OWASP Toronto Chapter Meetup

August 21, 2019

2019 Global Azure BOOTCAMP

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

Roy Kim

Microsoft® MVP Most Valuable Professional

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

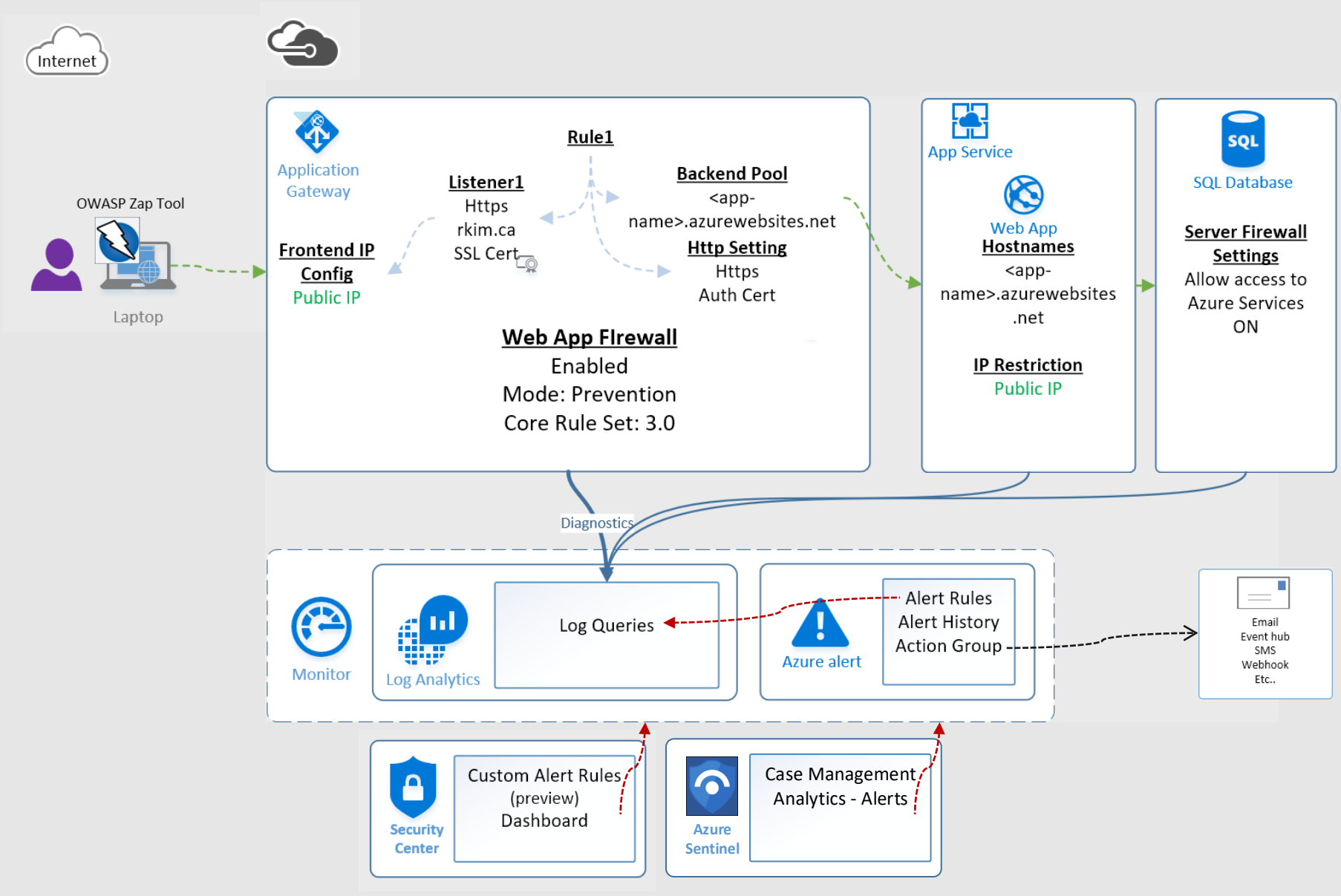
- Adopting the OWASP Top 10 is perhaps the most effective first step towards changing the software development culture within your organization into one that produces secure code.

