IriusRisk

USE CASE

Power BI Dashboard

Use Case

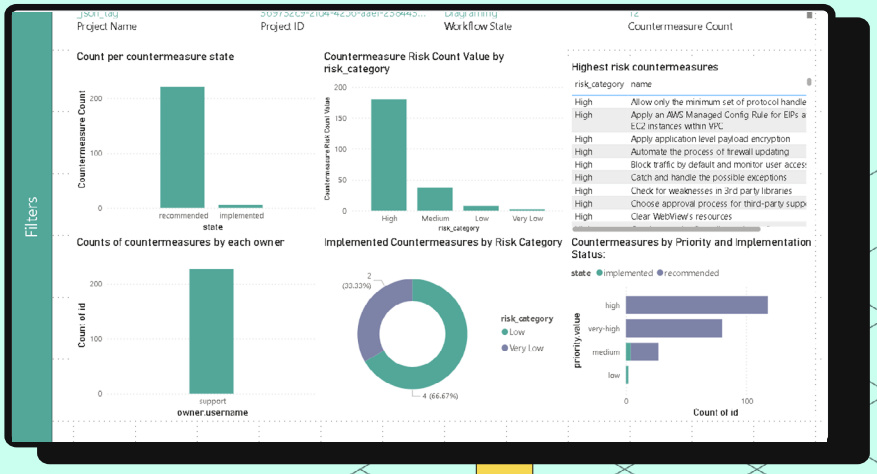
The customer is seeking more flexibility in the way they view and analyze data within IriusRisk reporting dashboards and generated reports. IriusRisk provides comprehensive data through its API, but creating custom reports can be complex and time-consuming, especially for teams with limited capacity or technical resources.

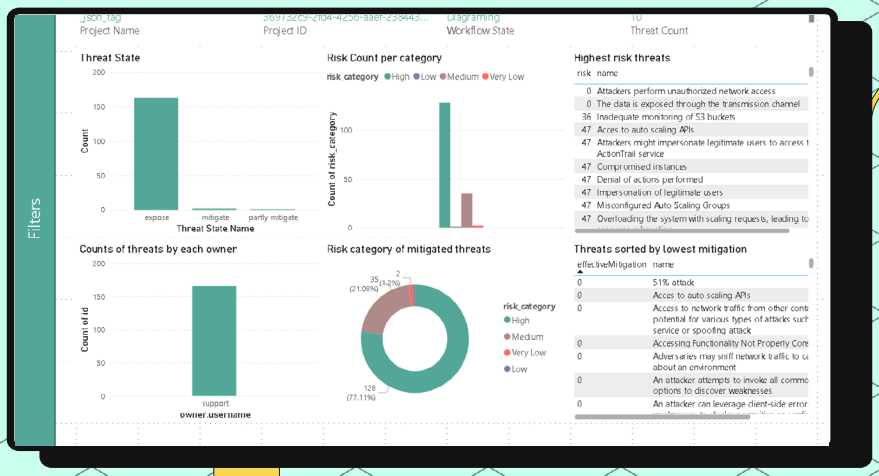
Requirements

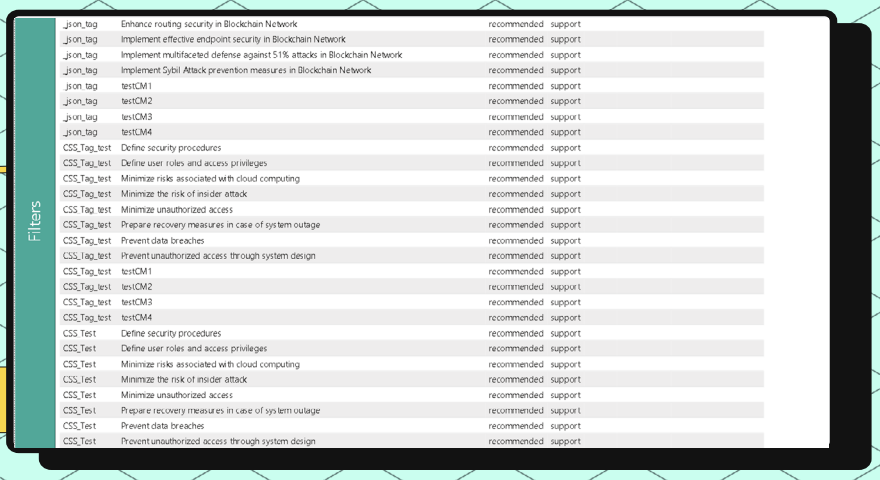
The customer is a Microsoft-based organization that leverages PowerBi to visualize data from various sources. They need the ability to re-configure and expand dashboards with minimal external support.

