GC-132 Microsoft Azure Sentinel to ConnectWise Integration

Authors: Christy Neal, Miseker Birega, Ryan James, Charul Patel, L. Renee Davis Townsend, Matthew Parker

Abstract

Our client, Cybriant, utilizes Microsoft Azure Sentinel to detect and analyze security incidents. To manage these incidents, Cybriant needed to manually transfer data collected into ConnectWise Manage, the platform Cybriant utilizes to manage incident tickets internally. Using Logic Apps, our team created an integration solution to aid Cybriant with this time-consuming process. Once incidents are detected in Sentinel, our integration solution automatically triggers the creation of a ticket containing important incident information in ConnectWise. When the ticket is handled or closed in ConnectWise, our integration tool communicates with Sentinel to modify or close this ticket. Key Vaults are used to provide a central location to update security keys. Our integration solution permits security, precision, and efficiency for our client.

Introduction

Cybriant, a leading Managed Security Services Provider, utilizes Microsoft Azure Sentinel to detect and analyze security incidents. Cybriant utilizes ConnectWise Manage to internally manage incident tickets. In order to create tickets, Cybriant analysts needed to manually transfer data collected into ConnectWise Manage. Manually entering this data for each detected incident was inefficient and error-prone. Using Logic Apps, our team created an integration solution to aid Cybriant with this time-consuming process.

Project Goals

Provide our client with a tool to automate ConnectWise ticket creation and decrease duplicate work.

Create an efficient and sustainable integration tool between Microsoft Azure and ConnectWise Manage.

Materials and Methods

We utilized agile development in 2-week sprints to create our integration solution. We used the following tools throughout the process:

- Cybriant GitHub
- Cybriant accounts for each team member
- ConnectWise accounts for each team member
- Azure Sentinel accounts for each team member
- Global Azure account for the team
- REST APIs
- JSON
- Logic Apps
- Azure Sentinel

Results

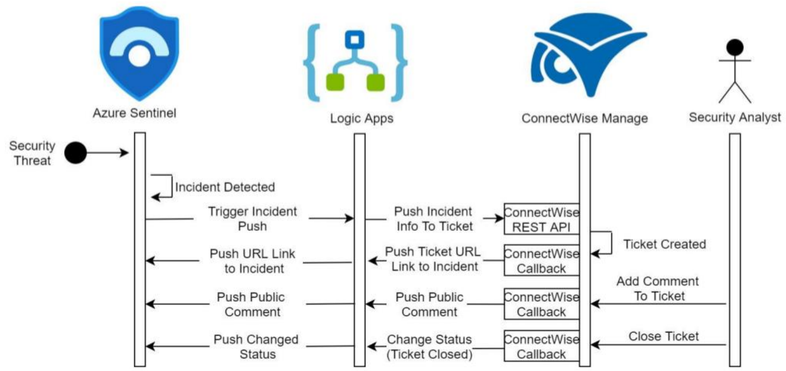

Fig.1 Sequence diagram demonstrating the flow between the three systems

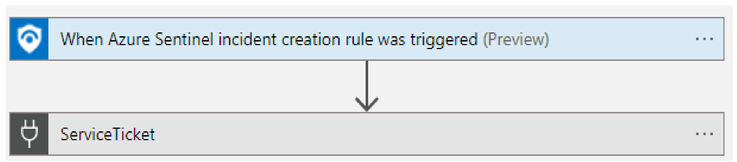

Fig.2 A workflow in the LogicApp to create a service ticket in to ConnectWise Manage from an incident trigger in the Azure sentinel

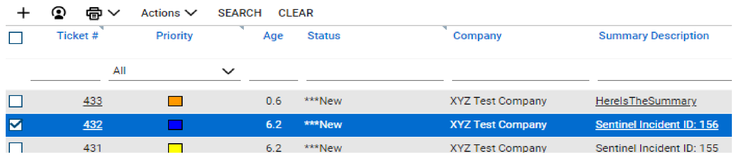

Fig.3 A service ticket is created in ConnectWise Manage

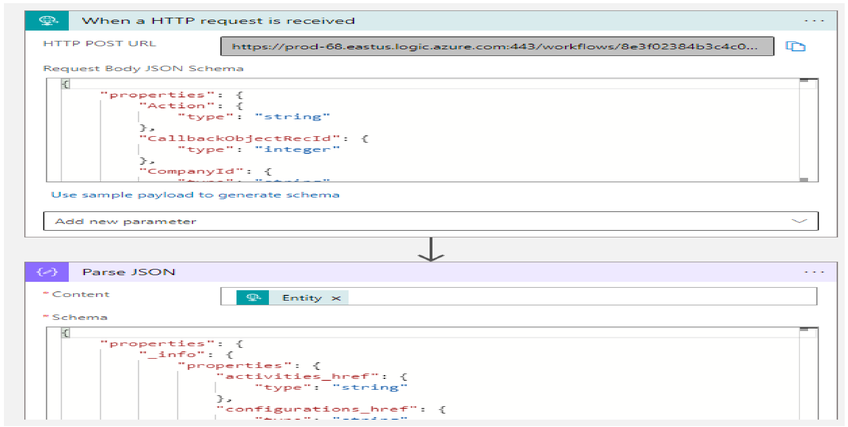

Fig.4 A workflow in the LogicApp updates an incident status in the Azure sentinel, after the ticket closure in the ConnectWise Manage

Conclusion

Our solution not only increases Cybriant's efficiency but also increases the reliability of the information included in tickets. Analysts no longer are required to check if there are incidents; tickets are created automatically when incidents are detected. Additionally, redundant work is eliminated by requiring information to be updated in one central location. Our final product that we will give to our client includes documents that will enable replication for the client to develop features in the future. Our integration solution is scalable and sustainable.

Acknowledgments

We would like to thank Cybriant, our client, for their support, and Justin Scott, our architect, for sharing his expertise and industry knowledge.
Thank you to Dr. Reza Parizi, our project advisor, for his assistance and guidance.

Contact Information

Christy Neal – christydneal@gmail.com
Miseker Birega – mbirega@students.kennesaw.edu
Ryan James – rjames57@students.kennesaw.edu
Charul Patel – cpatel33@students.kennesaw.edu
L. Renee Davis Townsend - ldavisto@students.kennesaw.edu
Matthew Parker - mpark110@students.kennesaw.edu

Project Website - https://sites.google.com/view/ksucapstone/

References

- https://azurecloudai.blog/2021/05/12/how-to-manually-create-an-azure-sentinel-incident/
- https://docs.microsoft.com/en-us/azure/sentinel/
- https://docs.microsoft.com/en-us/azure/data-explorer/
- https://docs.servicenow.com/bundle/rome-security-management/page/product/secops-integration-sir/secops-integration-ms-azure-sentinel/concept/microsoft-azure-sentinel-integration.html

KENNESAW STATE UNIVERSITY
COLLEGE OF COMPUTING AND SOFTWARE ENGINEERING