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

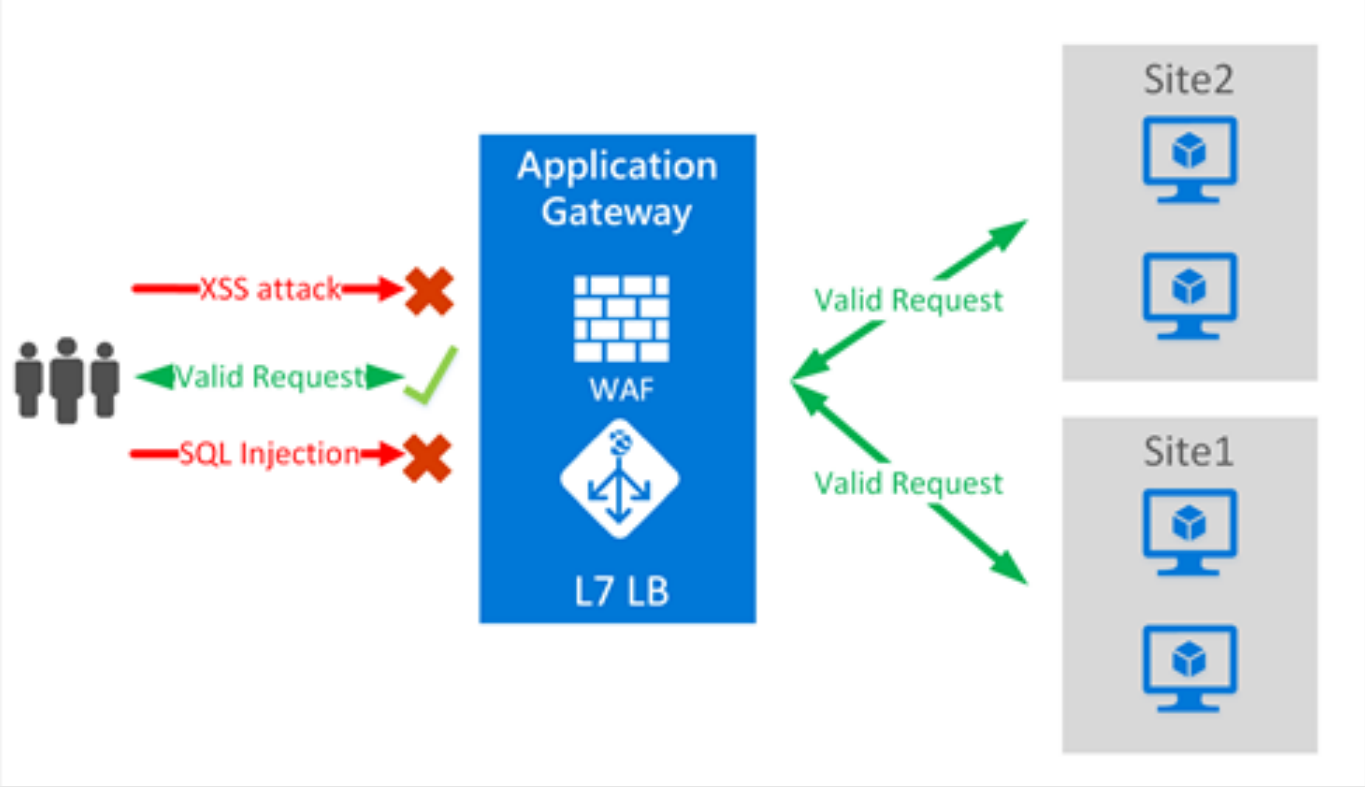
- one of the world's most popular free security tools
- actively maintained by hundreds of international volunteers*.
- automatically find security vulnerabilities in your web applications while you are developing and testing your applications.
- manual security testing for experienced penetration testers.
- 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

