Arctic EWS research paper

A strong case for the utility of cybersecurity monitoring in higher education

Arctic Security

EDUCAUSE

Table of contents

Arctic Security

EDUCAUSE

Executive summary

Cybersecurity is an increasingly important issue in higher education. There is clear demand for security solutions that are both accessible and effective at defending academic infrastructure. Arctic Security and EDUCAUSE have therefore been working as partners on a joint project whose goal is to establish the utility of external cybersecurity monitoring for higher education, and to identify services that could be made easily accessible and boost the cyber defenses of the association's members.

A serious security breach can cause significant damage, but most higher education institutions have restrictive limits in both staff and budget, which forces them to make tough decisions on which defensive measures can be taken. This is a dilemma, as the costs of cybersecurity insurance are quickly rising. What is the most effective way to defend the organization?

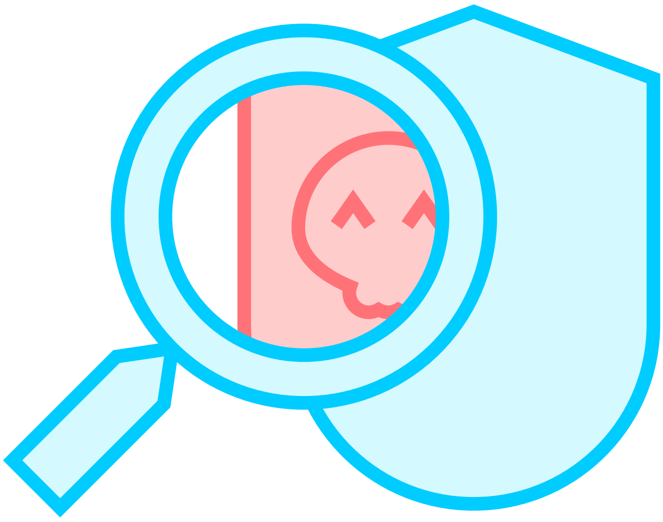
ARCTIC EWS, AT A GLANCE

- Early Warning Service (EWS)
- Cost-effective, low-overhead continuous cybersecurity monitoring service
- Reveals how porous firewalls are, leads to improved rule management
- Highlights security policy problems that tend to remain invisible
- Saves 5-20 hours per week of analyst work, in addition to training time
- Provides a clean bill of health for management and cyber-security insurance companies
- Finds problems with assets that have long been forgotten

Why is this so important to address?
One of the project participants put it well:

> *"For every single PII record lost, each record costs about $150 to remediate according to the Verizon Breach Report. Universities have thousands and thousands of alumni. So if you do the math, even with our cyber insurance, the financial impact of a breach could be staggering. So in that perspective, a breach could seriously impact any organization. I want to be the one that says I have done everything in my potential to prevent risks of the university."*
>
> **— Tom Dugas, CISO, Duquesne University**

This joint research project of Arctic Security and EDUCAUSE has produced a wealth of interesting findings. We saw systemic problems related to firewall management, established security processes, processes related to incident response, change management, vulnerability management, asset management, and stakeholder communications during the project. Several project participants noticed security posture differences between campuses. Many of these issues are straightforward to address, but they can go unnoticed without external monitoring.



A typical university has excessively porous firewalls and issues with firewall rule management. Most of the research project participants found that they could significantly improve their security posture by adjusting their firewall policies, pruning rules, and have made plans for a less firewall-dependent architecture, such as zero-trust networks.

Network asset re-use policies are a common challenge for many universities, which shows up in external moni-to-ring. Assets that pop up in monitoring are often repurposed systems, and the issue is also linked with firewall policy management. The more research-heavy the institution is, the more likely it is that systems are just deployed to the network without any awareness by the security team. As they get tagged in external monitoring, many of these are databases, which increases the odds of data leakage.

External security monitoring highlights security policy problems that otherwise tend to remain invisible, such as communications issues between cybersecurity and IT functions. Security teams struggle to keep up with IT and are often stuck playing catch-up. The importance of a systematic vulnerability management process becomes plain to see with external monitoring, which also serves as a good starting point for addressing the problems and improving internal communication with stakeholders.

