

OWASP Toronto Chapter Meetup

August 21, 2019

OWASP Security Monitoring with Azure App Gateway, Log Analytics and Azure Sentinel



Roy Kim



2019

Global Azure
BOOTCAMP



About Me

- Career
 - Consultant to mid to large enterprise
 - Tech history: .NET, SharePoint, Office 365, Azure
- Independent Consultant
- Microsoft Azure MVP
- Blog: www.roykim.ca
- Twitter: @RoyKimYYZ
- roy@roykim.ca
- Lives in Toronto, Canada



Agenda

- Tackling Application Security Risks
- Solution Design: App Gateway(WAF), Azure App Service, Log Analytics, Alerting, Security Center, Azure Sentinel
- OWASP ZAP Penetration Testing Tool
- Demo
 - Configuration
 - ZAP Tool Attack Test
 - Monitoring with Log Analytics
 - Alerts & Security Center
 - Azure Sentinel
- Q & A

Application Security Risks

- Security threats are on the rise and constantly changing
- Applications are more complex and distributed such that there are increased attack surfaces
- What do we do?
- Where do we go for resources?

OWASP

- The [Open Web Application Security Project](#) (OWASP) is an open community dedicated to enabling organizations to develop more secure software by bring awareness, documentation and tools.
- [OWASP ModSecurity Core Rule Set \(CRS\)](#) is a set of generic attack detection rules for use with ModSecurity or compatible web application firewalls which aims to protect web applications from a wide range of attacks
 - **The 1st Line of Defense Against Web Application Attacks**

OWASP

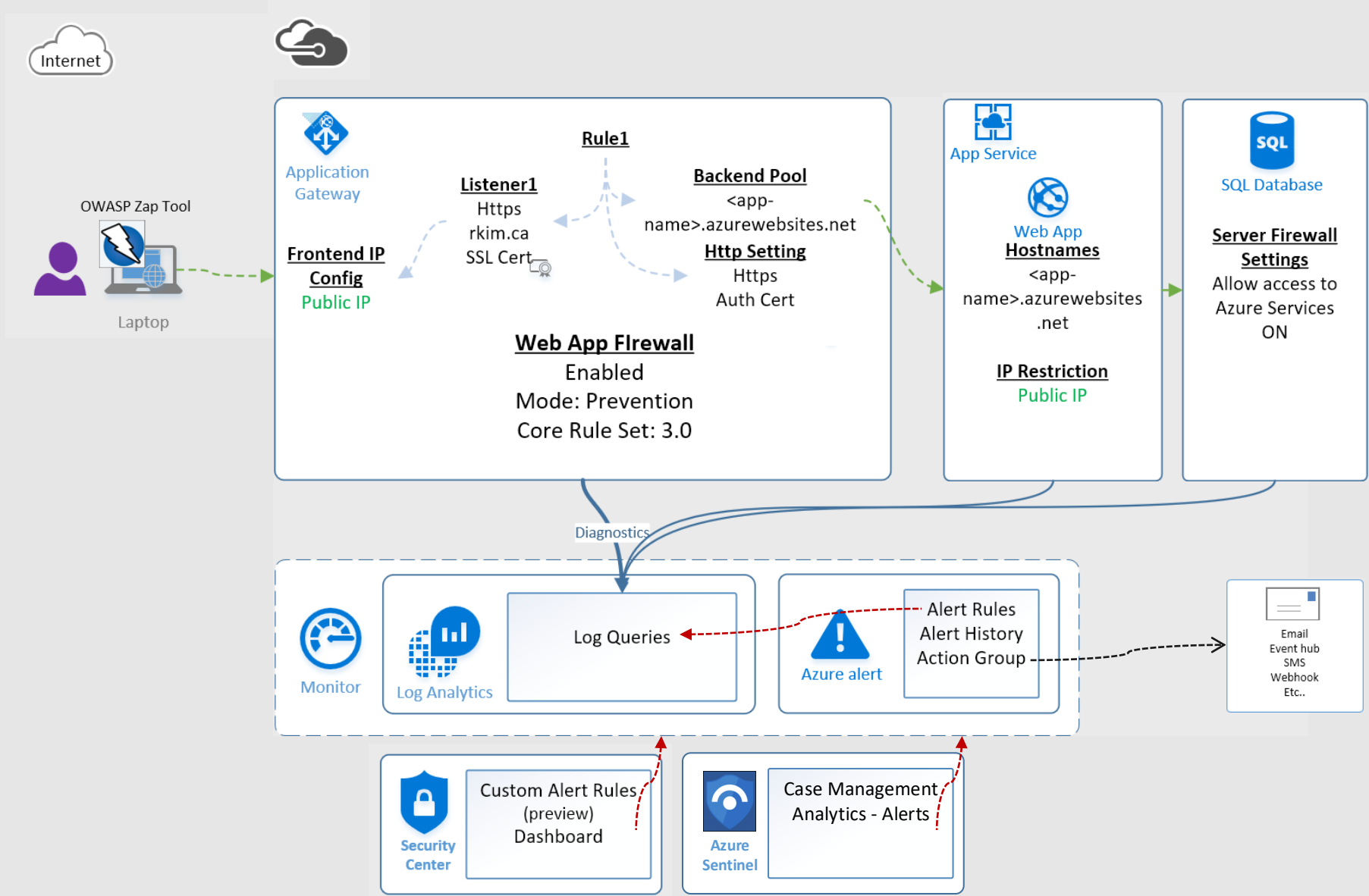
[OWASP Top 10 Most Critical Web Application Security Risks](#)