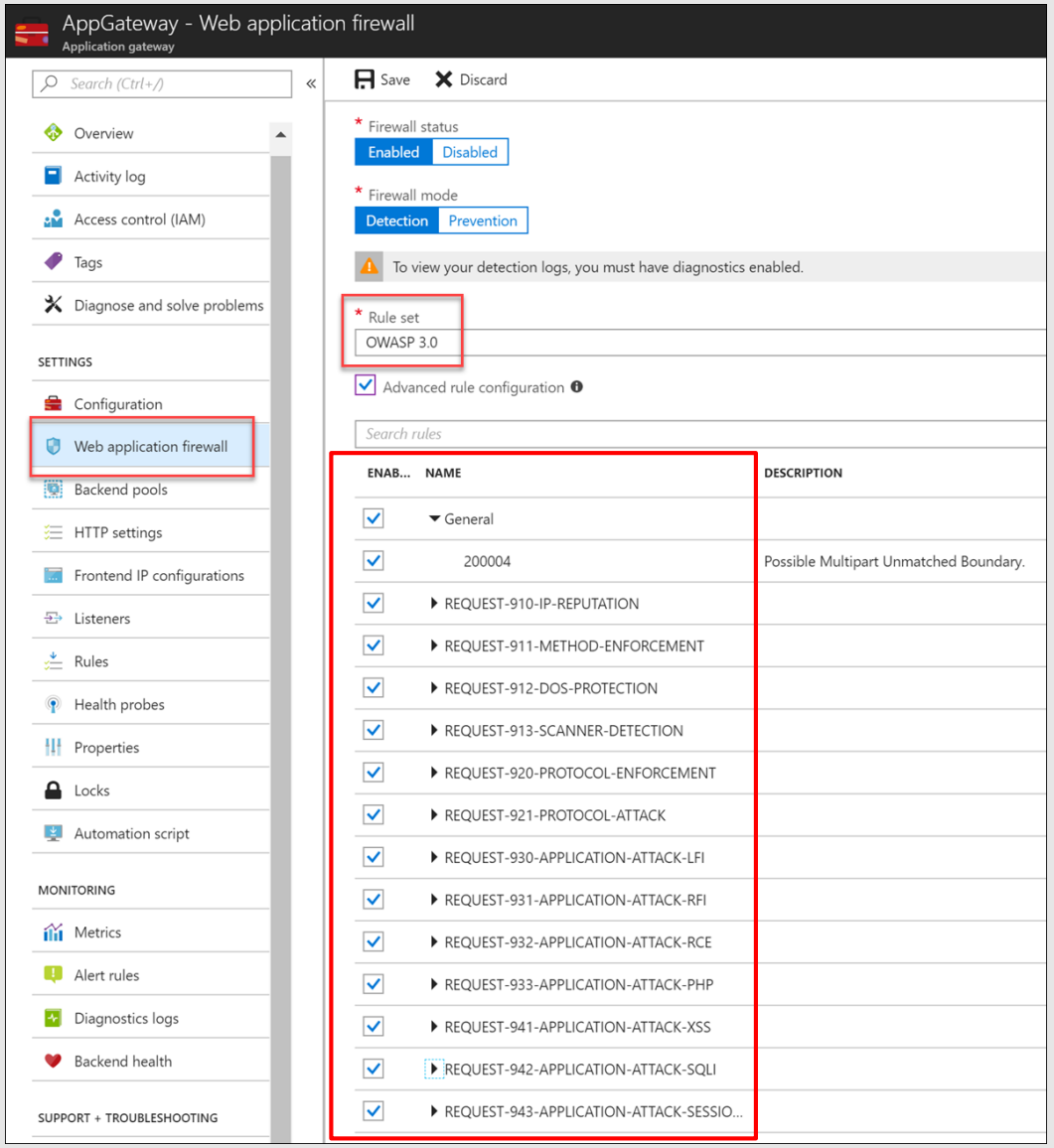
- An application delivery controller
- layer 7 load balancing/routing capabilities
- web application firewall.