Project participants determined that **data processing done by Arctic EWS is worth 5-20 hours of analyst work per week**, depending on the institution, plus the time and cost of staff training and infrastructure maintenance. A security team member could perform the work, but in practice, **dedicating that amount of time and finding the staff to do it are both difficult obstacles to overcome**. Participants also noted that producing a clean bill of health can be particularly beneficial in the future when negotiating cybersecurity insurance policy costs. **It's important emphasize on the verification of vulnerability fixes after they have been applied.** Otherwise, security problems may pop up again unexpectedly for various reasons, such as when a security fault is present in source images for services running in a virtual environment. Some project participants established the practice of performing verification scanning internally after notifying the asset owner to confirm that the issue was resolved.

External notifications also highlight issues that many universities have with network asset management and asset ownership documentation. Several project participants had trouble locating the vulnerable systems in their networks, which is a severe handicap and will cause problems in a crisis situation. However, working through notifications is a great way to begin the systematic documentation of the network, and they are useful for establishing better communication with various internal stakeholders.

External cybersecurity monitoring is one tool in your toolbox. It will not solve all the security problems for your organization, and it definitely does not catch everything. Every university needs a layered in-depth defense that consists of several security technologies. But **this approach does contribute in many ways, and it is helps spot mistakes and problems in security processes and in the rest of the security technology stack.** Sometimes it is the tool that can save your bacon.

Background

Arctic Security is a Finnish cybersecurity company that supports national cybersecurity authorities through the use of its national-scale incident notification platform. After showing the benefits of such systems in critical infrastructure space, Arctic Security is now focused on bringing these capabilities to a broader audience of MSSPs, enterprises, and higher education.

EDUCAUSE is a nonprofit association in the United States whose mission is "to advance higher education through the use of information technology". EDUCAUSE has a member base of over 2,000 higher education institutions.

Project participants are EDUCAUSE members from R1, R2 and M1 universities in USA.

Project design

The research project spanned three months, from July 15 to October 15, 2021. Participant onboarding was done in the weeks leading up to the project and included a number of steps. First, participants completed a form where they described the networks they wished to have as part of the project. Arctic Security provided open-source asset discovery assessments, from which the participants could choose to include additional network assets, and many of the universities did do so. Participants then received a six-month historical report of security issues seen in matching with their network assets.

The notification categories were suspected compromise, vulnerable services, and open services. Every day, participants received notifications of the previous 24 hours of aggregated events. The Shadowserver foundation was promoted as an additional data source, and participants could register and include the Shadowserver reports to the Arctic EWS reporting during the project.

Each participant was given a random letter code from A-J, used in the diagrams and descriptions to keep the participant's information confidential.

Arctic EWS delivered notifications either through emails or configurable API endpoints. Participants started with the emails and could choose to use the APIs, and they could integrate their notifications with case management systems where applicable. Notifications were tagged based on their reported network types if they provided that information.

The participants were tracked over the study period to observe what effect taking action on the notifications had on their external security posture, from the perspective of Arctic EWS. Improving security at this scale usually means long-term work, and it took about a month until changes became visible. Figure 1 shows how the participants compare with each other in terms of observed vulnerable services. The data has been normalized by taking into account the student population of each university.

The project participants can be roughly divided into three groups. The first group (greens) had a low rate of observations and a downward trend over the project. The second group (blues) clustered around the average rate of observations and followed the overall trend. The third group (reds) had such a large number of observations that they stood out from the rest. Two of the three participants in this category were not actively engaging in the project and weren't available for interviews at the end. Presumably, they didn't have time to work with the notifications sent to them.