- Adopting the OWASP Top 10 is perhaps the most effective first step towards changing the software development culture within your organization into one that produces secure code.
 - 1) [A1:2017-Injection](#)
 - 2) [A2:2017-Broken Authentication](#)
 - 3) [A3:2017-Sensitive Data Exposure](#)
 - 4) [A4:2017-XML External Entities \(XXE\)](#)
 - 5) [A5:2017-Broken Access Control](#)
 - 6) [A6:2017-Security Misconfiguration](#)
 - 7) [A7:2017-Cross-Site Scripting \(XSS\)](#)
 - 8) [A8:2017-Insecure Deserialization](#)
 - 9) [A9:2017-Using Components with Known Vulnerabilities](#)
 - 10) [A10:2017-Insufficient Logging&Monitoring](#)

OWASP ZAP Penetration Testing Tool

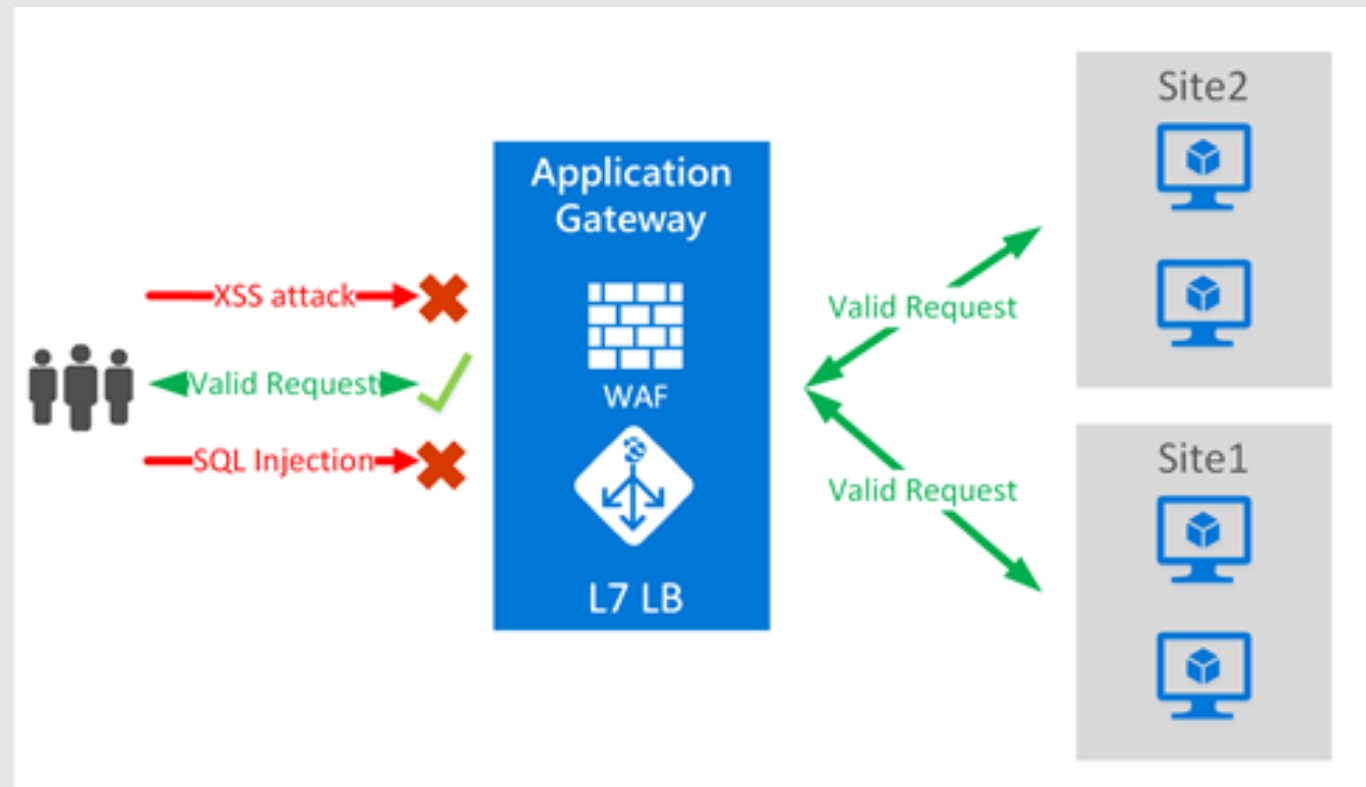
- one of the world's most popular free security tools
- actively maintained by hundreds of international volunteers^{*}.
- automatically find security vulnerabilities in your web applications while you are developing and testing your applications.
- manual security testing for experienced penetration testers.
- <https://www.zaproxy.org/>
 - New Feature: "heads up display" in browser experiences of ZAP features
 - <https://github.com/zaproxy/zap-hud>

Demo - Monitoring Solution Architecture



Azure Application Gateway

- An application delivery controller
- layer 7 load balancing/routing capabilities
- web application firewall.