Azure App Gateway's Web Application Firewall

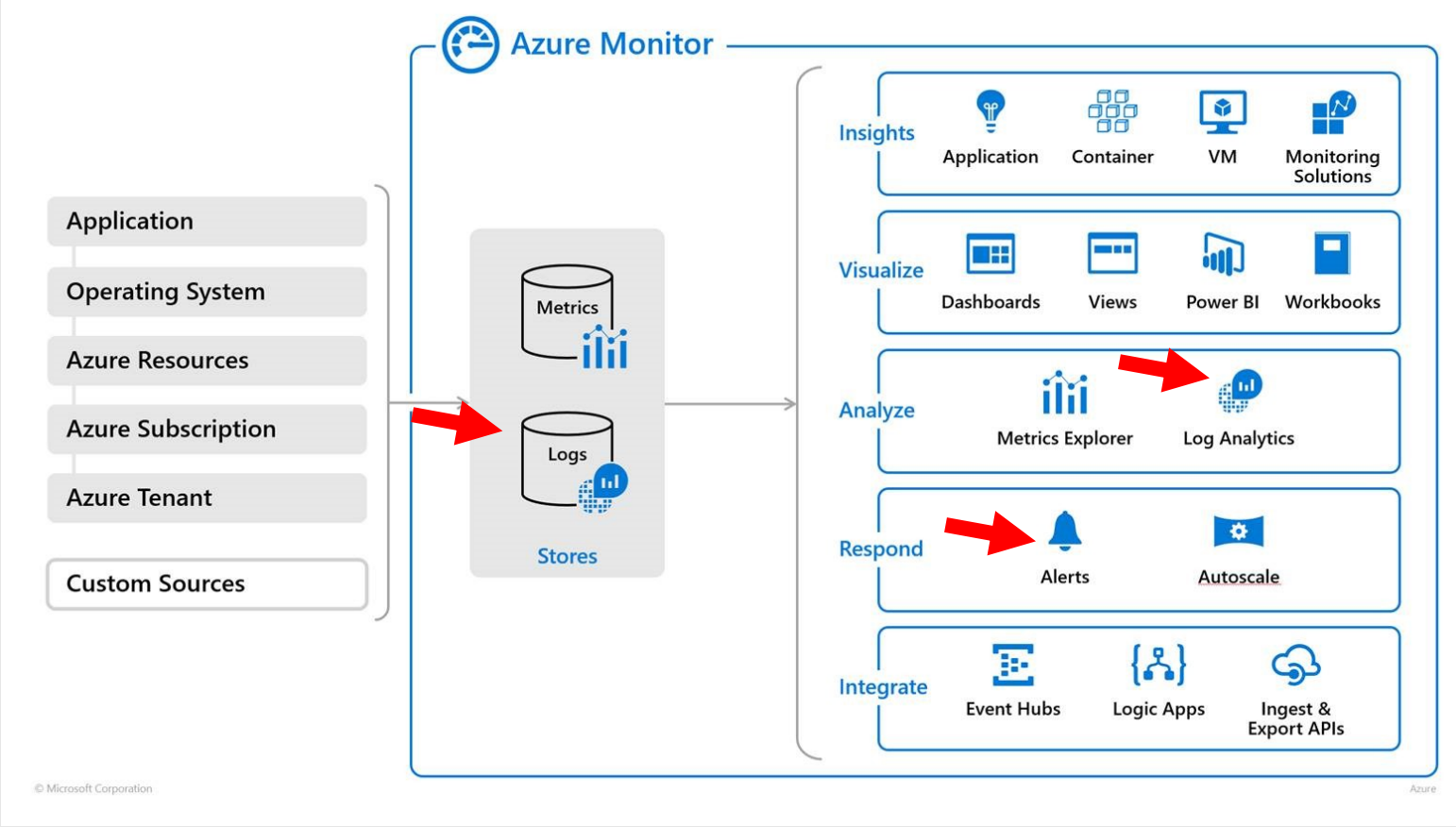
Protect your application from web vulnerabilities and attacks without modifying backend code. Uses OWASP ModSecurity Core Rule Set

