CASE STUDY

Private University Seeks Third-Party Vendor to Take Over Cybersecurity Tasks

BitLyft Cybersecurity

ORGANIZATION

Private university
in Mississippi

INDUSTRY

Higher Education

STUDENTS

4800+

LOG SOURCES

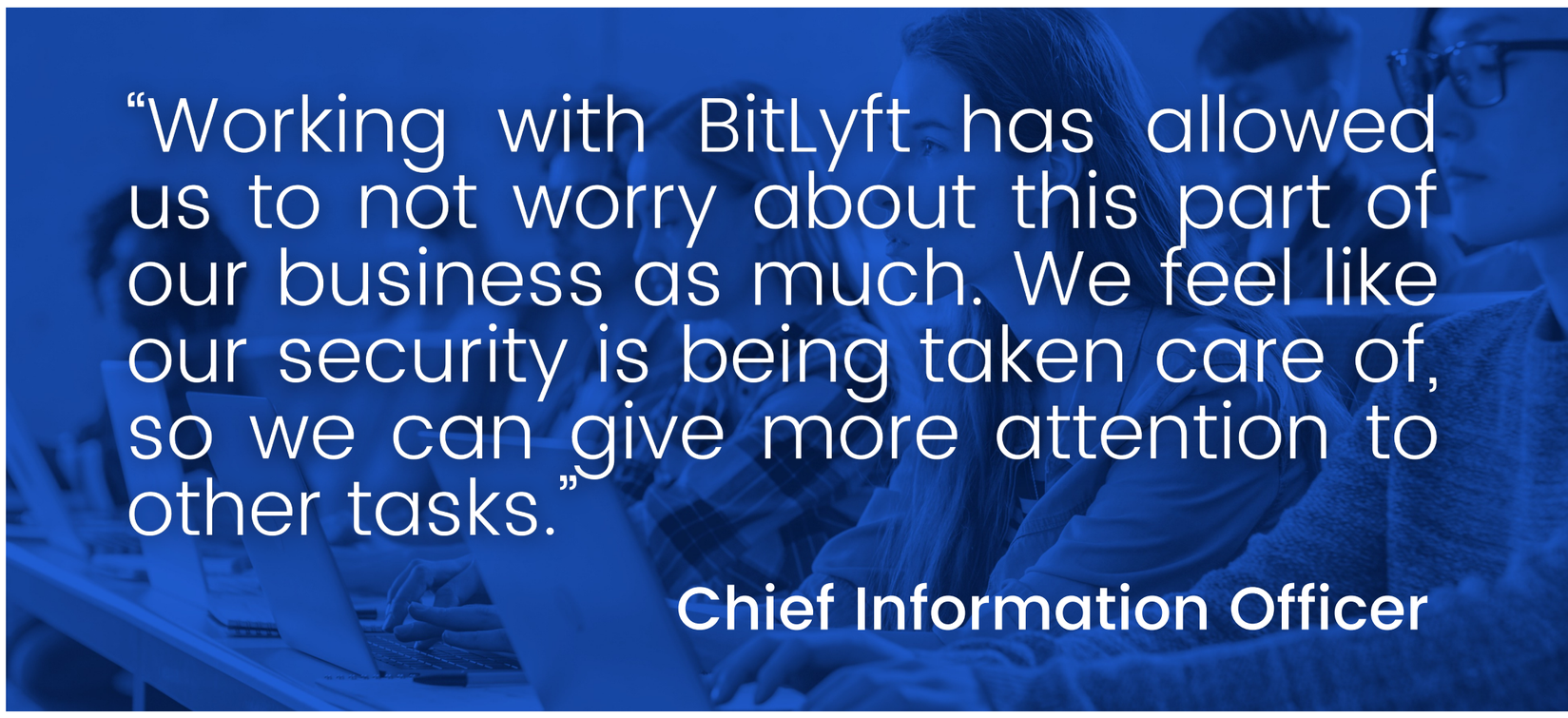
218 total sources from HP, Linux, GSuite, Palo Alto, CrowdStrike, IIS Web Server, Manage Engine, ProCurve Switch, Zeek Network Monitor, Qualys Vulnerability Scanner, Apache Web Server, Windows Servers

KEY IMPACTS

- School IT team was able to stop wearing both IT and cybersecurity hats
- Deeper visibility and understanding of university network
- BitLyft Automations helped reduce human time spent remediating security issues

“We know that we can count on the BitLyft team to stick with us until any concerns on our side are taken care of.”

- Chief Information Officer



THE CHALLENGE

As cybersecurity concerns grow and regulations expand, many organizations find themselves in search of information. This was true for the IT staff of a private university in Mississippi. After attending a couple cybersecurity conferences and reading more about the topic, the university determined it needed a strategy. With some knowledge in hand, the institution signed a contract with a consultant from one of the conferences. The contract included an annual risk assessment and advisory services.

During their first year of partnership, the consultant covered network monitoring. The university gained a lot of insight about the topic, but realized it was not adequately prepared to handle the workload on its own. Not only did the institution lack staff, but they didn’t have the right certifications or subject matter experts. In addition, the team didn’t have the time to only work on this one aspect of their business. According to the audit, the university needed to hire a Chief Security Information Officer (CISO) or Chief Security Officer (CSO), but the salary range for both of these positions was out of budget.

Further contributing to the IT staff’s challenges was the plethora of alerts coming in from their Security Incident and Event Management (SIEM) system. “We were trying to process all of the university’s traffic, but we could not keep up with the raw data or the amount of alerts coming out of the system,” said the university’s Network and Security Manager. With this knowledge in place, the university began to look for a third-party to monitor their systems.

THE SOLUTION

After speaking with some local companies, the university made a connection with BitLyft at a higher education council event.

“We liked that BitLyft was a smaller company; we felt like we could be listened to better,” said the university’s CIO. “We also liked that they had other universities as clients with similar size, budget and staff.”

CASE STUDY

Private University Seeks Third-Party Vendor to Take Over Cybersecurity Tasks

BitLyft immediately installed its SIEM management tool on many of the university's most prominent servers and workstations to monitor network traffic. This gave the institution a more advanced look into their network landscape. The two parties connect once a week for a meeting to discuss any concerns that either may have.

"The meetings can last five-minutes or they can last one-hour depending on any concerns," said the Network and Security Manager. "We know that we can count on the BitLyft team to stick with us until any concerns on our side are taken care of."

THE RESULTS

With an established partnership, the university's IT staff can finally give attention back to the other facets of its business.

"Working with BitLyft has allowed us to not worry about this part of our business as much," said the CIO. "We feel like our security is being taken care of, so we can give more attention to other tasks." Partnering with BitLyft also reduces the number of network alerts the university has to monitor.

88.9 HOURS, OR 55% OF A 160 AVERAGE HOUR WORK MONTH, WERE SPENT REMEDIATING EMAIL ACCOUNT ISSUES.

BITLYFT AIR MODULES REDUCED THAT TIME TO ZERO.

"Before BitLyft, we were having to go through as many alerts as we could and try to figure out what was genuine or not," said the Network and Security Manager. "Oftentimes, we would have to ignore items because we did not have enough man hours to go through everything."

In a final statement, the university's CIO noted, "We feel very comfortable with the entire team at BitLyft. We feel like we can discuss what our needs for the university are and BitLyft will provide the service that we're looking for."

Clarity of Network Landscape

Regained IT Focus

Reduced Security Alerts

info@bitlyft.com | www.bitlyft.com | 517.220.0990