Azure App Gateway's Web Application Firewall

Protect your application from web vulnerabilities and attacks without modifying backend code. Uses [OWASP ModSecurity Core Rule Set](#)

- SQL injection
- Cross site scripting
- Common attacks such as command injection, HTTP request smuggling, HTTP response splitting, and remote file inclusion attack
- HTTP protocol violations
- HTTP protocol anomalies
- Bots, crawlers, and scanners
- Common application misconfigurations (e.g. Apache, IIS, etc.)
- HTTP Denial of Service

AppGateway - Web application firewall
Application gateway

Search (Ctrl+/) Save Discard

* Firewall status
Enabled Disabled

* Firewall mode
Detection Prevention

To view your detection logs, you must have diagnostics enabled.

* Rule set
OWASP 3.0

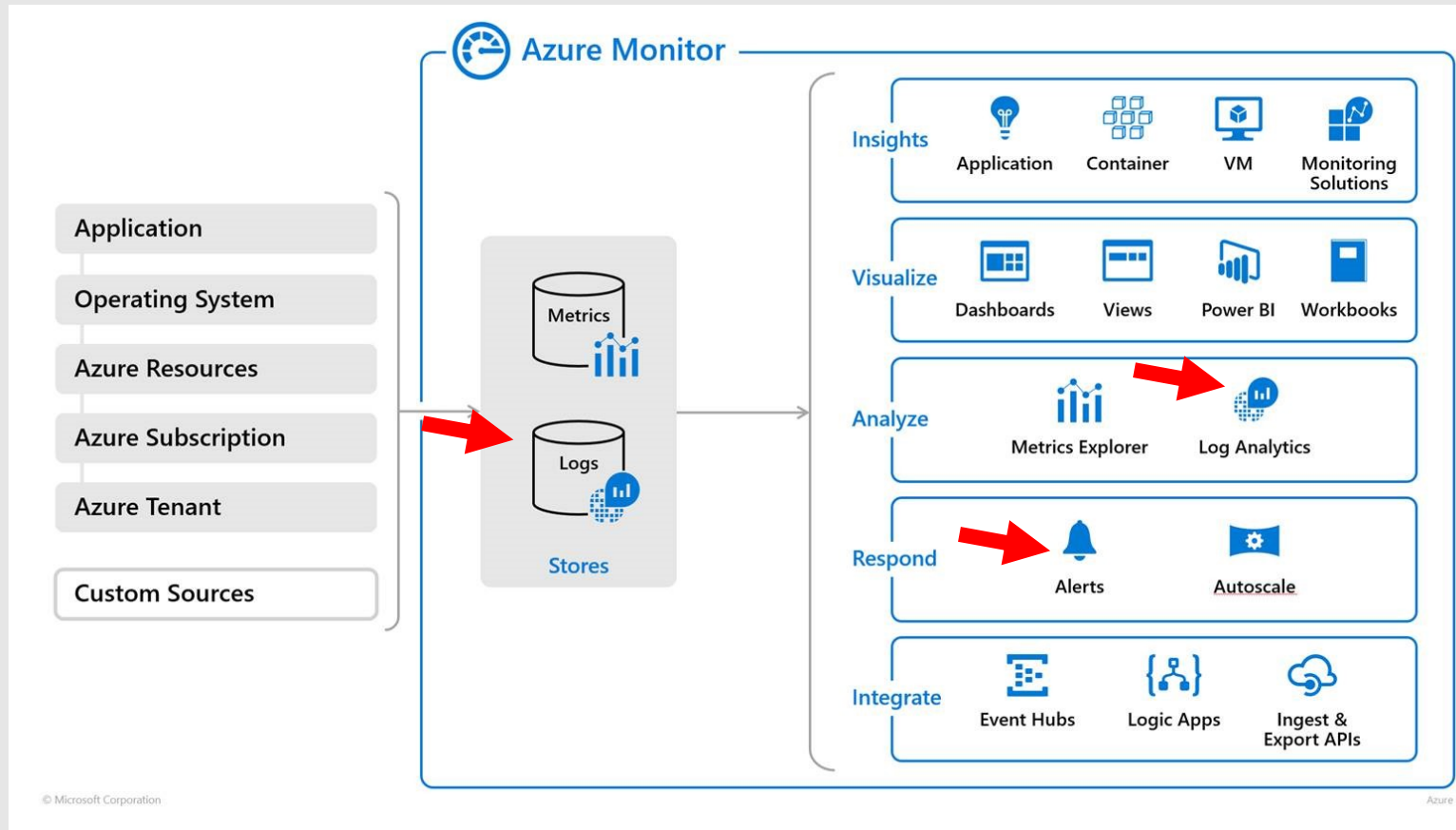
Advanced rule configuration

Search rules

ENAB...	NAME	DESCRIPTION
<input checked="" type="checkbox"/>	General	
<input checked="" type="checkbox"/>	200004	Possible Multipart Unmatched Boundary.
<input checked="" type="checkbox"/>	REQUEST-910-IP-REPUTATION	