- 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



Log Analytics

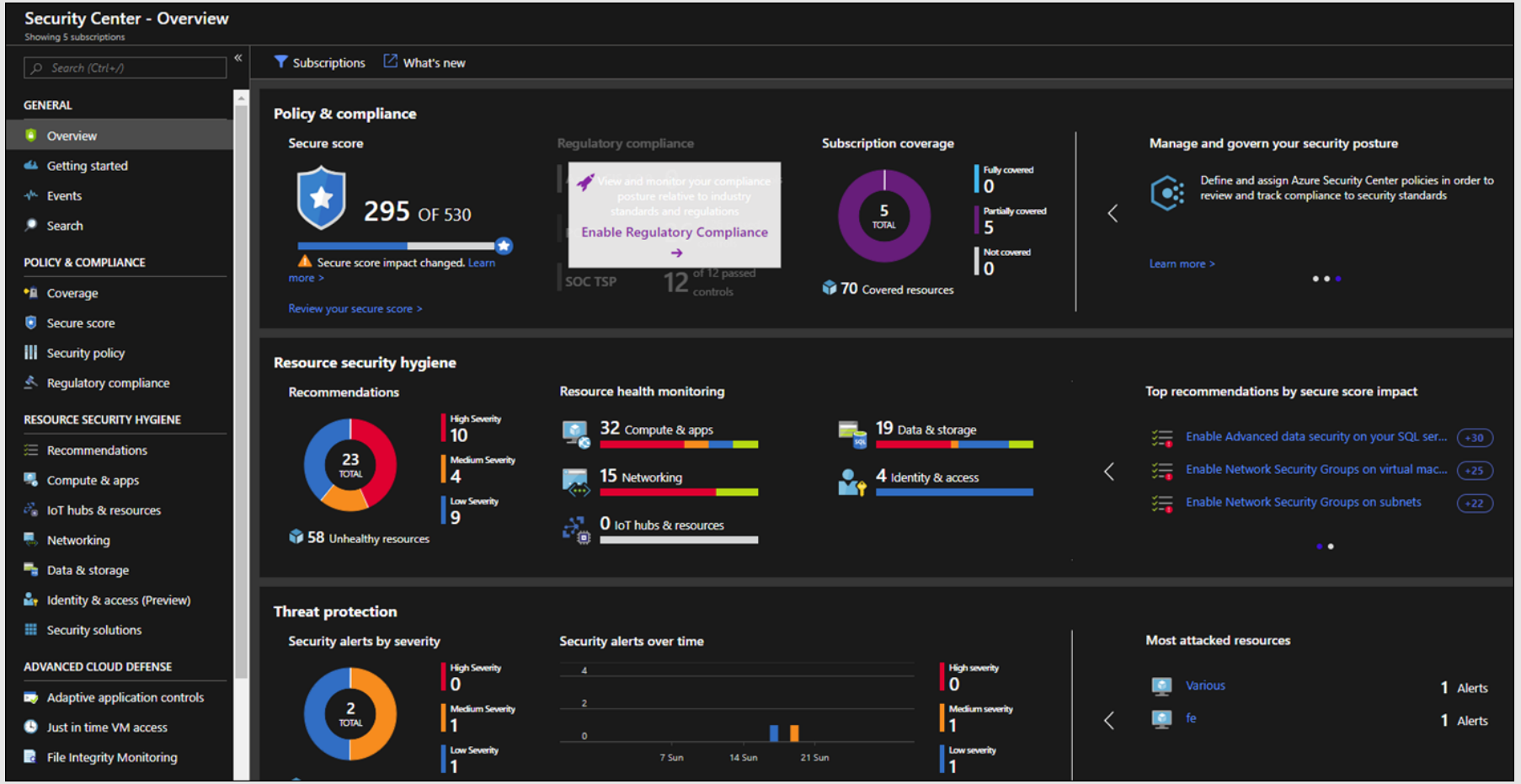
- Collecting telemetry and other data from a variety of sources
- a query language and analytics engine that gives you insights



https://docs.microsoft.com/en-us/azure/azure-monitor/azure-monitor-rebrand#log-analytics-redefinition

