INDUSTRY SPEAKS

Securing Higher Ed in an AI-Driven World

Higher education leaders must understand the risks and benefits of artificial intelligence and machine learning as they deploy these tools and take advantage of the opportunity to advance technology-based transformation within the institution.

Artificial intelligence and machine learning have great potential in higher education to enable new modes of learning, improve research outcomes, and accelerate decision-making. At the same time, these technologies are changing the cybersecurity picture, giving bad actors the means to fine-tune and scale their attacks.

"AI affords cyber criminals the ability to take their intent and multiply it," noted Mike Lauer, director public sector programs at Fortinet.

PRESENTED BY: CAMPUS TECHNOLOGY

SPONSORED BY: FORTINET

The Promise of AI…

With artificial intelligence, colleges and universities can support personalized learning, drive administrative efficiencies, and improve campus operations, Lauer said.

"How do we keep students engaged? How do we ensure that a student receives instruction at their own pace and level?" he said. AI can help to make this possible, empowering instructors to tailor their efforts.

It can likewise help the back office to "streamline administrative tasks, like admissions and scheduling," he said. And AI-driven interactions can help students self-serve when they're looking for answers to questions, easing the burden on those administrative teams.

AI has the potential to drive improvements in many areas on campus: streamlining and simplifying daily operations, and helping to inform better, faster decision-making on the part of campus leadership.

In terms of operations, campuses are mini-cities. "They have water, they have waste, they have energy, they have parking," Lauer said. AI has the potential to drive improvements in all those areas: streamlining and simplifying daily operations, and helping to inform better, faster decision-making on the part of campus leadership.

…and the Peril

AI is a double-edged sword, enabling bad actors to heighten the pace and intensity of their attacks on college and university systems. They're using it to go deeper into data harvesting, and they're tapping the power of AI to improve their own evasion strategies.

When it comes to data harvesting, bad actors "are looking

for things like intellectual property, research data, financial details," Lauer said. They need to correlate that data in order to use it for ransomware or other exploits, and "AI has the ability to sift through just vast amounts of data, and especially if it's stolen data."

In terms of detection-evasion, AI enables cyber attackers to write code on the fly, which in turn helps them mask their exploits. "When you're speaking of malware … that becomes an evasion technique," he said. "It actually makes it really hard for malware detection to take place."

AI in Cyber Defense

While the capabilities inherent in artificial intelligence can be used to accelerate cyber attacks, those same qualities also can be used to strengthen cyber defenses within higher ed, offering improved risk analysis, streamlined threat detection, and automated incident response.

While the capabilities inherent in artificial intelligence can be used to accelerate cyber attacks, those same qualities also can be used to strengthen cyber defenses within higher ed.

Cyber defense has been largely manual in the past, with administrators poring over activity logs and looking for signs of threat. The sheer volume of network and system data today makes this difficult. "There's so much that is happening, so much that's going on," Lauer said.

Tools like Fortinet's Fortiguard Labs threat intelligence platform can help here. Supported by AI, "we look at billions and billions and billions of threat indicators all throughout the day," Lauer said. Those insights can help schools to take rapid defensive action in the face of emerging threats.

Going forward, AI-driven insights will inform not just daily defenses, but larger institutional policies in support of cybersecurity. “We’re starting to see this conversation of cybersecurity operations and the risk management, [with schools exploring] the policy side of doing something actionable with that perceived risk,” Lauer said.

AI today can support real-time monitoring, giving visibility across the entire digital surface. It can support enhanced and orchestrated threat-identification and response.

Schools can look to AI for defense against “zero day” threats, malware and other forms of attack that may linger undetected in their systems. They can leverage machine-speed insights “to find out where these exploits are sitting,” Lauer said.

AI today can support real-time monitoring, giving visibility across the entire digital surface. It can support enhanced and orchestrated threat-identification and response.

With AI’s capabilities around natural language processing, or NLP, cyber defenders are gaining deeper insights into hackers’ strategies. They are gleaning threat intelligence and identifying emerging attack strategies “from all across all the forums — the dark web, social media, anything that has a digital presence,” Lauer said.

“Once we find what’s there, we can automatically put that information into other tools that are there. That’s useful for automated penetration testing based off of where these threat actors are coming from and how they’re going to try to hit my general network or my general footprint,” he said.

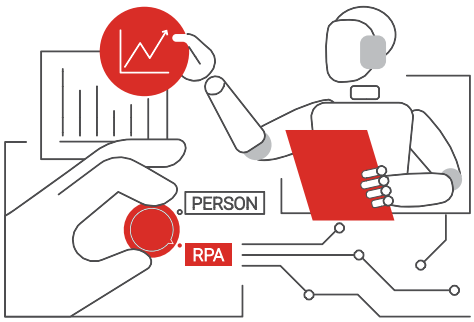
Going Forward

Given the emerging role of AI in cybersecurity — both

the peril and promise — there are steps that school IT teams take today to put themselves on a stronger footing. They can simplify their technology ecosystems, and get proactive on zero trust strategies.

Given the state of the threat landscape, "you would be best to start to reduce the complexity of some of the technologies you have, of your overall footprint," Lauer said. He points to the notion of a cybersecurity master architecture as a good starting point. Under such a plan, IT might invest in a limited number of interoperable platforms, "so that you can have a uniform view of what's out there."

Such an interoperable-platform environment "makes the use of AI/ML tools much more powerful, because I have a uniform system that they're moving across," he said.



School IT teams can take steps to put themselves on a stronger footing. They can simplify their technology ecosystems, and get proactive on zero trust strategies.

Schools should also be making the shift from perimeter-based security to a zero trust architecture, Lauer asserted. In higher ed, "we have lots of different disparate things going on, and then on top of that, you have a lot of different users that need access to those different things." In such an environment, "I'm always going to have an open spot in my perimeter."

Rather than trying to safeguard that inherently porous perimeter, schools can look to zero trust as a more robust and effective means of securing their systems and data.

"Zero trust architecture says: I'm not going to trust anyone, no matter where they're at. I'm always going to verify. That is a philosophical change that will help the conversation," Lauer said. An integrated and dynamic security platform, supported by AI, could help bring that vision to life.