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

Strengthening cybersecurity: CU teams unite to form CU Security+ and implement a SIEM solution [1]

June 28, 2024 by UIS Communications [2]

ETA: Congratulations to team members, Sarah Braun, Scott Maize, John Scudder, Charlotte Russell, Sean Clark, Chris Edmundson, David Capps, Brad Judy, Keith Lehigh, Cindy Kraft and Steve Thormod, recipients of one of the four 2024 CU Innovation & Efficiency Awards [3]! The awards recognize CU employees whose ideas and innovations save the university time, money and resources.

Protecting the University of Colorado's critical data is a top priority for every CU campus and CU System. Information security officers monitor CU IT systems for signs of attacks and suspicious behavior using a Security Information and Event Monitoring (SIEM) system. SIEM solutions allow teams to monitor thousands of log events generated by CU applications every second, an impossible without advanced automated tools.

Multiple CU information security teams united to form CU Security+, a forum for separate security teams to work together for mutual benefit. The teams collaborate across campuses to maximize efficiency from shared knowledge and experiences.

CU Security+ tackled the challenge of finding and implementing a new SIEM tool that would more effectively correlate data from multiple origins, offer visibility into CU's complex network, create meaningful alerts and aid in the investigation of potential threats.

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.

The previous hardware and service issues are now gone. The new cloud-based SIEM solution now allows Information Security teams to focus more of their time on using their skills and expertise to protect CU IT services and data.

"The performance of the new tool is so much better … something that would take hours to run now takes about a minute," said Brad Judy, CU deputy chief information security officer.

Judy shared his enthusiasm for the multi-campus collaboration as each team leverages the new monitoring tool. "We can share things we're learning, exchanging notes on things that

worked well and problems we encountered that we found solutions to — so others don’t have to go down the same path.”

Since implementing the new system in 2023, teams have already rolled out new detections that have alerted CU to attacks against employee payroll, VPN services and more.

CU Security+ members and others involved in the project include Sarah Braun, CU Boulder information security officer (ISO), Sean Clark, CU Anschutz Medical Campus ISO, Chris Edmundson, CU Denver security operations manager, Scott Maize, CU Boulder associate director of Information Security, Charlotte Russell, assistant vice chancellor for IT Security and Compliance, John Scudder, CU Boulder security operations program manager, David Capps, CU CISO, Brad Judy, CU deputy CISO Keith Lehigh, CU System information security officer, and two UIS project managers, Cindy Kraft and Steve Thormod.

Display Title:
Strengthening cybersecurity: CU teams unite to form CU Security+ and implement a SIEM solution
Send email when Published:
No

Links
[1] https://www.cu.edu/blog/uis-news/strengthening-cybersecurity-cu-teams-unite-form-cu-security-and-implement-siem [2] https://www.cu.edu/blog/uis-news/author/65709
[3] https://www.cu.edu/controller/news/office-university-controller-news/june-27-2024-edition/cu-innovation-efficiency