



Staying on Top of Cybersecurity: A Conversation with Two University CISOs

In this interview Tom Dugas, chief information security officer for **Duquesne University**, and Rick Haugerud, CISO for the **University of Nebraska-Lincoln**, explain how Internet2's NET+ program is helping them manage cybersecurity for their institutions.

How are your institutions involved with Internet2 and the NET+ security program?

TOM DUGAS: I'm most involved in working with the **NET+** program by both purchasing software and services through the NET+ agreement, and also helping to bring new services to the forefront for the benefit of other institutions, such as with the **Cloud Scorecard** initiative. Part of my role is to work with the Internet2 team to help them understand what needs we have in the community and, where it's necessary, to sponsor important service providers. Other people on my staff are involved in the NET+ Splunk advisory board, which is another vehicle for our voices to shape the direction of the program.

One of the things that happens as part of the community-led effort is that it helps shepherd a corporation or company through what we call a service evaluation effort, in which we actually make sure the service is fit-for-purpose, available, secure and evaluated for the rest of the community. So, rather than having 100 universities do the evaluation of one single service independently on their own, which is what we did for many, many years, we decided that we would do that as a coordinated effort among our universities so we could benefit from each other's knowledge and expertise.

RICK HAUGERUD: Participation in NET+ also offers that unified front and gives us a feedback loop directly into those vendors, so we can talk about things that are specific to the higher ed environment. It might be important integrations with other academic applications, terms or something else. The NET+ team sponsors an advisory board with all of these firms, that really gives us a seat at the table as they decide on future service features and the audiences they are going to impact. As individual universities, we don't get that opportunity.

What are some of security technologies that you have acquired through this relationship?

RICK: The first one that comes to mind is **Splunk**. Splunk is where we consolidate the machine logs and authentication logs for all of the systems at the university. If we were to have some type of a security event, we'd go into that system to identify what happened on this particular day at this particular time. For our centralized log management correlation system, we had a very small Splunk instance – somewhere between 10 and 30 gigabytes – and we needed to expand that. A number of our peers put together a service evaluation for log management using Splunk. Having other schools already doing that helped not only in terms of what they were buying but for the price they were paying. When that was done, I was able to expand that license to several 100 gigabytes in order to meet our needs.

Then, during the pandemic, the first week that we went live with full remote learning and remote work we knew that the legacy VPN we had installed was not going to hold up. So, we had to identify something that allowed us to scale service up and down as we needed it. We were able to take advantage of **Palo Alto Network's Prisma Access**, which was in the service evaluation process and is now available in the **NET+ Palo Alto Networks program**.

TOM: We have nine security-related NET+ services in operation at the university in some way, shape or form. When the pandemic hit, it caused us to rethink a lot of things we were doing. As our students and our employees went off campus, our ability to secure the identities of our people on campus really became critical. And so, everything we did worldwide – and I say worldwide because we have students now coming and connecting internationally to our services – was coming in through our identity access management system with **Duo Security**.



What have you learned in the last year that has been really important to keeping students, staff and faculty secure?

RICK: In March 2020, I was feeling more comfortable in terms of what our border looked like and the things that we were protecting our constituents from. Then the pandemic happened and people started grabbing devices off of their desks and old laptops out of storage closets and dragging them home to put on home networks – and who knows how they were being secured, if they were being secured at all. I thought I had a fairly good plan in place and tools deployed across my infrastructure to protect us, but that was all out the window.

And so, over the last year we've been looking at services and products we can deploy that will protect our users as well at home as we could when they were on campus. And there's nothing like having a community of your peers to have those conversations with and to learn what they're doing, how long it took them to get there, what bumps they ran into along the way and ultimately, how they were able to steer around those. That's significantly beneficial to all of us, and that is a huge value of participating with Internet2 overall and through the NET+ program for specific cloud and security solutions.

TOM: Last March, for about the first three weeks – for the only time in Duquesne history – we had the most secure network we ever had and ever will have again in the history of the university – because no one was there. And because of that, the user perspective of risk was gone. We were able

to use our analytics and our posture to understand what was happening on our network, why it was happening and what risks we were seeing that we hadn't been noticing because of the volume of traffic. And we were able to really identify a lot of risks that we would never have seen in the past and we were able to patch them and remediate them quickly.

Also, we have seen the reliance of third-party integrations go up drastically. I am equally as concerned about how we have to engage with our vendors and constituents the same way we do our own campus. And so now my job is not just to be the CISO for Duquesne; it's almost to act as the CISO for the 200 or 300 third-parties that we engage with and share institutional private and restricted data with – that we need to treat the same way I do my people on campus and my systems on campus. That is a daunting task for a university.

And NET+ is helping you make that possible?

TOM: The service evaluation effort that we collectively perform helps us bring those products to market faster and more efficiently than we could ever do on our own. And, we do it with a trusted perspective that a number of our peers have all reviewed and assessed. Do we think it will be 100% of the way we would do it? Maybe not, but we could finish that 10% at our own institutions. But that 90% really helps us bring that product to market faster and helps us provide such a valuable service for our community collectively. Without NET+, and the mechanism it provides to deliver services, it would be a lot harder for all of us collectively. It's invaluable.