INL/MIS-24-79761-Revision-0

Lessons Learned for Responsible Use of Cloud in the Cirrus Project, Following the CrowdStrike Outage Event

October 2024

Remy Vanece Stolworthy, Julia Catherine Morgan, Emma Mary Stewart

Idaho National Laboratory

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/MIS-24-79761-Revision-0

Lessons Learned for Responsible Use of Cloud in the Cirrus Project, Following the CrowdStrike Outage Event

Remy Vanece Stolworthy, Julia Catherine Morgan, Emma Mary Stewart

October 2024

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

CIRRUS
A cloud feasibility assessment tool

Lessons Learned for Responsible Use of Cloud in the Cirrus Project, Following the CrowdStrike Outage Event

A disruption in CrowdStrike's Falcon cybersecurity platform on July 19th, 2024, caused worldwide chaos. This event highlights the imperative need for cloud security measures for networks that are critically reliant on cloud technology. This incident negatively impacted air travel, government networks, and critical infrastructure sectors such as hospitals and financial institutions. While no electric utilities had a physical impact, and few had an IT impact, there were issues created by loss of cloud services, and other interrelated industries. For utilities and energy distribution organizations, understanding and mitigating these risks is essential. The Cirrus tool offers a strategic solution engineered to weave cloud integration seamlessly into the fabric of operational management, thereby enhancing resilience and streamlining efficiency in the face of digital challenges.[1]

The Event

A flawed CrowdStrike antivirus software update caused a global IT outage which affected Microsoft Windows devices, leading to the infamous blue screen of death, grounded flights, and disruptions across various industries. Despite CrowdStrike's quick response to isolate and fix the issue, the incident required multiple manual reboots and file deletions on all affected devices.[2] This event is causing experts to evaluate potential points of failure related to vendor lock-in and network connectivity architecture, along with mass pushes of software across many entities, something that a cloud-based system can enable.

How Cirrus' Capabilities Can Help

Cirrus, a web-based tool designed for grid and utility professionals, offers a strategic pathway to navigating the complexities of cloud integration by considering key performance indicators, high consequence events, and risk analysis to develop holistic risk informed approaches for seamless cloud technology integration. Cirrus' key capabilities include:

1. **Comprehensive Risk Assessment and Management:** Cirrus provides a detailed risk assessment framework tailored for utilities by identifying potential vulnerabilities.
2. **Compliance and Regulatory Alignment:** Cirrus leverages Cyber-Informed Engineering[3] to provide a structured approach to regulatory compliance and reduce the risk of operational disruptions.
3. **Secure Integration and Management of Third-Party Services:** Integrating third-party services and vendors can introduce additional risks. Cirrus facilitates evaluation of the security posture of these entities and ensures that their practices align with the organization's security requirements.
4. **Incident Response and Recovery:** A well-defined incident response plan is essential for minimizing downtime. Cirrus provides comprehensive incident response strategies, enabling quick recovery from IT disruptions.
5. **Evaluation of Outage Consequences:** A key capability of Cirrus is its evaluation of the consequences of outages in critical system components. This assessment is particularly vital for smaller entities that rely on third-party services, helping them understand the potential impacts of disruptions on their essential functions. The output of the assessment emphasizes the importance of asking the right questions of vendors, significantly enhancing the understanding of potential risks and ensuring alignment with operational needs.

Conclusion

The recent IT outage linked to CrowdStrike's antivirus software serves as a stark reminder of the vulnerabilities inherent in cloud-based systems and the potential for widespread disruption. By leveraging Cirrus, organizations and utilities can significantly enhance their security posture. Proactive risk management, enhanced data protection, compliance alignment, and resilient infrastructure are essential to safeguarding critical services and maintaining operational continuity. The integration of Cirrus into an organization's cloud strategy is not just beneficial; it is imperative for future-proofing operations against the complexities and threats. Cirrus provides a robust solution to swiftly and effectively mitigate disruptive events, preserving the integrity, availability, and reliability of essential services.

[1] https://inl.gov/document/cirrus/
[2] https://www.usatoday.com/story/money/2024/07/19/global-outage-communications-systems/74465953007/
[3] https://inl.gov/national-security/cie/