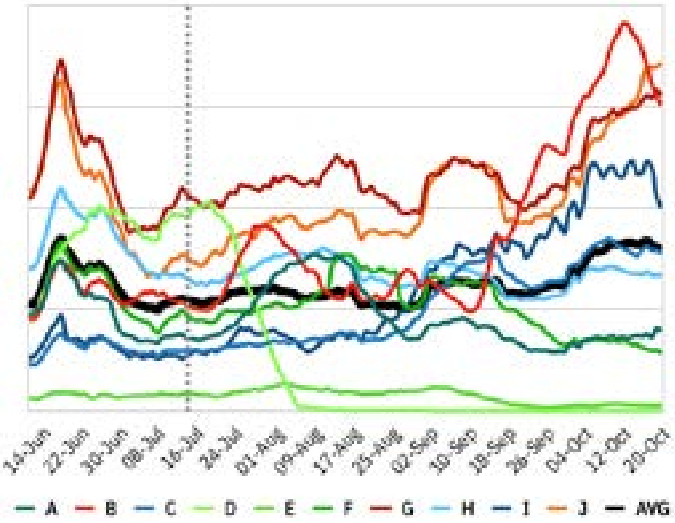


Figure 1: Reported vulnerable services per day, adjusted to student population

Identifying vulnerabilities

> *"EWS is helping us to identify vulnerabilities. In fact, we are trying to set up a vulnerability management program. Being able to see that these open services exist will help us craft policy moving forward, implement a scanning methodology, and to figure out how to close them down."*
>
> **— CISO, University H**

According to most participants, tracking vulnerabilities and risk exposure are some of the most important functions of cybersecurity teams, and Arctic EWS monitoring contributed to that meaningfully. One of the participants (C) was alerted to up to 300 known vulnerable services daily. They created a two-week deduplicated baseline for starting to mitigate the issues, reaching out systematically to the asset managers to remove the problems.

For university F, the chosen approach was sorting the reported vulnerable services by how easy they were to mitigate and start to work down from the easiest to address each one. Microsoft-related services that were open to the internet, including Kerberos, were first. Then they removed issues around DNS and multicast DNS, and so on down the list until they are now left with remote usability protocols, which require more internal dialog with the various business units to address.

With the project starting during the summer recess, a few of the project participants took an aggressive approach from the beginning by prioritizing and quickly removing all the reported issues. Those two (D & E) can be identified in the incident tracking graph as the lines that trend towards zero. After about a month of service, just in time for the start of the new school year, they achieved what we call a "green" report, with only a handful of issues arriving now and then.

The examples show the two different use cases for continuous monitoring. Typically, new subscribers face a large number of vulnerable systems, which then need to be taken care of. This is especially true for larger organizations with a sprawling infrastructure. Eventually, as the subscriber resolves the number of notifications, work generated by EWS turns into addressing individual issues that pop up over time. These are incidents that result from new vulnerabilities, malware infections, configuration changes, repurposed assets, firewall configuration changes, network topology changes, and most commonly, when someone plugs in something unexpected to the network.

Both workflows are important, and we are striving for Arctic EWS subscribers to get to the state where there is nothing new to report on that day. Regardless, peace and tranquility never last forever; new problems turn up, and older, overlooked issues get added to EWS for monitoring. However, that is the very goal and philosophy of the service.

From single issues to continuous external monitoring

> *"Arctic EWS highlighted faults in some of the operational practices that we had, and showed on a clear daily basis that it was happening consistently, not as a onesie-twosie type of exception or device misconfiguration. By calling it out to us, Arctic EWS allowed us to identify where the problem actually was in order to address it directly at its source, and we could also show it wasn't just something we suspected, but that others were seeing it too."*
>
> **— Mark Herron, CISO, Case Western Reserve University**

Once they started receiving notifications from Arctic EWS, project participants made several higher-level observations about their current security posture. For many, the number of observed issues was a surprise. However, a few of the participants had existing processes for gathering information, so they had an idea of what to expect.

Another finding was that there were also sets of procedures or operating practices instituted a long time ago that had not been kept up to date with best practices. Decisions made previously about security protocols related to the firewalls turned out to not work as well as thought.

For example, a firewall is configured to block anything that's not a legitimate protocol. But what happens when someone is trying to talk to an exposed MySQL server? The MySQL communications protocol is perfectly legitimate, so it is allowed through by the firewall. This was a root cause for many observations of different database servers available to the internet from the university networks.

Of course, database servers should not be attached directly to externally facing interfaces, so there is security education work to be done. However, firewall maintainers also need to have a solid understanding of how the security device is operating.

> *“One of the things [EWS] has done is drive us towards this zero-trust architecture, which gets rid of the reliance on so many firewalls in which people are hesitant to make changes because they may have cascading effects.”*
>
> **— CISO, University F**

One of the main reasons interviewees gave for having so many visible issues was that larger university networks do not get re-architected frequently to keep them easy to maintain. A redesign is a laborious and expensive process to undertake, so for many, the day-to-day is working with the architecture they have inherited and trying their best to overcome its limitations.

