Application: 5833

The Jenzabar Managed Services Responds to CrowdStrike Crisis

Page: General Information

Provide information about the company to be considered for the award. If you will be nominating an individual, specify the nominee's employer.

Name of Organization/Company

Jenzabar

███████████████████

█████████████

Additional Contacts

I do not wish to list additional contacts

Page: Entry Information

Entry Title

The Jenzabar Managed Services Responds to CrowdStrike Crisis

Category

J08. Technology Team of the Year - Educational Technology

Technology Team Submission Format

Written Answers

a. Briefly describe the nominated technology team: its history and past performance (up to 200 words). Required

With their wealth of personal and research data, higher education institutions are increasingly becoming prime targets for cyberattacks, particularly ransomware. These incidents not only compromise sensitive student and faculty information but also threaten the continuity of academic operations. In some cases, cyberattacks have resulted in institutions shutting their doors for good.

The Jenzabar Managed Services team provides higher education institutions with specialized support that enhances cybersecurity, optimizes operations, and improves user experiences. The Jenzabar Managed Services team provides dedicated servers, vigilant monitoring, and industry standard failover recovery to ensure colleges and universities have the means to scale their technology and safeguard institutional and student data against potential threats.

This year alone, Jenzabar's Managed Services team has thwarted 10 ransomware attacks. Additionally, the team played a significant role in minimizing the impact the CrowdStrike outage had on client institutions. During the July 2024 incident, more than 8 million systems around the world crashed and were unable to properly restart, resulting in approximately $10 billion USD in financial damage. Many schools were affected during this time, but Jenzabar's Managed Services team was able to intervene and get systems back online in a matter of hours.

b. Outline the technology team's achievements since the beginning of 2023 that you wish to bring to the judges' attention (up to 250 words). Required

Jenzabar uses CrowdStrike—a cybersecurity technology company—as its endpoint detection and response provider for SaaS solutions. CrowdStrike effectively serves as Jenzabar's eyes on its customers' systems, providing 24/7 critical support against cyber threats. On July 19, CrowdStrike pushed out an update that crashed Windows systems globally.

At 3:00 AM on July 19, Jenzabar received an alert from its overnight team indicating there was an issue on one-third of its client-hosted servers. This meant hundreds of institutions and more than 1,000 systems were essentially non-functional. Recognizing the urgency of the situation, the Jenzabar Managed Services team sprang into action.

Over the next hour, the team worked tirelessly to assess the extent of the disruptions and identify the source. Internal research, coupled with the early morning news cycle, revealed it was the CrowdStrike update error, and Jenzabar quickly devised a strategy for implementing a rapid recovery plan. The team called an all-hands meeting at 8:00 AM, communicated the strategy, and mobilized over 60 staff members to work system-by-system until functionality had been restored to all impacted servers. Jenzabar worked across time zones, first addressing East Coast clients, then moving to Central and farther west.

c. Explain why the achievements you have highlighted are unique or significant. If possible compare the achievements to the performance of other players in your industry and/or to the team's past performance (up to 250 words). Required

According to CrowdStrike, most businesses were back online within a week. However, most experts quoted in the news coverage of the incident said, realistically, it could take several weeks for organizations to fully recover from CrowdStrike's IT failure. Meanwhile, the Jenzabar Managed Services team had the problem entirely handled within a matter of hours, ensuring institutions could continue business-as-usual and would suffer no ill effects of prolonged downtime.

This is incredibly significant because it not only highlights the talent of Jenzabar's Managed Services team, but also its preparedness for any incident. The team's dedication to providing customers with 24/7 monitoring meant that the moment the issue occurred, Jenzabar was aware and able to begin working toward a solution.

It is also important to note that, while the team regularly holds webinars and conference presentations designed to educate clients on how to improve campus security, in the wake of the CrowdStrike incident, they've expanded their efforts to support and educate higher education institutions. One of the team's most recent initiatives was a presentation at the HESS Consortium during which they discussed the CrowdStrike incident and provided guidance to HESS member institutions on ways they can enhance their own cybersecurity posture and resilience moving forward.

d. Reference any attachments of supporting materials throughout this nomination and how they provide evidence of the claims you have made in this nomination (up to 250 words). Optional

Thank you notes from our clients:

"We just came up! Our Orientation is today so we are SO SO relieved."

"Thank you for the post and for all the hard work. It just reminds me what a great decision it was to go hosted!"

"I know it's a tough day that's not your fault, but your efforts to help customers are much appreciated!"

"A big thank you goes out to you and your team for the titanic effort in fixing the CrowdStrike incident last week. Just knowing what we had to go through on-premises, I cannot even imagine what it was like for your team. Great job, all!"

Coverage of the CrowdStrike Incident:

• Delta sues CrowdStrike for millions of dollars lost between 7/19-7/24. CrowdStrike argues that Delta is trying to shift the blame for its own poor response to the crisis. Meanwhile, Jenzabar's fast response had clients operational in mere hours. https://www.darkreading.com/cyberattacks-data-breaches/delta-launches-500m-lawsuit-crowdstrike

• One in 10 German companies are looking to switch IT security vendors after experiencing 10+ hours of business disruption and 2-3 days until full recovery. Jenzabar clients were fully recovered by 1 pm on the 19th. https://www.cio.com/article/3537281/german-firms-shed-light-on-crowdstrike-disasters-fallout.html

• This article discusses how CrowdStrike incident impact institutions across the country, causing them to shut down operations, cancel classes, and lose access to essential information. https://www.insidehighered.com/news/tech-innovation/administrative-tech/2024/07/22/how-crowdstrike-global-technology-outage

Webpage Link

[REDACTED FOR PUBLICATION]

Would you like to add an additional webpage link?

██

██████████

████████████████████████████████
████████████████████████████████

Would you like to add an additional webpage link?

Supporting Document

No File Uploaded

Would you like to add an additional supporting document?

By your submission of this entry to The Stevie Awards, you verify that you have read and agreed to abide by the regulations, terms and conditions of the competition (https://www.asia.stevieawards.com/rules-and-terms-conditions-competition).

Terms and Conditions

I Agree