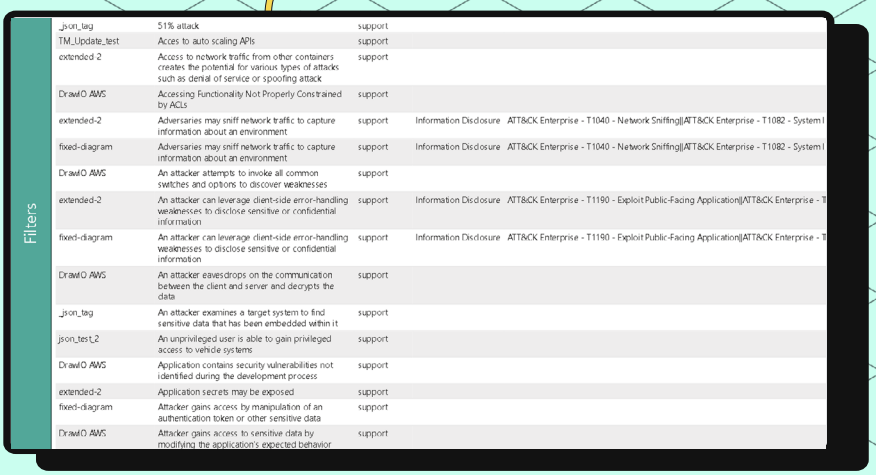
Solution

A PowerBi-integrated Python script that aggregates data from multiple IriusRisk endpoints, enabling tailored reporting and deeper insights. Customized dashboard configuration that builds upon the standard IriusRisk reports, with additional functionality for aggregating data by Business Unit, Custom Fields, and other key metrics.


Filters
Project Name
Project ID
Workflow State
Countermeasure Count
Count per countermeasure state
Countermeasure Count
recommended
implemented
state
Countermeasure Risk Count Value by risk_category
Countermeasure Risk Count Value
High
Medium
Low
Very Low
risk_category
Highest risk countermeasures
risk_category
name
High
Allow only the minimum set of protocol handle
High
Apply an AWS Managed Config Rule for EIPs a
EC2 instances within VPC
High
Apply application level payload encryption
High
Automate the process of firewall updating
High
Block traffic by default and monitor user acces
High
Catch and handle the possible exceptions
High
Check for weaknesses in 3rd party libraries
High
Choose approval process for third-party supp
High
Clear WebView's resources
Counts of countermeasures by each owner
Count of id
support
owner.username
Implemented Countermeasures by Risk Category
2
(33.33%)
4 (66.67%)
risk_category
Low
Very Low
Countermeasures by Priority and Implementation Status:
state
implemented
recommended
priority.value
high
very-high
medium
low
Count of id


Filters
Project Name
Project ID
Workflow State
Threat Count
Threat State
Count
expose
mitigate
partly mitigate
Threat State Name
Risk Count per category
risk category
High
Low
Medium
Very Low
Count of risk_category
Highest risk threats
risk
name
0 Attackers perform unauthorized network access
0 The data is exposed through the transmission channel
36 Inadequate monitoring of S3 buckets
47 Acces to auto scaling APIs
47 Attackers might impersonate legitimate users to access t
ActionTrail service
47 Compromised instances
47 Denial of actions performed
47 Impersonation of legitimate users
47 Misconfigured Auto Scaling Groups
47 Overloading the system with scaling requests, leading to
Counts of threats by each owner
Count of id
support
owner.username
Risk category of mitigated threats
2
35
(21.08%)
(1.2%)
128
(77.11%)
risk_category
High
Medium
Very Low
Low
Threats sorted by lowest mitigation
effectiveMitigation
name
0 51% attack
0 Acces to auto scaling APIs
0 Access to network traffic from other conta
potential for various types of attacks such
service or spoofing attack
0 Accessing Functionality Not Properly Cons
0 Adversaries may sniff network traffic to c
about an environment
0 An attacker attempts to invoke all commo
options to discover weaknesses
0 An attacker can leverage client-side error


