UC-176

Cybriant: Attack Surface Management

Author(s): Diwakar Rai, David Laurent, Jose Mendoza, Daniel Gutierrez, Nic Agyen-Frempong

Abstract

As businesses and organizations expand their operation digitally, so too do the vectors for attack expand. In partnership with Cybriant, this application develops an Attack Surface Composite Score by breaking down various attack common vectors. DKIM records, Open Port Scanning, and other metrics are compiled with the aid of Google Cloud Run jobs, deposited into Google BigQuery for analysis, and packaged and generated using Grafana as the front-end for our software stack. Our resulting application presents rapid, easy to understand breakdowns of various cybersecurity metrics and their impact.

Introduction

Our project with Cybriant focuses on developing an Attack Surface Management system tailored for mid-sized companies to improve their security posture and lower cybersecurity insurance costs. By analyzing security factors that impact BitSight ratings, this system will provide actionable insights that help organizations understand and reduce their risk.

Research Question(s)

1. What security metrics have a tremendous impact on a company's BitSight rating?
2. How can Google Chronicle and BigQuery data enhance attack analysis?
3. What are key challenges in adapting attack management for small and mid-sized companies?
4. How can the system ensure future data source integration?
5. what is the best approach for scoring an organization's cybersecurity hygiene ?

Materials and Methods

We began by reviewing existing Attack Surface Management solutions and BitSight rating factors to identify key security metrics. Next, we explored Google Cloud tools, including BigQuery and Google Chronicle SIEM, to evaluate their integration for data analysis. To build our scoring model, we studied cybersecurity rating methods and examined tools like OWASP AMASS for data collection and analysis enhancements.

Results

We were able to compile a list of 10 key attack vectors which we felt were the most common and vulnerable areas for domains. We compared our vectors to those found in a BitSight rating, and how these vectors could improve an organization's security profile. These vectors include the following:
[SPF Domains, DKIM Records, DMARC Usage, TLS/SSL Certificates Open Port Scanning, IP Range reputation, Domain Squatting, RUF/RUA Reports, HaveIBeenPwned, (email) and Shodan Analysis.]
These results were then analyzed and stored as jobs in Google Cloud Run, before being sent to Google BigQuery. Once parsed, this data is then forwarded to our Kibana visualization, presenting an easy to understand overview of a given domain's attack surface.

ASM Goals

- Develop containers and instances in the Cloud that analyze a set of security metrics.
- Schedule Cloud Run and BigQuery to develop historical attack surface data over time.
- Perform data analysis using Google BigQuery and Google Chronicle SIEM to house and parse aggregate data.
- Isolate critical breaches and vulnerabilities and how they are resolved over time.
- Generate reports on past and present issues and propose solutions.

Reference 3: BitSight/ASM Overview

Figure 1: Grafana Dashboard showing a company's example ASM.

Conclusions

- The major criteria that impact a company's attack rating were the frequency of breaches, security, hygiene, user vulnerability, and public disclosure of breaches. An organization must ensure that all publicly facing digital entry points are properly sanitized, its user base well guarded against common phishing attacks, and have proper policy in place when breaches inevitably occur.
- Security posture is not about perfection, its about consistency.

Acknowledgments

Sean Mitchell - Customer Success Manager
Pramit Bhatia - Software Engineer
Andrew Hamilton - Chief Technology Officer
Byron DeLoach - Vice President of Managed Services
Donald Privitera - Lecturer of Information Technology
Yan Huang - Associate Professor of Software Engineering

Contact Information

David Laurent - dlauren1@students.kennesaw.edu
Diwakar Rai - drai5@students.kennesaw.edu
Jose Mendoza - jmendo28@students.kennesaw.edu
Nic Agyen-Frempong - nagyenfr@students.kennesaw.edu
Daniel Gutierrez - Dgutier8@students.kennesaw.edu

References

Managed Vulnerability

Cybriant SDS

Create jobs | Cloud Run Documentation

https://cloud.google.com/bigquery/docs

KENNESAW STATE UNIVERSITY
COLLEGE OF COMPUTING AND SOFTWARE ENGINEERING