CASE STUDY

LABYRINTH

LIFE SCIENCE & PHARMACEUTICAL R&D

Broader Detection No Additional SIEM Cost

3000+ Employees Distributed Global Infrastructure

SUMMARY

A global life sciences and pharmaceutical research organization expanded threat detection across internal infrastructure without scaling telemetry, building custom logic, or adding operational and engineering overhead.

With a mature security stack in place, the organization needed to expand detection coverage across the environment. The economics of doing this within the existing SIEM model were prohibitive: scaling telemetry collection to the required level would have cost a six-figure sum annually, before accounting for the engineering effort to build and sustain it.
LABYRINTH was introduced as a specialized detection layer. Detection coverage expanded. SIEM costs did not.

BETTER DETECTION ECONOMICS. BROADER COVERAGE. LESS OPERATIONAL OVERHEAD.

100 GB+
Daily telemetry that didn't need collecting

Minimized
Engineering and operational overhead

Six-figure
Annual spend avoided ~5× lower cost than the SIEM alternative

CLIENT

Operating across distributed R&D, laboratory, and enterprise environments, the organization manages intellectual property, scientific workflows, and business-critical systems that depend on consistent uptime and controlled access.

More than 3,000 employees rely on that infrastructure daily.

Its security stack was already mature. SIEM, EDR, NGFW, and centralized monitoring were in place and working as intended. The gap was not in what the stack could see. It was in what expanding that visibility would cost to sustain.

CHALLENGE

Two detection gaps needed closing: reconnaissance and service discovery activity inside the internal network, and identity-focused attack techniques targeting Active Directory. Both were solvable within existing SIEM infrastructure. Neither was solvable at a justifiable cost.

Achieving the required visibility through conventional telemetry expansion meant collecting over 100 GB of additional data per day, writing and maintaining custom detection logic, deploying canary assets across the environment, and absorbing the ongoing engineering load to keep it current. The security team also needed to scale SIEM capacity by 2 to 2.5 times its current size.

info@labyrinth.tech

labyrinth.tech

CASE STUDY

LABYRINTH

REQUIREMENT	SIEM SCALE-UP PATH	LABYRINTH PATH
TELEMETRY VOLUME	100 GB+ per day, additional	No increase required
DETECTION LOGIC	Built and maintained internally	Supported out of the box
INFRASTRUCTURE SCALE	SIEM capacity ×2 to ×2.5	No SIEM changes
AD VISIBILITY	Full telemetry centralized	Local processing, relevant events only
ANNUAL COST	Six-figure increase	~5× lower

SOLUTION

The organization reframed the decision. Instead of scaling existing infrastructure, the question became whether a purpose-built detection layer could deliver the same outcome without the significant cost, time, or engineering resources that building and sustaining that capability internally would demand. Instead of scaling telemetry collection, the organization scaled certainty. LABYRINTH became that layer, deployed to detect where existing infrastructure could not reach.

Two workstreams were addressed:

1

Internal network detection

LABYRINTH decoys deployed across internal infrastructure to surface reconnaissance, service discovery, and unauthorized exploration. Detection generated through direct interaction with deception assets. No additional telemetry collection. No correlation rules to build or sustain.

2

Identity and Active Directory

Suspicious activity on domain controllers analyzed locally. Only relevant security events forwarded for centralized investigation. Full visibility into identity-focused attack techniques without centralizing full Active Directory telemetry volume.

RESULTS

Broader detection coverage

Reconnaissance, service discovery, and identity-focused attack techniques visible across the environment. Coverage expanded without expanding infrastructure.

Six-figure annual cost avoided

Full detection coverage delivered across the environment. SIEM infrastructure unchanged. Telemetry volume unchanged.

Confirmed signals, not correlation scores

Interaction with a decoy is a confirmed threat. Analysts act on evidence with full investigation context, not alert queues to triage.

No added engineering effort

Detection logic is supported out of the box rather than built or maintained internally. Integrated with existing security workflow from deployment. The security team gained coverage, not overhead.

info@labyrinth.tech

labyrinth.tech