While the cybersecurity situation has dramatically changed over the past few years,previously practical decisions made when network designs were created 5-10 years ago are now having a detrimental influence on the security of the networks.

UNIVERSITY	VULNERABLE SERVICE	SUSPECTED COMPROMISE
A	10270	840
B	44120	1594
C	25212	538
D	3531	6
E	2080	193
F	15010	744
G	39176	2673
H	35090	453
I	5374	243
J	38008	383
TOTAL	**217868**	**7667**

Table 1: Sum of observations in two of the three categories for all the universities who received notifications Arctic EWS during the project. Student networks accounted for majority of the suspected compromise types.

Finding the patterns

> *“We noticed a pattern that most of the, say, VNC vulnerabilities, belong to roughly the same department or two departments. That leads us to take on a further conversation with those departments, letting them know that this needs to be closed at the border and asking them if there’s any reason why it shouldn’t be closed.”*
>
> **— Principal Information Security Analyst, University C**

When you deal with individual incidents, it’s sometimes difficult to notice patterns of issues or behaviors. In the rush of things, you handle the case at hand and then move on to the next one. When Arctic EWS was enabled, the volume of the notifications increased for every participant. The larger volume of material helped them to identify patterns in the notifications.

Several project participants noticed security posture differences between campuses, indicating systematic security problems. The most common examples were related to exposed remote access and management software, such as RDP, Apple Remote Desktop, and VMWare management consoles.

These issues come up as remote IT teams set up infrastructure to serve the staff, but do not necessarily follow a standard security policy. They may allow local services that are not approved in the overall security policy, but these individual cases don’t flag systematic issues.

The problems are usually solvable through the education of IT staff and the blocking of access to certain services at the perimeter. Without external monitoring, they can go unnoticed. And without proper visibility, you don’t know where the problems lie, which makes it difficult to enforce a consistent security policy.

Besides Arctic EWS, you can also use periodic internal and external security scans from other security vendors to address these issues. The universities that already performed such network scans every few weeks before this project started were less likely to be surprised by the Arctic EWS results. However, they did mention that the prioritized EWS results were easy to act upon.

Reusing network assets

> *"The concrete problems we have are related to the reuse of IP addresses without also making sure that they're ready to be reused. Just because they're available and nothing is using them, it doesn't mean that there aren't accommodations in the firewall from having used them in the past."*
>
> **— Mark Herron, CISO, Case Western Reserve University**

Monitoring of network asset re-use policies is a challenge for many universities, and this quickly became visible with external monitoring. As the project participants tracked down reported issues and the systems in question were located, assets that turned up in monitoring are often repurposed systems.

How does this become a problem? A system or virtual machine gets repurposed for a new use and continues to have its assigned address, and new rules are added to the firewall to enable the required services. Unfortunately, when IP addresses get reused or reassigned, that doesn't mean that the firewall rules have been checked to ensure that any previous permissions have been removed. There needs to be a consistent process to maintain the firewall security policy and a checklist to ensure that all steps are taken. The process is particularly important when multiple people or teams are managing the rules.

A few participants spent a good amount of back-and-forth time with the IT team to figure out why security problems kept coming back. Base images of a virtual machine are another way for vulnerabilities to sneak back in. It is easy to reintroduce the issue that has already been "fixed" once the system is re-imaged. It can be a factor that can cause frustration between IT and security because it's mentally taxing to go back to fix the same thing several times after you've moved on. A large part of achieving sustainable security is accomplishing it without making it a chore for the IT staff.

The illusion of firewall effectiveness

> *"Arctic EWS identified things that needed to change at the border, which in turn, when we brought this up to our CISO, made her think: 'Well then, what are the top 10 things that should be blocked at the border and why aren't we doing it?' So, it progressed into this deeper conversation between us and our networking team members."*
>
> **— Principal Information Security Analyst, University C**

Often, there is an illusion that the firewall infrastructure in place has been designed and implemented correctly and everything is safe on that front. That illusion doesn't usually break until concretely proven otherwise. Usually, the evidence for disrupting that belief needs to come from the outside. Unfortunately, many organizations do not have a way to systematically gather outside information that would help to reveal the invisible issues.

In this project, we saw how a typical university has porous firewalls and issues with firewall rule management. The problems arise from the very complex operational environment, where exceptions must be made for many systems. That is typically not an issue in a network where a more consistent change management process exists. A less firewall-dependent zero-trust architecture may be a good long-term solution for university networks.