<input checked="" type="checkbox"/>	REQUEST-911-METHOD-ENFORCEMENT	
<input checked="" type="checkbox"/>	REQUEST-912-DOS-PROTECTION	
<input checked="" type="checkbox"/>	REQUEST-913-SCANNER-DETECTION	
<input checked="" type="checkbox"/>	REQUEST-920-PROTOCOL-ENFORCEMENT	
<input checked="" type="checkbox"/>	REQUEST-921-PROTOCOL-ATTACK	
<input checked="" type="checkbox"/>	REQUEST-930-APPLICATION-ATTACK-LFI	
<input checked="" type="checkbox"/>	REQUEST-931-APPLICATION-ATTACK-RFI	
<input checked="" type="checkbox"/>	REQUEST-932-APPLICATION-ATTACK-RCE	
<input checked="" type="checkbox"/>	REQUEST-933-APPLICATION-ATTACK-PHP	
<input checked="" type="checkbox"/>	REQUEST-941-APPLICATION-ATTACK-XSS	
<input checked="" type="checkbox"/>	REQUEST-942-APPLICATION-ATTACK-SQLI	
<input checked="" type="checkbox"/>	REQUEST-943-APPLICATION-ATTACK-SESSIO...	

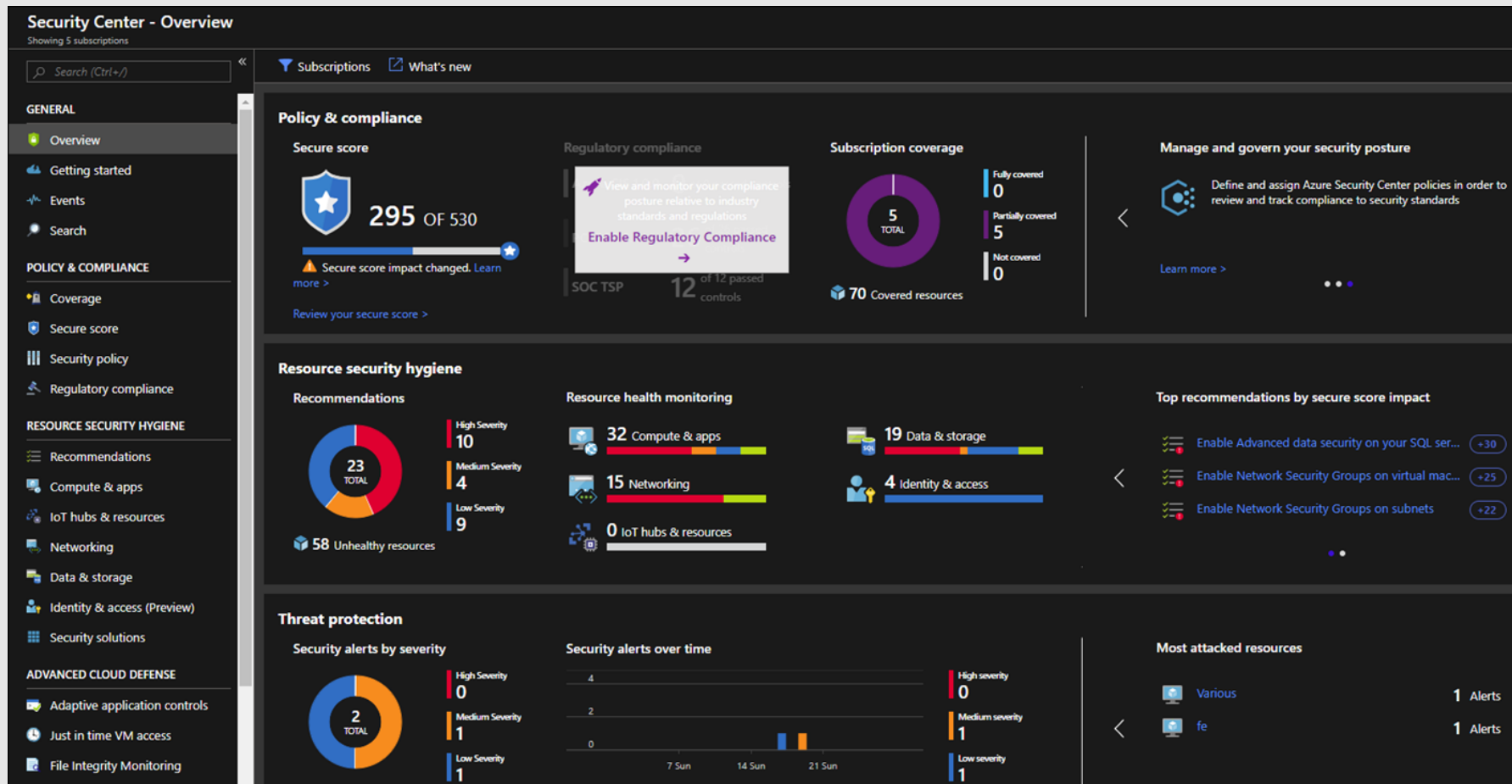
Log Analytics

- Collecting telemetry and other data from a variety of sources
- a query language and analytics engine that gives you insights



