gravwell | GONZAGA UNIVERSITY

CASE STUDY

Gonzaga University

Gonzaga University, nestled in Spokane, Washington, stands as a beacon of academic excellence and holistic education. Founded in 1887 Gonzaga embodies a rich tradition of Jesuit values, fostering a community that prioritizes intellectual growth, social justice, and service to others.

With a commitment to educating the whole person, Gonzaga offers a diverse range of undergraduate, graduate, and professional programs, emphasizing critical thinking, ethical leadership, and global engagement.
Renowned for its tight-knit community and vibrant campus life, Gonzaga instills a passion for learning, encourages dialogue across disciplines, and prepares students to become compassionate, ethical leaders in an ever-changing world.

THE CHALLENGE

Too Little Value Out of Traditional SIEM

The Gonzaga security team was relying heavily on a traditional SIEM. The solution had been in place for several years but had never fully been implemented or adopted by the wider team due to difficulties collecting the breadth of log sources, the time required to maintain the deployment, and grappling with how the architecture should be arranged in their environment.
The outcome was a very expensive solution, that did not achieve Gonzaga's organizational goals and the time spent to fix these issues was unacceptably high.

LACKING VISIBILITY

The Gonzaga team needed a centralized location that provided visibility into all of their logs. The team needed to know what they were looking at and what they were defending.
The team wanted a solution to future-proof their security program. That provided them with complete visibility, did not punish them for collecting more data and empowered them to hunt and identify anomalous behavior

HOW DO WE SPEND OUR BUDGET MORE EFFECTIVELY?

Upon initial deployment, every department used the traditional SIEM at one point. With the challenges identified the engagement and use reduced over time leaving senior leadership asking the question…

HOW DO WE DEPLOY OUR BUDGET MOST EFFECTIVELY?

The team wanted a tool that worked for them. They needed a SIEM that delivered on the value articulated at purchase and at a price that was commensurate with that value creation.

INDUSTRY

University

YEAR FOUNDED

1887

LOCATION

Spokane, Washington

COMPANY SIZE

1001-5000

SERVICE

Gonzaga University, nestled in Spokane, Washington, stands as a beacon of academic excellence and holistic education.

SOLUTION

Log Analysis, SIEM, Detection & Response

THE SOLUTION

To assess Gravwell's impact we spoke with Angel Alvarez, Security Engineer and Primary Gravwell user at Gonzaga Univeristy.

STREAMLINED ALERT HANDLING

In our IT environment, grappling with numerous alerts, from password resets to firewall actions, was a challenge. Gravwell has streamlined and consolidated these alerts, offering a clearer view of our security landscape. This shift has been crucial in distinguishing and prioritizing critical alerts that were previously buried in a flood of emails. With Gravwell, we've gained better control over logs and alerts, significantly improving our incident response capabilities.

ENHANCED REPORTING CAPABILITIES

Gravwell has empowered our team to generate detailed reports, critical for overseeing our distributed IT department. Daily reports on user changes, coupled with weekly reports on computer objects, provide a comprehensive overview of our system. Uncovering instances of business operations failures through improved observability has been a noteworthy achievement. Gravwell's reporting capabilities have become an essential tool in our proactive security approach.

USER-FRIENDLY TRANSITION

The shift to Gravwell has been transformative for our university cybersecurity team. Gravwell's intuitive interface and user-friendly design have addressed a critical need for enhanced observability in our medium-to-large IT environment. Its simplicity is particularly advantageous in an IT landscape where not everyone is keen on dev ops activities. As someone who enjoys tinkering and scripting, I found Gravwell's setup to be straightforward, allowing us to adapt quickly.

EFFECTIVE INCIDENT RESPONSE

A specific incident involving a brute force attempt on the admin account showcased Gravwell's effectiveness. Utilizing a resource template in Gravwell, we efficiently plugged in the username, allowing us to extract and analyze relevant logs promptly. This incident response capability has proven invaluable in addressing security threats swiftly and effectively. Gravwell's contribution extends beyond incident response to comprehensive monitoring of firewall and config changes, as well as intrusion prevention system (IPS) activities.

PROACTIVE SECURITY MEASURES AND UNFORESEEN DISCOVERIES

Gravwell has allowed us to shift from a reactive to a proactive security stance. Tiered accounts and notifications for password resets have significantly enhanced our security posture. An unexpected benefit was uncovering students misusing Tier 1 accounts to reset other students' passwords – a clear red flag that we promptly addressed. Gravwell's ability to reveal such unexpected patterns has added a layer of security awareness we didn't initially anticipate.

THE RESULT

A Small But Mighty Security Team

With Gravwell's ability to create a unified view of your environment and no limits over the questions you can ask of your data all within a pricing structure that you control Gonzaga's security team created an automated, systematic, repeatable, predictable, and shareable approach to security that improves their overall security posture.

GONZAGA UNIVERSITY

Gravwell is easy to configure, easy to set up, and easy to architect. You get a lot more bang for your buck when compared to other tools on the market. Even with a lean team, you can make use of Gravwell

Angel Alvarez

Security Engineer at Gonzaga University