack Simulation (BAS), Automated Penetration Testing, and Red Teaming—not only simulate and emulate real-world attack techniques to focus on the most significant risks but also help BFSI organizations automate threat-led penetration testing, ensuring compliance with standards like DORA.

This data-driven approach allows security teams to prioritize remediation efforts efficiently, reducing operational burden, enhancing security posture, and ensuring long-term resilience against advanced threats.

Adversarial Exposure Validation with Picus Security Validation Platform

As the leading Adversarial Exposure Validation solution, **Picus Security Validation Platform** is unmatched in enabling an organization to focus on and remediate the exposures posing the greatest risk. No other solution can match its leading integrations with existing vulnerability management systems while offering the broadest exposure validation through the use of advanced technologies such as Breach and Attack Simulation, Automated Penetration Testing, and Red Teaming. Additionally, actionable insights and remediation guidance through Picus Mitigation Library empower the ability to take immediate, assured action against validated exposures.

Below, you will find information cards for Picus products that support the validation step of the CTEM lifecycle most effectively.

Automated Pentesting and Red Teaming with Picus

Unlike other solutions, Picus Attack Path Validation (APV) doesn't overwhelm security teams by revealing thousands of theoretical attack paths that are difficult to prioritize. Instead, it simulates the actions of a real-world attacker to identify the shortest path and confirm that it poses a genuine risk.

Using the results of network discovery and enumeration, the Picus platform determines how to achieve the objective in the most efficient and evasive way possible. The real-world actions simulated by Picus APV include:

- **Credential Harvesting**
- **Password Cracking**
- **Data Gathering**
- **Lateral Movement**
- **Privilege Escalation**,
- **Masquerading**,
- **Vulnerability Exploitation**
- **Kerberoasting**

Breach and Attack Simulation with Picus

The Picus Security Control Validation (SCV) product, which is powered on our cutting-edge Breach and Attack Simulation (BAS), enables BFSI organizations to proactively defend against real-world threats by simulating the TTPs used in actual threat and malware campaigns. It offers extensive threat coverage:

- **25,000+ attack actions,**
- **~6,000 threats from network infiltration, endpoint, web application, email-infiltration, and data exfiltration attacks,**
- **10,000+ vendor-specific mitigation suggestions, and 600 generic mitigation suggestions, it offers extensive coverage.**

The platform also features **ready-to-run** and **dynamic threat templates** for emerging threats targeting specific industries and regions, ensuring tailored protection for each organization's unique environment.

About the Picus Security Validation Platform

Reduce your threat exposure with real-world attack simulations and AI-driven insights.

Security Control Validation

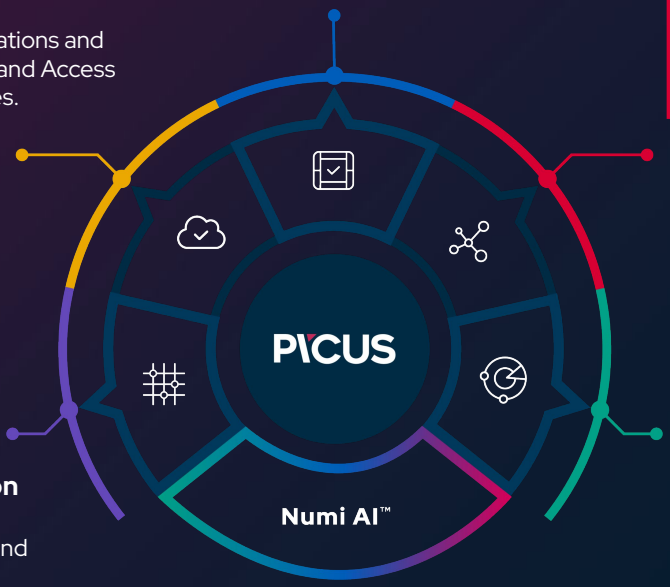
Measure and optimize the effectiveness of security controls with Breach and Attack Simulation.

Cloud Security Validation

Identify cloud misconfigurations and overly permissive Identity and Access Management (IAM) policies.

Attack Path Validation

Eliminate high-risk attack paths that attackers could exploit to compromise users and assets.



Attack Surface Validation

Enhance visibility of internal and external cyber assets and the security risks they pose.

Detection Rule Validation

Optimize detection efficacy by identifying performance issues affecting detection rules.

Elevate your security capabilities with the Picus Security Validation Platform

REQUEST A DEMO

PICUS

picussecurity.com

FROST & SULLIVAN FROST RADAR™ LEADER Global Breach and Attack Simulation 2022

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2023

GLOBAL INFOSEC AWARDS WINNERS CYBER DEFENSE MAGAZINE 2024

Gartner Peer Insights Customers' Choice 2024

4.8/5.0

Highest-rated vendor*

Breach and Attack Simulation

*Gartner, Voice of the Customer for Breach and Attack Simulation Tools, Peer Contributors, 30 January 2024