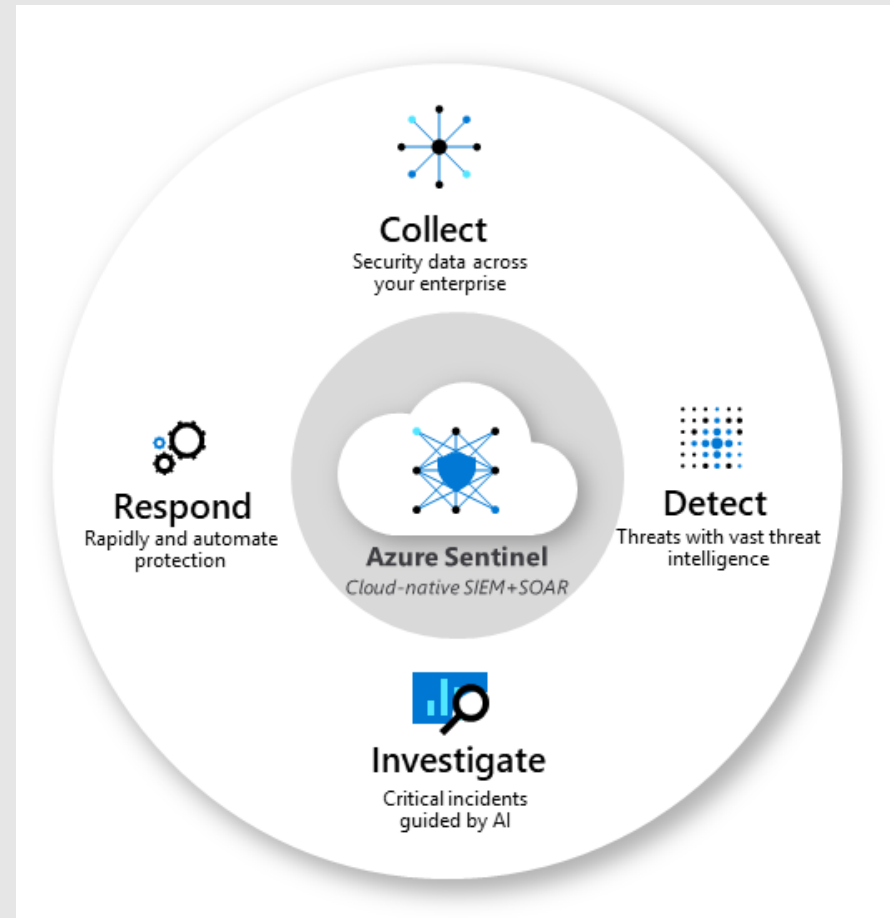
Azure Security Center

- security management system that strengthens the security posture of your data centers, and provides advanced threat protection



Azure Sentinel (preview)

- a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution



Azure Sentinel (preview)

Azure Sentinel - Overview

Selected workspace: 'rkimOMS' - PREVIEW

Search (Ctrl+*f*) Refresh Last 7 days

1.9M ↓ 22.8K **3** ↑ 3 **3** ↑ 3

Events Alerts Cases

CASES BY STATUS

NEW (2) IN PROGRESS (1) CLOSED (RESOLVED) (0) CLOSED (DISMISSED) (0)

Events and alerts over time

Events Alerts

Category	Value
Alerts	3
AZUREMETRICS	1.8M
AZUREDIAGNO...	111.2K
APPLICATION...	24.5K
OTHERS (5)	3K

Potential malicious events

POTENTIAL MALICIOUS EVENTS: 0

OUTBOUND: 0 ▲

INBOUND AND UNKNOWN: 0 ▼

Recent cases

Test APPLICATION-ATTACK-SQLI	1 Alerts
Test APPLICATION-ATTACK-SQLI	1 Alerts
Test APPLICATION-ATTACK-SQLI	1 Alerts

