Early Warning for Higher Education

Visibility into Cybersecurity Issues Across Campus, Cloud Services, and your Vendors

Arctic Security

Arctic Security

Secure Your Campus from the Outside In

Cyber threats target universities with strained resources.

In higher education, security teams face a perfect storm: decentralized systems, limited budgets, legacy infrastructure, and a culture of academic freedom. The result? Many exposed, vulnerable, and unmanaged systems that attackers love to exploit.

Arctic EWS gives you the visibility you are missing.

Early Warning Service is a cloud-based monitoring service that continuously matches external cyber threats to your assets. Based on your domains, networks, cloud assets and vendors, it alerts you to real issues with clarity and speed.

No more false alarms. No more guesswork. IT friendly notifications with no cybersecurity expertise required.

Built for Higher Education Challenges

Decentralized IT? no problem.

Arctic EWS was built for distributed, sometimes unruly environments just like yours. Whether you manage one campus or ten, we monitor the external footprint across all departments, subnets, cloud services and vendors.

Only the Alerts That Matter.

Your most limited resource is time, and it is precious. With a false-positive rate under 2%, Arctic EWS filters out the noise and gives you actionable alerts prioritized by urgency. You will be able to act on them with confidence.

Real world case: Lost in the Network

With a US based university, Arctic EWS uncovered a serious oversight. The central IT team discovered a lab server they didn't even know existed, exposed to the internet, running outdated services.

The server belonged to a research department and had gone untouched and unpatched for years.

"We don't know what we don't know. There are faculties hosting machines we have never touched. Some of them have open ports or vulnerable services running, and we only find out after there's a breach." - IT Manager

With Arctic EWS, the server was flagged and remediated within a day, likely preventing a serious data exposure.

Managing cybersecurity exposure in Higher-Ed is vital for securing the networks against highly disruptive cybersecurity threats.

Why Higher Education Chooses Arctic EWS

Effortless Monthly Reporting

Clear and actionable monthly reports give you structured, decision-ready data, and helps IT communicate about cybersecurity with management. Organize the insights by campus, faculty, or infrastructure type for context.

What do we detect?

- Exposed systems & known vulnerabilities
- Misconfigured services and vendor systems
- Shadow IT and abandoned assets
- Systems already suspected of being compromised
- Leaked or stolen credentials

Zero Complexity to Get Started

No hardware. No heavy integrations. Just add your digital assets, and we start monitoring right away. Arctic EWS works alongside your existing tools, acting as an **added layer of protection** — without added complexity.

With Arctic EWS, You Will:

- **Empower your IT team to contribute to cyber security**
- **Reduce detection and response times dramatically**
- **Catch cyber security issues your other tools miss**
- **Gain visibility across your operational footprint**

Request free assessment for your institution:

https://www.arcticsecurity.com/tailored-ews-demo