Many research project participants found that they could significantly improve their security posture by adjusting their firewall policies, pruning rules, and improving communications with various stakeholders.

It's a good practice to have scheduled meetings between the security and IT side of the organization to keep tabs on what has been implemented without the other party's knowledge. Participants shared experiences of how they have improved on the situation by simply improving on the collaboration. Communication is essential for decentralized organizations and can have an enormous impact on your security posture.

It is prudent to have a system where all firewall rules related to a system are reviewed periodically. Otherwise, unless you do systematic external scanning, outdated rules can sneak in unnoticed. Pruning firewall rules systematically is helpful in several ways. Over time as more rules are added than are removed, the management of the rules becomes untenable due to sheer mass.

The traditional approaches also include arranging for scheduled penetration testing of your network, where network scanning is a part of the service. These scans can be comprehensive, although it can also be quite expensive to arrange them frequently. Annual or semi-annual scans are the norm. The downside is that a lot can happen between those reviews because very few IT environments stay static for such a long period.

Improving communication

> *“Getting notifications let us put data in the hands of those who were going to be held responsible for security breaches. We were able to show folks that this is available online, here’s a third party who went and discovered these things and asked: ‘Do you understand that it’s now exposed probably more than you would like?’ This breeds new conversation, a report from an outside agency. They allow us to have more collaborative conversations, which is great.”*
>
> **— CISO, University F**

External security monitoring highlights security policy problems that otherwise tend to remain invisible, such as communications issues between cybersecurity and IT functions. Security teams struggle to keep up with IT and are often stuck playing catch-up. The importance of a systematic vulnerability management process becomes plain to see with external monitoring, which also serves as a good starting point for addressing the problems and improving internal communication with stakeholders.

A good case study was with university E that received a report about having their F5 load balancers control interface exposed to the internet. While it didn’t have a vulnerability at the time, it’s still not a good decision to expose it. When they communicated about this to the infrastructure team, it disappeared from the internet. It was later acknowledged to have been misconfigured in follow-up between the security and network teams.

The interaction brings up the communications problems within the organization and shows how a security team may be operating on an assumption rather than a factual situation picture.

Receiving the notification provided the security team with the kind of evidence that they needed to support the submission of a budget proposal for implementing proper privileged access management tools and procedures for the university networks. Having that system in place would have prevented important devices from being exposed to the internet and then having that access removed without leaving any trace of the incident.

Revealing asset management-related issues

> *“As an R1 research institute, we have principal investigators, grad students and undergrad students who are all involved in research projects, and all standing up infrastructure under the desk at any moment. None of this necessarily went through any sort of validation and acceptance. So, we saw both shadow and abandoned infrastructure during the project.”*
>
> **— CISO, University F**

The research-heavy R1 and R2 universities are in a unique position from the expectations of the staff and students that they need to cater for, and the cybersecurity team often gets the short end of the stick. Unexpected systems are plugged into the network and often left there without the security staff knowing their presence. When these systems become vulnerable, unexpected information may leak out. Even more alarmingly, after being exploited, they become steppingstones for lateral movement inside the network.

There was a great deal of variety in the level of awareness of the location of the assets. There were also differences in whether they could find them after being informed about an issue. Those responsible for a single campus had a reasonably accurate picture and could deal with them promptly. For multi-campus universities, it was often complicated and time-consuming to locate the offending system.

External notifications highlight issues that universities have with network asset management and asset ownership documentation. Many project participants had obstacles finding the vulnerable systems in their networks, which is a severe handicap in a crisis situation.

Once you have a strategy for maintaining an asset management database, working through the notifications is a practical way to begin the systematic documentation of the network. Notifications serve as a way to catch assets that have been misclassified when there are events and are also a useful trigger and medium for establishing better communication with various internal stakeholders.