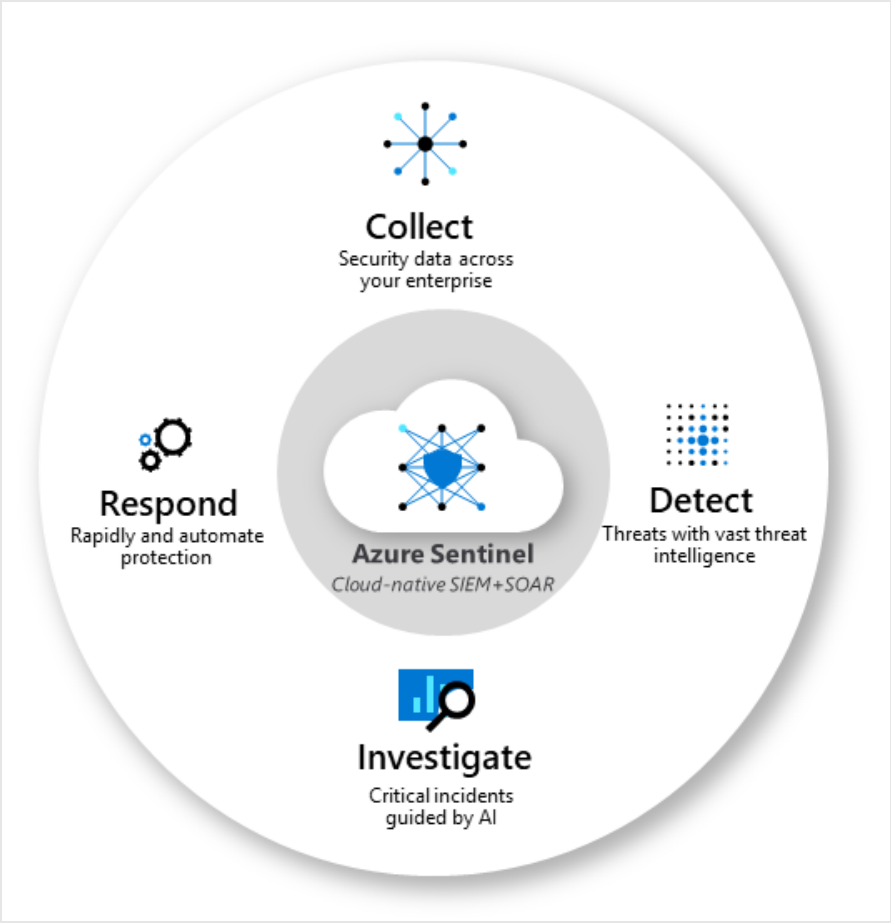
Azure Security Center

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

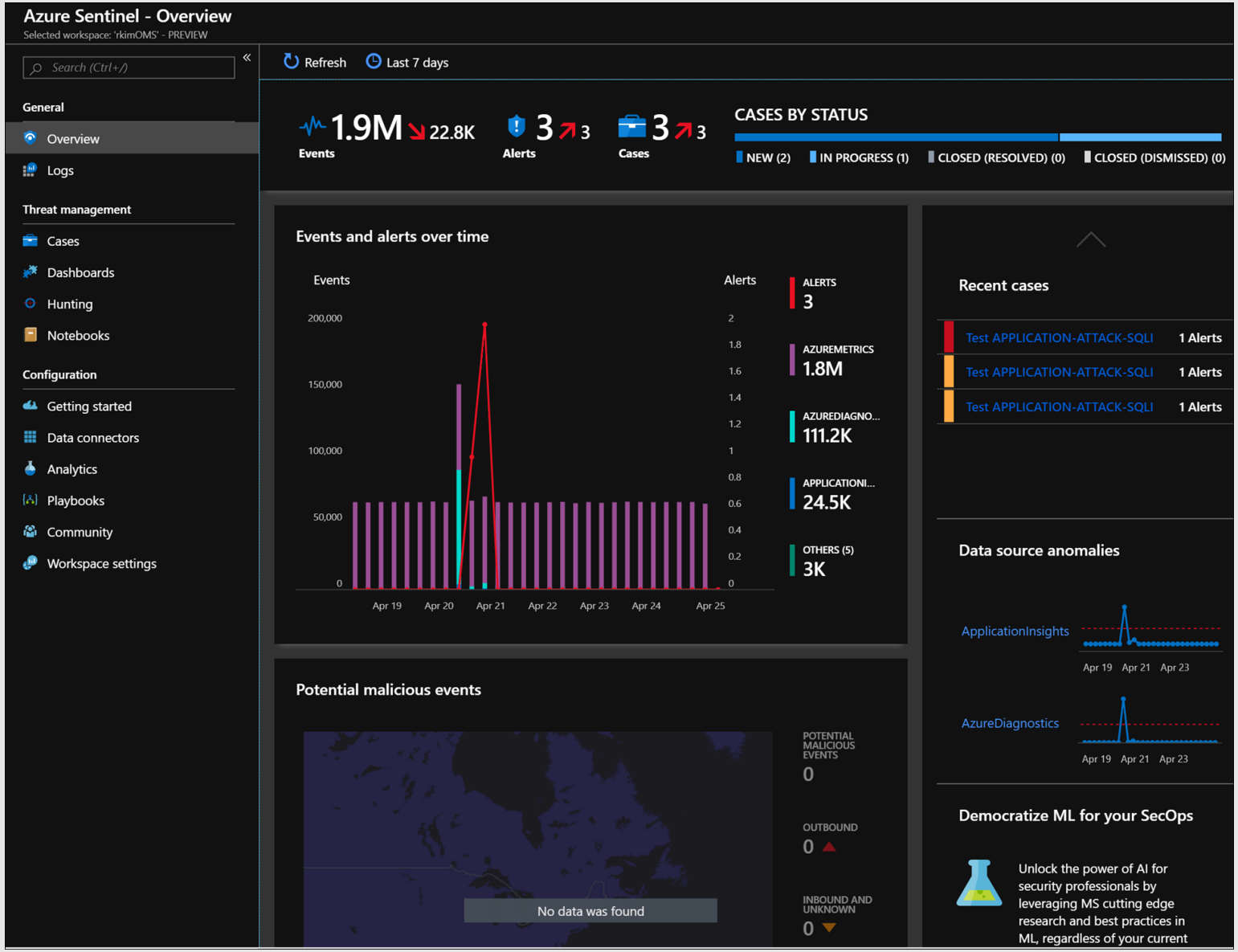


Azure Sentinel (preview)

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



Azure Sentinel (preview)



