RAPID7

CUSTOMER STORY

OUTNUMBERED? NEVER OUTPACED: HOW SOCS TOOK COMMAND WITH RAPID7

STREAMLINING THREAT DETECTION AND ENHANCING SECURITY OPERATIONS WITH RAPID7

UNIVERSITY OF RICHMOND

Industry	Company Size
Education	Enterprise (Large)

The University of Richmond is a private liberal arts institution founded in 1830, with around 4,000 undergraduate and graduate students. Its academic reputation spans law, business, leadership studies, and continuing education. To protect this environment, Director of Information Security John Craft and Security Analyst Robert Baskette lead a dedicated cybersecurity team responsible for safeguarding digital operations and ensuring a secure campus learning and research experience.

What changed

Before adopting Rapid7, the university lacked a centralized Security Information and Event Management (SIEM) system. Logs were scattered across servers, making it difficult to correlate events or detect threats. As Craft described, the team was “flying blind” without a cohesive view of their environment.

Manual processes for log management and investigation were time-intensive, often requiring hours to trace a single activity. The university recognized it needed a modern SIEM to unify visibility, reduce blind spots, and accelerate incident response.

The Rapid7 MDR experience

Following a competitive RFP process with five SIEM vendors, the university selected Rapid7’s next-gen SIEM and automation solutions for their comprehensive capabilities, competitive pricing, and outstanding proof-of-concept support.

The next-gen SIEM provided a centralized platform to collect and correlate logs across diverse systems, giving the team a clear, real-time view of activity. Its intuitive interface allowed quick analysis of login attempts, firewall logs, and intrusion detection system data, turning fragmented visibility into actionable intelligence.

With Rapid7's automation solution, the university automated repetitive tasks and orchestrated workflows across tools, streamlining processes and accelerating response times. Together, the solutions transformed their approach, enabling faster detection, efficient response, and stronger overall security operations.

> It [next-gen SIEM] 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**

RESULTS AT A GLANCE

- Hours of manual investigation reduced to minutes
- Real-time correlation of logs and faster detection
- Automated workflows
- Centralized visibility across systems and applications
- Cost-effective SIEM with predictable pricing

Built for what's next

With Rapid7, the University of Richmond shifted from reactive to proactive threat management. Investigations that once took hours now take minutes, freeing the team to focus on strategic tasks like threat hunting and tuning alerts. As Baskette noted, "This used to take me two or three hours manually. Now, it takes about 10 minutes with Rapid7." The University of Richmond continues to expand SIEM coverage and automation, confident in a scalable foundation for future needs. Rapid7's predictable pricing and comprehensive features have made it a recommended solution to other universities seeking to modernize their SIEM.

> 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**

READY TO OUTPACE EVERY THREAT?

See how Rapid7's AI-powered SIEM helps SOCs adapt faster, cut through noise, and command with confidence.

LEARN MORE

REQUEST A DEMO

Exciting News: The next-gen SIEM functionality described in this case study is a core component of the recently announced Incident Command, which adds Attack Surface Management to provide SOC analysts with complete visibility into the entire threat attack surface.

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.

RAPID7

SECURE YOUR

Cloud | Applications | Infrastructure | Network | Data

ACCELERATE WITH

Command Platform | Exposure Management | Attack Surface Management | Vulnerability Management | Cloud-Native Application Protection | Application Security | Next-Gen SIEM | Threat Intelligence | MDR Services | Incident Response Services | MVM Services

SECURITY BUILT TO OUTPACE ATTACKERS

Try our security platform risk-free - start your trial at **rapid7.com**