Arctic EWS vs. DIY

> *"I am estimating that this service would save us between 5 and 10 hours of work per week in pulling this all information together. You are doing it for us and actually sending us the information already sifted through"*
>
> **— Mark Herron, Case Western Reserve University**

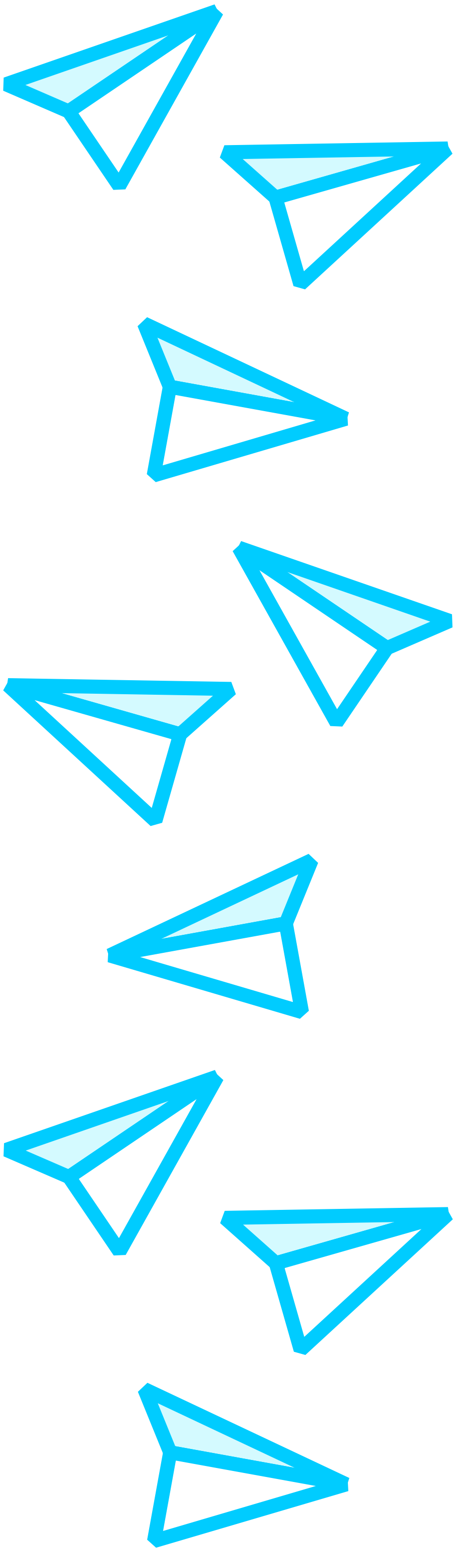
Project participants estimated that the data gathering and processing by Arctic EWS would consume 5 to 20 hours' worth of analyst work per week, depending on the institution. This kind of work would involve collecting relevant information from external sources, converting it into a helpful format, and processing it to match against the known assets.

Those universities who were already engaged in collecting data from other sources, such as Shodan, CISA, REN-ISAC, or Dorkbot, noted that the content Arctic Security provided via its EWS service exceeded in several metrics the amount of information that had been previously available.

Those who already did data collection and scanning said that they normally do the scanning periodically, typically every few weeks, rather than as continuous monitoring.

A security staff member can perform the work to replicate Arctic EWS in-house; it just takes time and effort. Dedicating that amount of time and finding the staff to do it are significant obstacles to overcome.

> *"Given the size of my team and the limited resources we have, we will not be able to do that ourselves. We just don't have the capacity or capability to do that on our own. So, the value of Arctic EWS to me is the fact of having somebody looking over our shoulder to make sure we're following the right path."*
>
> **— Tom Dugas, Duquesne University**



Project participants added that one of the benefits of outsourcing the work to Arctic EWS is managing the considerable turnover in cybersecurity staff. Every few years, a new person needs to learn the skillset and gain the experience of finding the relevant data.

While working in cybersecurity domain is rewarding in general, working with this kind of data in-house is also not necessarily the exciting part of it. That can lead to the work becoming a low-priority task and lead to less motivated staff who seek other opportunities.

In addition, participants noted that it was helpful that the data was delivered as a service without needing to stand up infrastructure for collecting and processing it. The universities already have plenty of infrastructure to look after as it is.

Also, since it was an external service using information already available from the Internet, complex contracts and privacy agreements were not required to get started with EWS.

Conclusions

The EDUCAUSE and Arctic Security joint venture in providing Arctic EWS for higher ed was successful. We interviewed eight out of the 10 participants at the end of the project and gathered their feedback.

