PICUS | Sutter Health

CASE STUDY

Sutter Health's Continuous Security Validation With Picus

Sutter Health strengthened cybersecurity by moving from manual testing to continuous, automated validation with Picus. Real-world attack simulations and SIEM/EDR integration cut validation from weeks to under an hour, improved team collaboration, provided real-time control visibility, and supported faster remediation, executive reporting, and HIPAA compliance.

About Sutter Health

Industry: Healthcare

Headquarters: United States

Number of Employees:
50,000 - 75,000

Products:

- Security Control Validation (SCV)
- Picus integrations with SIEM, EDR and threat intelligence platforms

Challenges:

- Manual testing slowed detection and response
- Limited visibility reduced insight into control effectiveness
- Limited ability to prioritize vulnerabilities and remediation
- Validation required significant manual effort, creating delays and siloed teams
- Rapidly evolving threats increased the scope and complexity of compliance obligations

Solutions:

- Automated simulations cut validation cycles from weeks to under an hour
- Real-time reporting clarified which controls worked, which failed, and why
- Actionable results enabled the team to address the highest-impact gaps first
- Automation and SIEM/EDR integrations freed teams from manual coordination and re-testing, and improved collaboration
- Continuous simulations with up-to-date threat intelligence supported proactive defense and HIPAA reporting

Results:

- Shorter validation cycles, cut from weeks to under an hour
- Real-time visibility into which controls work, which fail, and why
- Improved collaboration between Red Team and Detection Engineering
- Faster remediation and clearer executive reporting
- Continuous simulations supporting HIPAA compliance

> ***"We had the right tools and the right people," said Jaime Rodriguez, Manager of the Red Team, "but running tests, waiting for results, and revalidating could stretch over multiple weeks. We needed a faster and more consistent way to confirm that our defenses worked as intended."***

Business Challenge

Before adopting Picus, many testing and validation processes were manual. The red team spent days or weeks running simulations while Detection Engineering waited for results before tuning alerts. The process worked, but it was slow and resource-intensive.

With Sutter Health's large, distributed network, extensive partner ecosystem, and broad attack surface, cybersecurity remains an enterprise-level priority that demands both technological rigor and measurable assurance.

- **Manual Testing and Validation Processes**
  Many testing and validation processes were manual, with the red team spending days or weeks running simulations.
- **Slow, Resource-Intensive Workflows**
  Detection Engineering often waited for results before tuning alerts, making the process slow and resource-intensive.
- **Limited Real-Time Visibility Into Control Effectiveness**
  The lack of real-time visibility made it difficult to measure whether controls were performing effectively.
- **Difficulty Prioritizing Vulnerabilities and Demonstrating Improvement**
  Without timely validation results, it was challenging to prioritize remediation and demonstrate continuous improvement to leadership.

Solution Overview

Sutter Health adopted Picus Security Control Validation (SCV) to automate testing and improve collaboration across its cybersecurity functions. By integrating live threat intelligence feeds directly into Picus, Rodriguez and his team could design simulations that mirrored active adversary behavior.

Automation reduced manual workloads and enabled Detection Engineering to update and validate rules almost immediately. Picus integrated with Sutter's SIEM, EDR, and web application monitoring solutions, creating a single, correlated view of security posture and supporting faster, data-driven decisions.

- **Automated Security Control Validation**
  Real-world simulations replaced manual testing and accelerated validation cycles.
- **Real-Time Visibility**
  Reporting clearly shows which controls are effective, which fail and why.
- **SIEM and EDR Integrations**
  Integrations eliminate redundant testing and support faster remediation.
- **Executive-Ready Reporting**
  Quantifiable data from Picus reports appears in monthly operations reviews and executive summaries.

> ***"Instead of sending a manual request to our red team and waiting for results," Rodriguez explained, "I can enter the indicators into Picus, launch a simulation, and have a full report in about an hour."***

picussecurity.com

Experience Picus *in Action*

GET A DEMO

Gartner Peer Insights Customers' Choice 2025™

4.8/5.0

Highest-rated vendor*

Breach and Attack Simulation

*Gartner, Voice of the Customer for Adversarial Exposure Validation, Peer Contributors, 30 October 2025

WINTER 2026 G2 **Leader**

4.9/5.0

#1 Solution Provider*

Breach and Attack Simulation

*G2, Breach and Attack Simulation (BAS) Solutions, Winter Grid Report, 3 December 2025