Filters
_json_tag Enhance routing security in Blockchain Network recommended support
_json_tag Implement effective endpoint security in Blockchain Network recommended support
_json_tag Implement multifaceted defense against 51% attacks in Blockchain Network recommended support
_json_tag Implement Sybil Attack prevention measures in Blockchain Network recommended support
_json_tag testCM1 recommended support
_json_tag testCM2 recommended support
_json_tag testCM3 recommended support
_json_tag testCM4 recommended support
CSS_Tag_test Define security procedures recommended support
CSS_Tag_test Define user roles and access privileges recommended support
CSS_Tag_test Minimize risks associated with cloud computing recommended support
CSS_Tag_test Minimize the risk of insider attack recommended support
CSS_Tag_test Minimize unauthorized access recommended support
CSS_Tag_test Prepare recovery measures in case of system outage recommended support
CSS_Tag_test Prevent data breaches recommended support
CSS_Tag_test Prevent unauthorized access through system design recommended support
CSS_Tag_test testCM1 recommended support
CSS_Tag_test testCM2 recommended support
CSS_Tag_test testCM3 recommended support
CSS_Tag_test testCM4 recommended support
CSS_Test Define security procedures recommended support
CSS_Test Define user roles and access privileges recommended support
CSS_Test Minimize risks associated with cloud computing recommended support
CSS_Test Minimize the risk of insider attack recommended support
CSS_Test Minimize unauthorized access recommended support
CSS_Test Prepare recovery measures in case of system outage recommended support
CSS_Test Prevent data breaches recommended support
CSS_Test Prevent unauthorized access through system design recommended support


Filters
_json_tag 51% attack support
TM_Update_test Acces to auto scaling APIs support
extended-2 Access to network traffic from other containers creates the potential for various types of attacks such as denial of service or spoofing attack support
DrawIO AWS Accessing Functionality Not Properly Constrained by ACLs support
extended-2 Adversaries may sniff network traffic to capture information about an environment support Information Disclosure ATT&CK Enterprise - T1040 - Network Sniffing|ATT&CK Enterprise - T1082 - System I
fixed-diagram Adversaries may sniff network traffic to capture information about an environment support Information Disclosure ATT&CK Enterprise - T1040 - Network Sniffing|ATT&CK Enterprise - T1082 - System I
DrawIO AWS An attacker attempts to invoke all common switches and options to discover weaknesses support
extended-2 An attacker can leverage client-side error-handling weaknesses to disclose sensitive or confidential information support Information Disclosure ATT&CK Enterprise - T1190 - Exploit Public-Facing Application|ATT&CK Enterprise - T
fixed-diagram An attacker can leverage client-side error-handling weaknesses to disclose sensitive or confidential information support Information Disclosure ATT&CK Enterprise - T1190 - Exploit Public-Facing Application|ATT&CK Enterprise - T
DrawIO AWS An attacker eavesdrops on the communication between the client and server and decrypts the data support
_json_tag An attacker examines a target system to find sensitive data that has been embedded within it support
json_test_2 An unprivileged user is able to gain privileged access to vehicle systems support
DrawIO AWS Application contains security vulnerabilities not identified during the development process support
extended-2 Application secrets may be exposed support
fixed-diagram Attacker gains access by manipulation of an authentication token or other sensitive data support
DrawIO AWS Attacker gains access to sensitive data by modifying the application's expected behavior support

IriusRisk