Data source anomalies

ApplicationInsights

AzureDiagnostics

Democratize ML for your SecOps

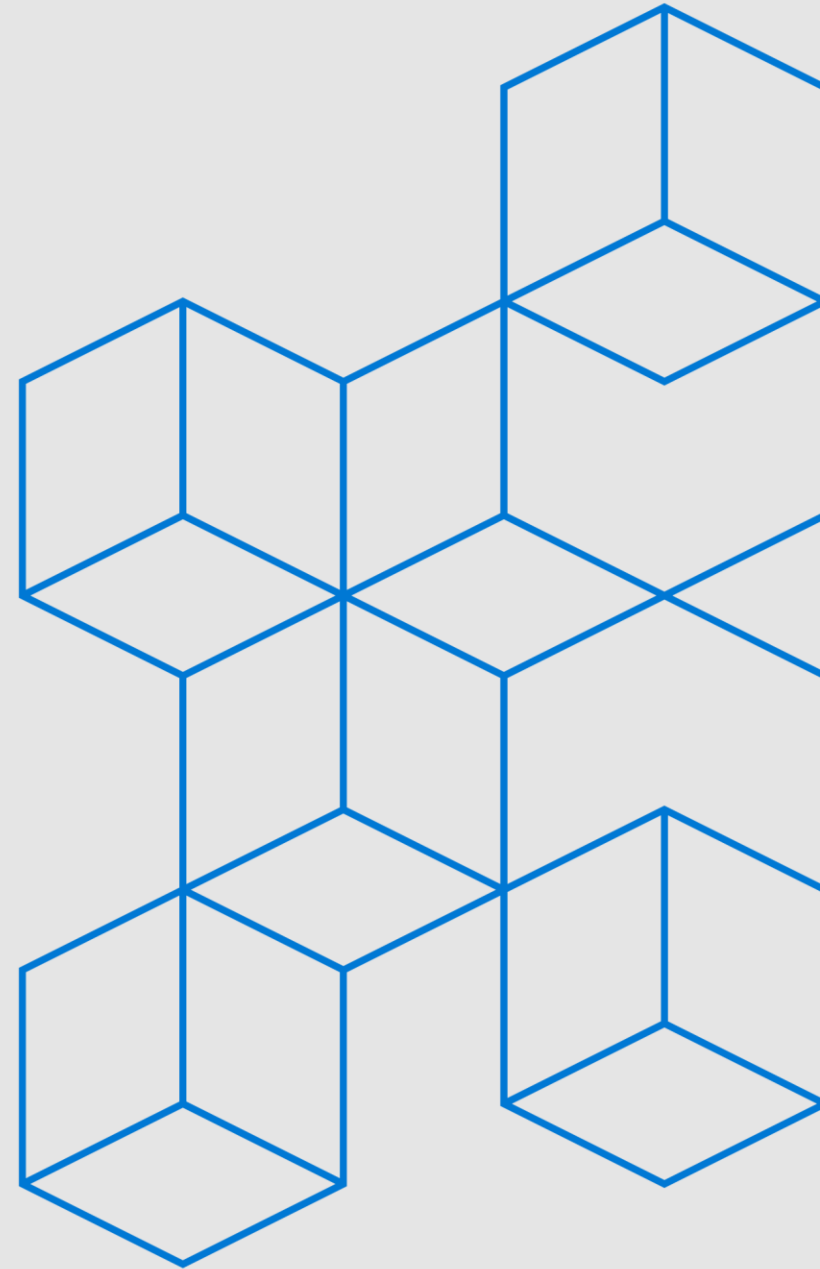
Unlock the power of AI for security professionals by leveraging MS cutting edge research and best practices in ML, regardless of your current



Demo

- Configuration
 - Penetration Test
 - Monitoring with Log Analytics
 - Alert
 - Security Center, Azure Sentinel
- * see appendix slides for demo screenshots

