RAPID7

CUSTOMER STORY

**Industry**
Education

**Region**
Americas

**Company Size**
Enterprise (Large)

**Products**
Deployment Services, InsightConnect, and InsightIDR

# STREAMLINING THREAT DETECTION AND ENHANCING SECURITY OPERATIONS WITH RAPID7

UNIVERSITY OF RICHMOND

# OVERVIEW

**The University of Richmond, a private liberal arts institution founded in 1830, fosters an environment where liberal arts intersect with acclaimed schools of law, business, leadership studies, and continuing education. With an enrollment of around 4,000 undergraduate and graduate students, Richmond is committed to providing an outstanding student experience through integrated coursework, hands-on research, creative expression, and experiential learning, empowering students to make a significant impact both on campus and beyond.**

Richmond's commitment to providing a forward-thinking, student-centered education extends beyond academics to include a secure digital environment essential for today's tech-driven educational landscape. Led by John Craft, Director of Information Security, and Robert Baskette, Security Analyst, Richmond's dedicated and highly-experienced cybersecurity team safeguards the university's digital operations, ensuring a safe learning and research environment for the entire campus community.

+

**LIBERAL ARTS**

**PRIVATE INSTITUTION FOUNDED IN 1830**

**WITH AN ENROLLMENT OF AROUND 4,000 UNDERGRADUATE AND GRADUATE STUDENTS**

# THE CHALLENGE

### Operating Without a SIEM: Navigating Blind Spots

Before adopting Rapid7, Richmond's security team lacked a centralized Security Information and Event Management (SIEM) system, creating gaps in visibility across their network. Logs were scattered across servers with no streamlined way to correlate events, detect threats, or gain insight into security incidents. Craft described this fragmented approach as "flying blind," lacking a cohesive view to detect and respond to threats in real time.

> **"We were essentially flying blind. Without a SIEM, we couldn't see the bigger picture, which made it difficult to detect and respond to threats in a timely manner."**
>
> John Craft, Director of Information Security at the University of Richmond

Without a SIEM, Richmond's team was forced to rely on manual processes for threat detection, combing through individual log files and cross-referencing data across sources. This time-intensive and inefficient process limited their ability to detect complex threats and respond quickly to incidents, posing challenges to secure Richmond's sensitive information. As Craft noted, "We were essentially flying blind. Without a SIEM, we couldn't see the bigger picture, which made it difficult to detect and respond to threats in a timely manner."

### Breaking Free from a Cumbersome Security Process

Manual processes for log management further hampered Richmond's security operations. Logs were stored on a basic syslog server, limiting correlation capabilities and requiring team members to jump between systems to document findings.

**THE LACK OF INTEGRATION ACROSS VARIOUS LOGS MADE IT DIFFICULT TO SEE CORRESPONDING ACTIVITY ACROSS SYSTEMS, INCREASING RICHMOND'S VULNERABILITY AND HAMPERING INCIDENT RESPONSE CAPABILITIES.**

# THE SOLUTION

## Finding the Perfect Fit

Richmond's search for a robust security solution began with a Request for Proposal (RFP) process, inviting five top SIEM vendors to demonstrate their solutions.  After thorough evaluations, including in-person demos and a proof of concept, Rapid7's InsightIDR and InsightConnect emerged as the clear winners.

## Standing Out from the Competition

Rapid7 distinguished itself with competitive pricing, comprehensive capabilities, and exceptional support throughout the proof-of-concept phase.

> **It [InsightIDR] was a top tier product, worked really well, and met all of our requirements. And the Rapid7 team was great to work with."**
>
> John Craft, Director of Information Security at the University of Richmond

InsightConnect's built-in Security Orchestration, Automation, and Response (SOAR) capabilities and seamless integration stood out, eliminating the need for additional purchases or complex setups. This all-in-one approach provided Richmond with an effective, easy-to-implement solution to streamline its security processes.

## Streamlining Security with Rapid7

With InsightIDR, Richmond gained a centralized platform to collect and correlate logs across various systems, eliminating the challenges of fragmented visibility and manual processes. InsightIDR's user-friendly interface allowed the team to quickly access and analyze activities such as login attempts, firewall logs, and intrusion detection system data. Rapid7's platform enabled faster, more efficient threat detection and incident response.

InsightConnect further enhanced Richmond's security by automating repetitive tasks and orchestrating workflows across tools. This accelerated time-consuming processes, allowing the team to focus on critical tasks faster. The SOAR capabilities streamlined incident response, enriching alerts with external data and making threat detection more  efficient.

# THE RESULTS

## Faster Threat Detection and Real-Time Security

Implementing Rapid7's solutions led to a significant boost in Richmond's security operations. Tasks like tracing VPN login activity, which previously took hours, now take just minutes. As Baskette stated, "This used to take me two or three hours manually. Now, it takes about 10 minutes with Rapid7." This substantial reduction in investigation time allowed the information security team to reallocate resources and time to more strategic tasks, like proactive threat hunting and fine-tuning alert configurations.

Rapid7's real-time alerting and response capabilities have improved Richmond's ability to swiftly detect and respond to threats. Baskette added, "The SIEM allows us to detect things and correlate in near real time." With this proactive approach, identifying compromised accounts or other security issues became faster and more accurate, strengthening Richmond's overall security posture.

## Expanding the Security Net

Richmond's information security team continues to expand log coverage, integrating additional applications and refining automation workflows. "We're adding more systems to the SIEM all the time," Craft said, "and working on tuning it so we only get alerts that matter." The next phase will include more complex integrations, such as connecting web servers with sophisticated log formats and streamlining responses to third-party services.

## The Future Is Secure with Rapid7

By adopting Rapid7, Richmond transformed its cybersecurity approach, shifting from  reactive to proactive threat management. As Craft succinctly put it, "You can't secure what you're not aware of." Rapid7 has not only enhanced Richmond's threat detection capabilities but also established a foundation for ongoing security improvements, empowering the institution to confidently protect its community's data.

Looking ahead, Richmond plans to expand log coverage and automate additional tasks with Rapid7, setting a high standard for cybersecurity in higher education. Rapid7 is here for that..

> **"This used to take me two or three hours manually. Now, it takes about 10 minutes with Rapid7."**
>
> Robert Baskett, Security Analyst at the University of Richmond

## Recommending Rapid7 to Other Universities

Richmond's positive experience has led its information security team to actively recommend Rapid7 to other universities. Craft shared , "I've recommended the product to several other universities that I know that were looking for either their first SIEM or looking at potentially replacing their existing SIEM." He highlighted Rapid7's comprehensive features, user-friendly interface, and predictable pricing model as standout advantages. Unlike vendors with variable pricing based on data volume, Rapid7 offers consistent costs, making it particularly appealing to budget-conscious institutions. With its powerful capabilities, ease of use, and cost-effectiveness, Rapid7 has become a preferred choice for higher education institutions aiming to strengthen their security posture.

> **"I've recommended the product to several other universities that I know that were looking for either their first SIEM or looking at potentially replacing their existing SIEM."**
>
> John Craft, Director of Information Security at the University of Richmond

## About Rapid7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open source communities and cutting-edge research–using these insights to optimize our products and arm the global security community with the latest in attacker methodology. Trusted by more than 11,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.

**View more success stories.**

**CUSTOMER STORIES**

RAPID7

**PRODUCTS**

Cloud Security
XDR & SIEM
Threat Intelligence
Vulnerability Risk Management
Application Security
Orchestration & Automation
Managed Services

**CONTACT US**

rapid7.com/contact

To learn more or start a free trial, visit:
rapid7.com/try/insight