Published on *University of Colorado* (https://www.cu.edu)

CU I&E Submission: Multicampus Security Log Monitoring [1]

Category

Technology

Submitted By

David Capps, david.capps@cu.edu [2], Chief Information Security Officer

Project Team

Sarah Braun, sarah.braun@colorado.edu [3], Information Security Officer
Sean Clark, sean.clark@cuanschutz.edu [4], Information Security Officer
Chris Edmundson, chris.edmundson@ucdenver.edu [5], Security Operations Manager
Scott Maize, scott.maize@colorado.edu [6], Associate Director of Information Security
Charlotte Russell, charlotte.russell@cuanschutz.edu [7], Assistant Vice Chancellor for IT Security and Compliance
John Scudder, john.scudder@colorado.edu [8], Security Operations Program Manager
David Capps, david.capps@cu.edu [9], CU Chief Information Security Officer
Brad Judy, brad.judy@cu.edu [10], CU Deputy Chief Information Security Officer
Cindy Kraft, cindy.kraft@cu.edu [11], UIS PMO Team Manager
Keith Lehigh, keith.lehigh@cu.edu [12], Information Security Officer
Steve Thormod, steve.thormod@cu.edu [13], Principal Project Manager

Project Description

One of the core functions of the information security teams at CU is to monitor CU IT systems for signs of attacks and potentially malicious behavior. A critical tool in our monitoring work is a Security Information and Event Monitoring (SIEM) system, which allows our teams to keep an eye on tens of thousands of log events generated by CU IT systems every second, a task that would be impossible without advanced, automated tools.

Multiple CU information security teams joined together through our multicampus CU Security+ group to select, procure and deploy a new SIEM system that would enable us to be more effective and efficient in protecting CU from cybercriminals. The CU Security+ group provides a forum for separate security teams to work together for mutual benefit. The teams chose to collaborate across campuses to take advantage of efficiencies from sharing knowledge and experiences.

Project Efficiency

Using a vendor-managed tool allowed us to spend our work hours on using a tool effectively and not chasing down hardware issues and managing software update processes. A tool that once distracted us from our core work is now empowering us to do more.

The team also partnered with the CU Procurement Service Center to identify the most cost effective and efficient process for acquiring the new service, including working to connect CU with a new pricing agreement that can be leveraged across CU.

Project Inspiration

The inspiration for the project was a group consensus that our prior log monitoring tool and processes had become a major limiting factor in CU's ability to move our information security abilities forward. Team members spent long hours on technical problems and limitations of our prior solution, sometimes needing to wait days for a search to complete. It became a daily frustration and distraction from our core duties to protect, detect and response to threats to CU IT services. We wanted to empower and focus our teams on work that best used their talents.

What Makes You Happiest about this Project?

Information security teams at CU are now able to focus more of their time on using their skills and expertise to protect CU IT services and data. Since implementing the new system, teams have already rolled out new detections that have alerted CU to attacks against employee payroll, VPN services, and more. The speed of searches has also made team members much more efficient, with results returned in seconds instead of hours.

Additional Information

Source URL:https://www.cu.edu/controller/i-e-awards/past-submissions/cu-ie-submission-multicampus-security-log-monitoring

Links
[1] https://www.cu.edu/controller/i-e-awards/past-submissions/cu-ie-submission-multicampus-security-log-monitoring [2] mailto:david.capps@cu.edu [3] mailto:sarah.braun@colorado.edu
[4] mailto:sean.clark@cuanschutz.edu [5] mailto:chris.edmundson@ucdenver.edu
[6] mailto:scott.maize@colorado.edu [7] mailto:charlotte.russell@cuanschutz.edu
[8] mailto:john.scudder@colorado.edu [9] mailto:David.Capps@cu.edu [10] mailto:brad.judy@cu.edu
[11] mailto:cindy.kraft@cu.edu [12] mailto:keith.lehigh@cu.edu [13] mailto:steve.thormod@cu.edu