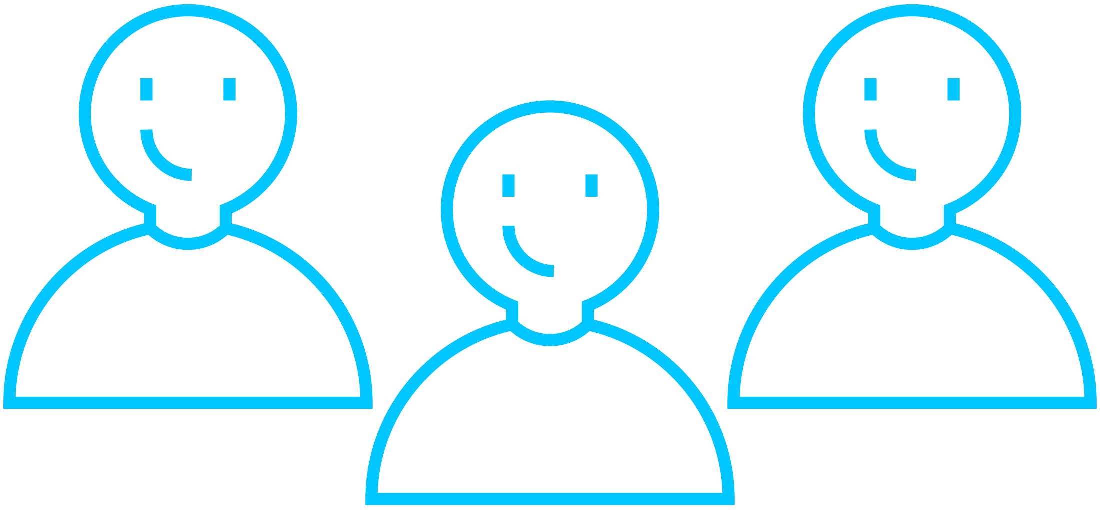
Six of the interviewees reported that they found new findings in the reported content, while two said that they already had access to the vulnerability side of the information through other means that they had developed. All participants except for one felt that the data was valuable and would contribute positively to security if they had continued access to it.

Five of the interviewees said that they found systemic problems by reviewing their notifications and then addressing them. The systemic problems identified through resolving the reported issues were related to firewall management, established security processes, processes related to incident response, change management, vulnerability management, asset management, and stakeholder communications.

Most were happy with how the data was delivered and said that API-based access would make it even more convenient. With everything accounted for, data from Arctic EWS was easy to act on, although many asked for dashboards and direct integrations to SIEMs and other systems. Those capabilities are available but were not included in this project's scope, which focused on the utility of the data itself.

Two participants expressed that their challenge was not about accessing the data but acting on the data gathered and finding the actual assets to fix the reported problem. They hoped that we could help solve that problem, and a follow-up project to research this topic is planned.

Arctic Security



Project participants

The universities were chosen to represent a range from single campus colleges to multiple campus university systems, and from different parts of the USA. Participants were also chosen so that they would represent a variety of functions, from teaching and research institutes to that host university hospitals. Ten of the institutions that were invited agreed to participate in the research program.

We thank all participants for their openness about the cybersecurity issues in academic networks, contributions and sharing in the project meetings, and insightful and frank commentary in the interviews.

Juha Haaga
Principal researcher, project lead

UNIVERSITY	CLASSIFICATION	PROJECT PARTICIPANTS
Case Western Reserve University (CRWU)	R1	Mark Herron, Tim Spiker
Duquesne University	R2	Tom Dugas
Marist College	M1	Emily Harris, Will Hongach
Northeastern University	R1	Harry Hoffman
Stony Brook University	R1	Matthew Nappi, Sanjay Kapur
University of Arizona	R1	Jayla Fry
University of California, San Diego (UCSD)	R1	Michael Corn
University of Connecticut (UCONN)	R1	Chris Bernard, Chris Tarricone
University of Hawaii	R1	Jodi Ito
University of Massachusetts (UMASS)	R1	Matthew Dalton, Jake Cunningham

Table 2: Project participants and their classifications, and project participants

Arctic Security

If you liked this paper and want to see more of this kind of material, we'd love to hear from you. Likewise, if you felt something was missing, still let us know. We are always happy to hear from you, no matter the reason. Head over to the our Contact Us page and share your thoughts!

And if you're interested in what we do and want to stay up to date, the best way to do that is by following us:

pat.healy@articsecurity.com

www.articsecurity.com