Roy Kim
www.roykim.ca



Conclusion

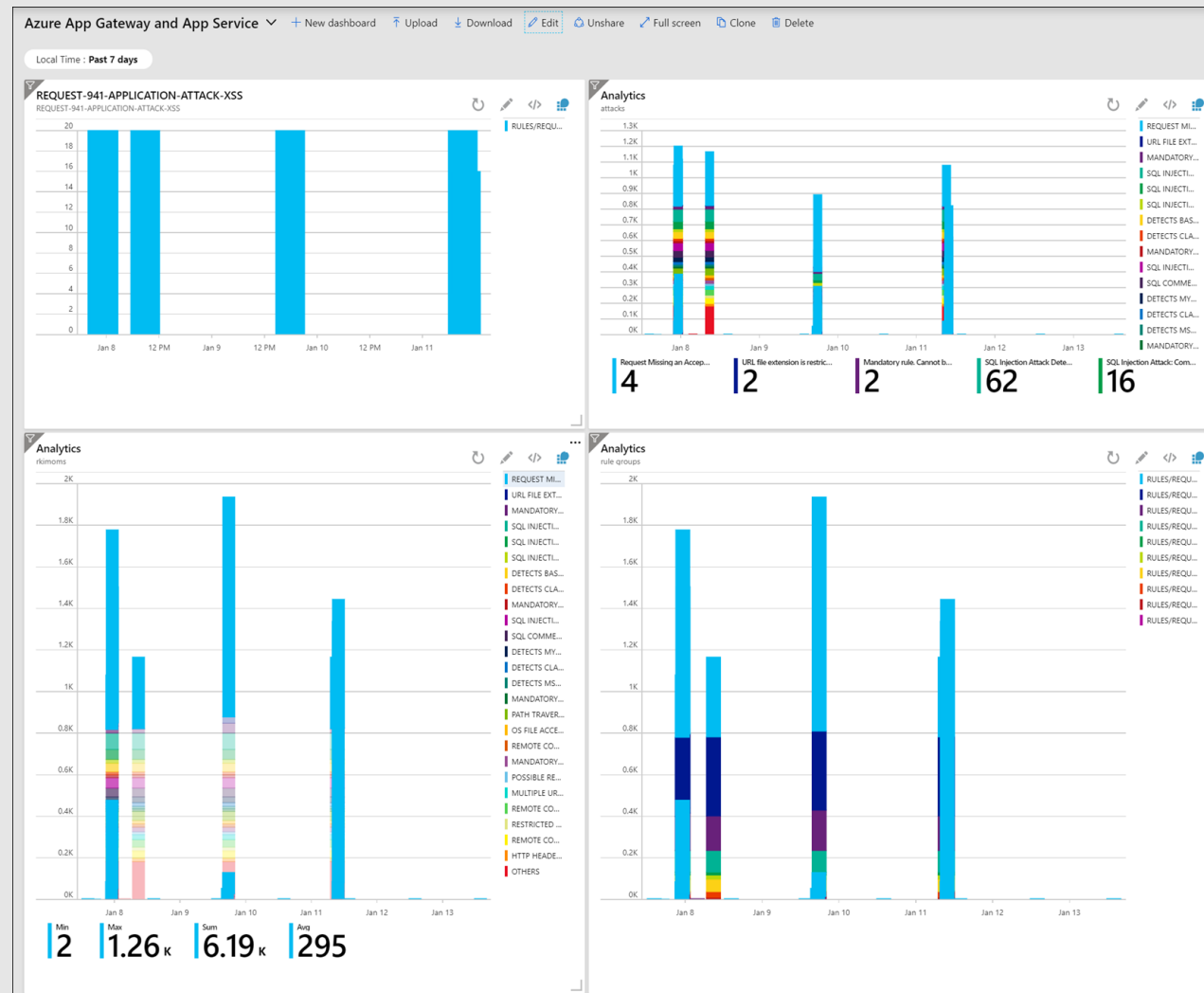
- Azure has the services and tools to rapidly build and deploy an effective security monitoring solution
- Customers can have a stable and secure experience from web attacks, threats and intrusions.
- Try it out and introduce these practices and techniques to your projects

Q&A

- Please fill out session evaluation
- roy@roykim.ca
- Blog: www.roykim.ca
- Twitter: @RoyKimYYZ

