

CASE STUDY

Global Retail Group Replaces Legacy BAS with Picus for Red Teaming and Auto-Remediation

A global retailer with stores, an online shop and thousands of servers relied on outside red team exercises, which were commonly delayed by months in legal and procurement reviews. Its older attack simulation tool sat alongside single-purpose products and did not work well with its endpoint protection or its IOC automation.

After a proof of concept, the team moved to Picus Breach and Attack Simulation (BAS) and now runs its red teaming operations with Picus attack simulations, continuously, across every environment. Unblocked IOCs flow automatically into the EDR for blocking, and AI Threat Builder keeps simulations in line with latest attacker techniques.

Industry:

Retail



Products:

- Breach and Attack Simulation (BAS)

About the company

The organization is a global retail group with stores, e-commerce and thousands of servers. Specialist security teams, from threat intelligence to endpoint protection, report to a quarterly security committee.

Challenges and Results:

- Red team exercises delayed for months by procurement**
→ Current attacker techniques simulated in-house, continuously
- No measured baseline for endpoint protection**
→ Endpoint protection measured, with ready-to-apply mitigations for each gap
- An IOC automation that wasn't working well**
→ Unblocked IOCs now go to the EDR automatically for blocking
- Threat intelligence with blind spots**
→ Picus AI Threat Builder adds data the intelligence team sometimes did not have
- Validation results that stayed with one team**
→ Findings shared across teams and the security committee

Problem:

Delayed Red Team Exercises, No Unified View, Broken Automation

"It is common for a red team exercise planned for February to be postponed until June due to delays in legal and procurement reviews. This represents a loss of time in testing tactics currently employed by attackers in real-time," said the Cybersecurity Lead.

Security is split across specialist teams, from email and web to endpoint protection on thousands of servers, with no single view of how their controls held up against real attacks. The incumbent breach and attack simulation tool did not run smoothly alongside the EDR, and an earlier IOC automation was also not working well.

"We had an automated process that was being executed. It was not functioning very well, ..." the platform owner said. The team focused on two priorities:

- Test the controls already in place against latest attacker techniques without waiting on a procurement cycle.
- Turn every unblocked threat into an action the right team, or an automation, can take.

Solution:

Continuous Validation Against Today's Attacks

The team ran a proof of concept to test whether Picus was mature enough to replace its incumbent tool, then deployed **Picus Breach and Attack Simulation (BAS)**.

The team deployed Picus BAS agents across each environment, from stores and Windows user machines to Linux and Windows servers, so every environment is measured against its own policies. Picus AI Threat Builder turns new threat intelligence into custom simulations, keeping tests in line with current attacker activity. A SOAR playbook takes every IOC that was not blocked and adds it to the EDR for direct blocking. Results reach the relevant security teams, and reports are pulled through the API for internal use.



"They download all IOCs that have not been blocked and automatically add them to the EDR for direct blocking. This part is complete," the platform owner said. The IOC automation that once fell short now runs end to end.

Outcome:

Continuous Validation and Red Teaming, Clear Gaps, Automated Fixes

The first measurements gave the endpoint team a clear baseline to work from, showing which gaps to fix, with ready-to-apply mitigations for each.

The response loop now runs without hand-offs. Every IOC that Picus shows was not blocked flows through the SOAR playbook into the EDR for direct blocking, taking over from the earlier IOC automation that had not worked well.

Measuring each environment against its own policies keeps every team focused on its own gaps. ***"The idea is to try to have a metric for each environment because each environment has its own different policies,"*** the platform owner said.

Picus AI Threat Builder also adds threat data that the intelligence team sometimes did not have.

Every simulation result maps to MITRE ATT&CK, the team's second priority after security control validation, and reports pulled through the API reach relevant security teams that own each control, as well as the quarterly security committee.

Instead of waiting months for a red teaming exercise, the organization now continuously tests its controls against today's attackers.



"For us, security control validation is the number one objective. But after that, I will say MITRE ATT&CK framework." The Cybersecurity Lead said.



Picus Security, a leading exposure validation company, **proves what attackers can exploit and what your defenses stop**, then closes real gaps with ready-to-deploy fixes and re-validates to confirm, at the machine speed today's AI threats demand. The Picus Platform spans [Breach and Attack Simulation](#), [Autonomous Penetration Testing](#) and [Exposure Validation](#), unified by [Picus Swarm](#), a swarm of AI agents that runs the whole validation loop continuously with human oversight. With 75+ integrations, it reaches across on-prem, hybrid cloud, and endpoint environments. Trusted by many Fortune 500 enterprises, Picus was named a 2026 Gartner Peer Insights Customers' Choice for Adversarial Exposure Validation and is recognized as an Innovation Leader in the Frost Radar for Automated Security Validation.