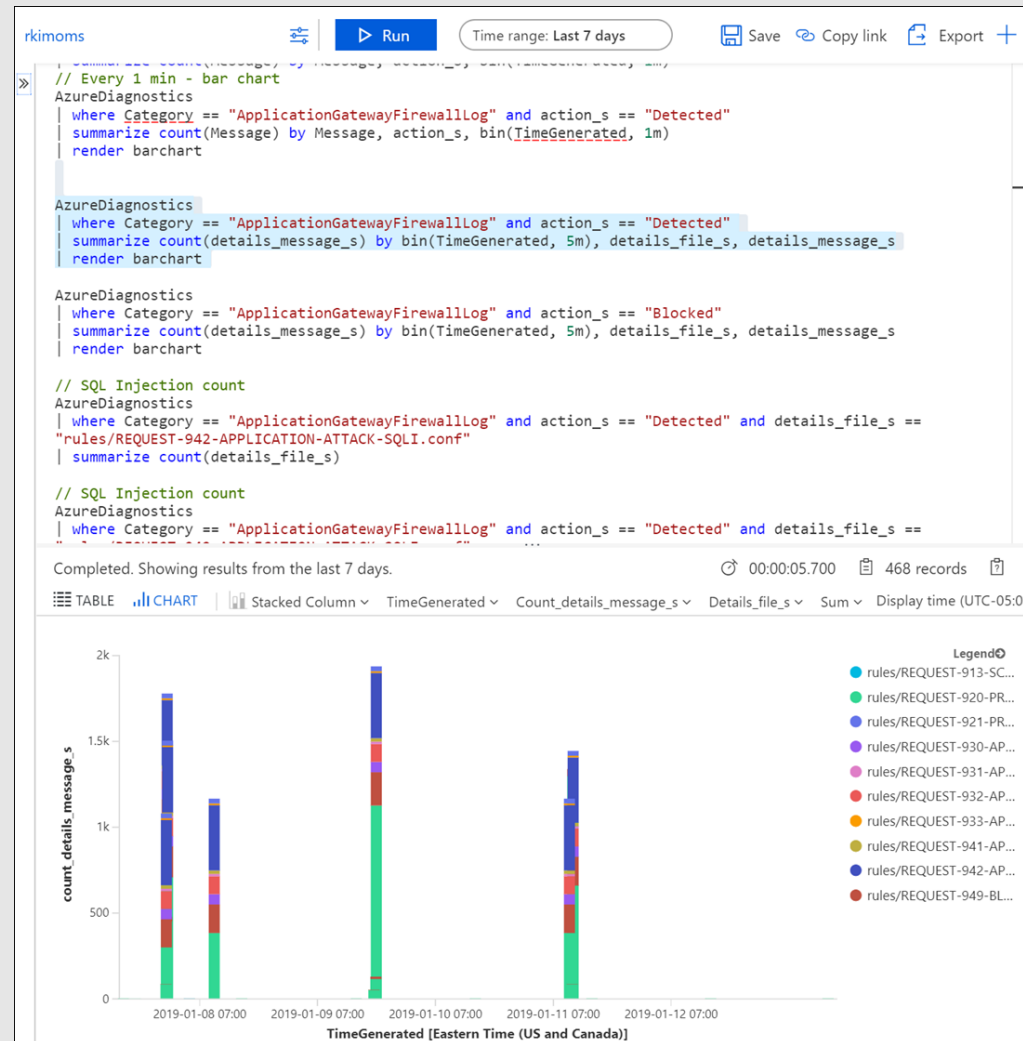
Appendix – Demo screen shots

Azure Portal Dashboard with charts from log analytics queries of WAF diagnostics



Appendix – Demo screen shots

Alert configuration using Log Analytics Query



Appendix – Demo screen shots

Alert configuration using Log Analytics Query

The screenshot displays the Azure portal interface for configuring an alert rule for an App Gateway. The main pane is titled "App Gateway 942-APPLICATION-ATTACK-SQLI" and shows the following configuration:

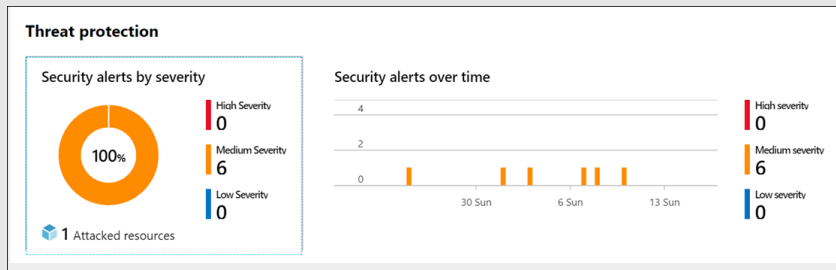
- RESOURCE:** rkimoms
- HIERARCHY:** Microsoft Azure Sponsorship > enterprise
- CONDITION:** Whenever the App Gateway 942-APPLICATION-ATTACK-SQLI is Greater than 250 c... \$ 1.50. Total \$ 1.50.
- ACTION GROUPS:** Operations (1 Email)
- ALERT DETAILS:** Alert rule name: App Gateway 942-APPLICATION-ATTACK-SQLI, Description: OWASP Rule 942-APPLICATION-ATTACK-SQLI, Severity: Warning (Sev 1), Suppress Alerts: checked, Suppress alerts for (in minutes): 30.

The right pane, titled "Configure signal logic", shows a graph of the signal logic and the following configuration:

- Search query:** AzureDiagnostics | where Category == "ApplicationGatewayFirewallLog" and action_s == "Detected" and details_file_s == "rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"
- Alert logic:** Based on: Number of results, Condition: Greater than, Threshold: 250.
- Condition preview:** Whenever the app gateway 942-application-attack-sqli is greater than 250 count
- Evaluated based on:** Period (in minutes): 5, Frequency (in minutes): 5.

Appendix – Demo screen shots

Azure Security Center – Custom Security Alert Rule using Log Analytics Query. Defined as Medium severity



Custom alert rules (Preview) > Edit custom alert rule

Edit custom alert rule

Name: Test APPLICATION-ATTACK-SQL

Description: Pen Test - App Gateway APPLICATION-ATTACK-SQL

Severity: Medium

Sources: Subscription

Criteria

Search Query: AzureDiagnostics | where Category == "ApplicationGatewayFirewallLog" and action_s == "Detected" and details_file_s == "rules/REQUEST-942-APPLICATION-ATTACK-SQL.conf"

Execute your search query now

Period: Over the last 10 minutes

Evaluation: Evaluation Frequency: Every 5 minutes

Generate alert based on: Number of results: Greater than; Threshold: 300

Suppress Alerts

OK

Home > Security Center - Overview > Security alerts

Security alerts

Filter

Some subscriptions have limited protection. Upgrade to Standard to enhance their security →

Medium severity

DESCRIPTION	COUNT	DETECTED BY	ENVIRONMENT	DATE	STATE	SEVERITY
Test APPLICATION-ATTACK-SQL	2	Alert Rule	Azure	01/11/19	Active	Medium
Test APPLICATION-ATTACK-SQL	2	Alert Rule	Azure	01/09/19	Active	Medium
Test APPLICATION-ATTACK-SQL	12	Alert Rule	Azure	01/08/19	Active	Medium
Test APPLICATION-ATTACK-SQL	15	Alert Rule	Azure	01/07/19	Active	Medium
Test APPLICATION-ATTACK-SQL	15	Alert Rule	Azure	01/04/19	Active	Medium
Test APPLICATION-ATTACK-SQL	13	Alert Rule	Azure	01/01/19	Active	Medium
APPLICATION-ATTACK-SQL	11	Alert Rule	Azure	12/26/18	Active	Medium
APPLICATION-ATTACK-SQL	4	Alert Rule	Azure	12/25/18	Active	Medium