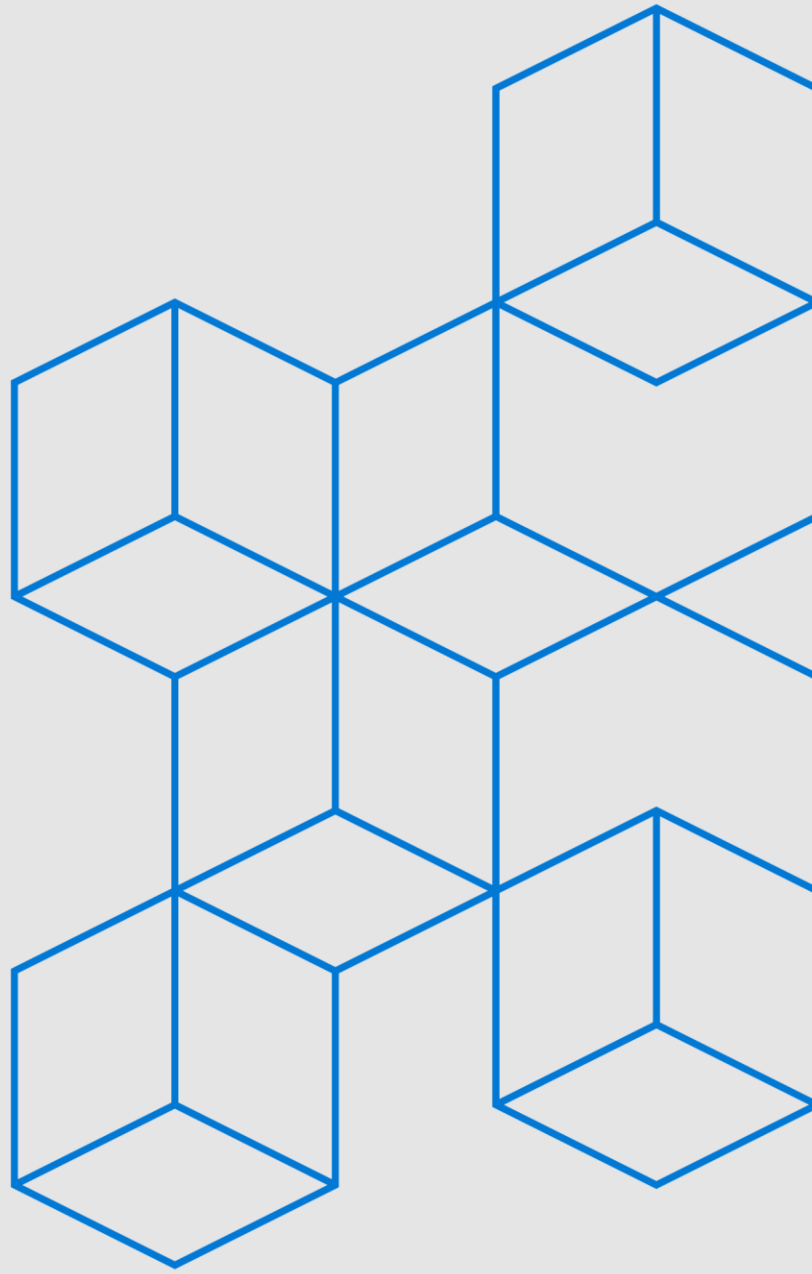
Microsoft

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

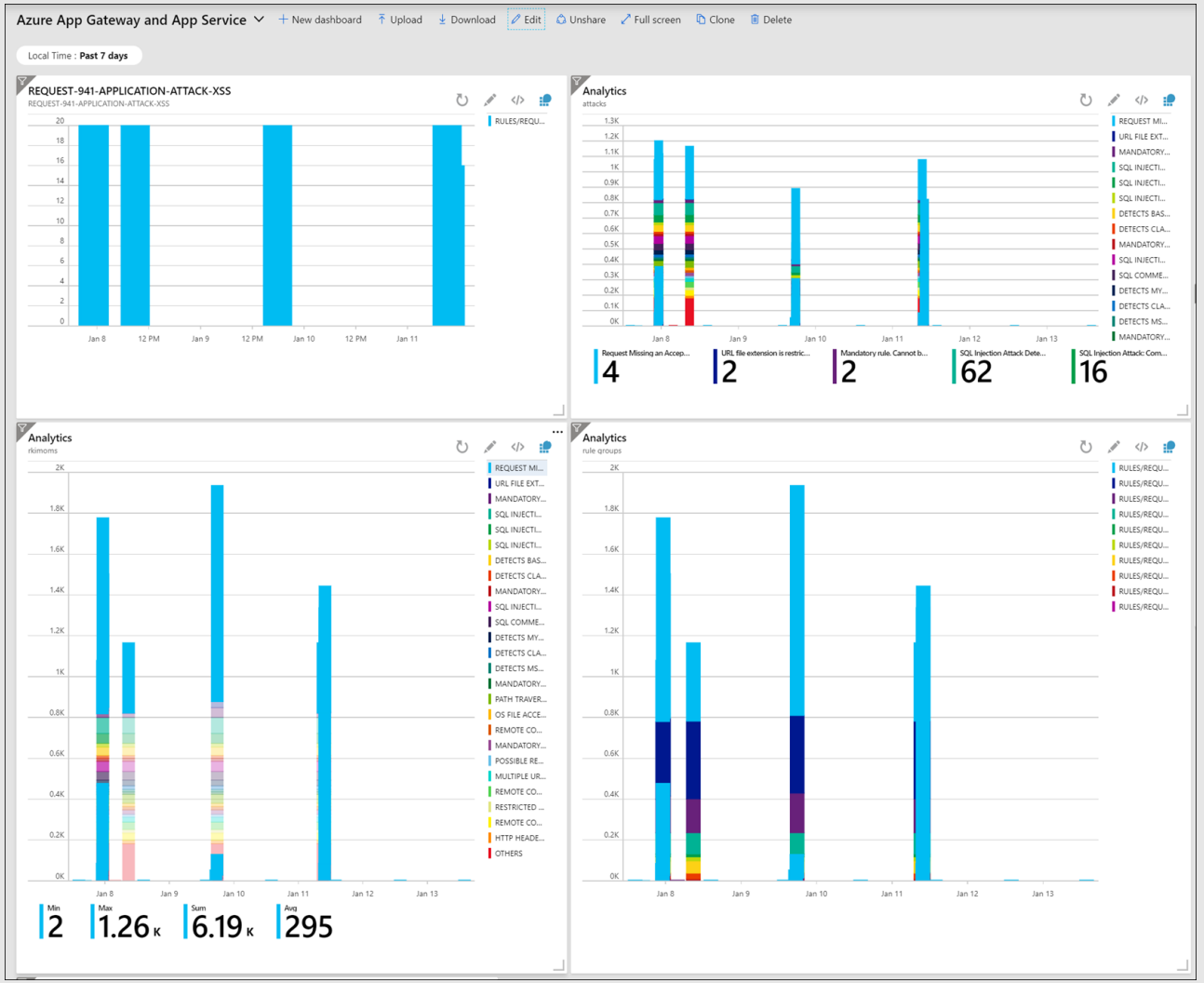
- Azure has the services and tools to rapidly build and deploy an effective security monitoring solution
- Customers can have a stable and secure experience from web attacks, threats and intrusions.
- Try it out and introduce these practices and techniques to your projects

Q&A

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

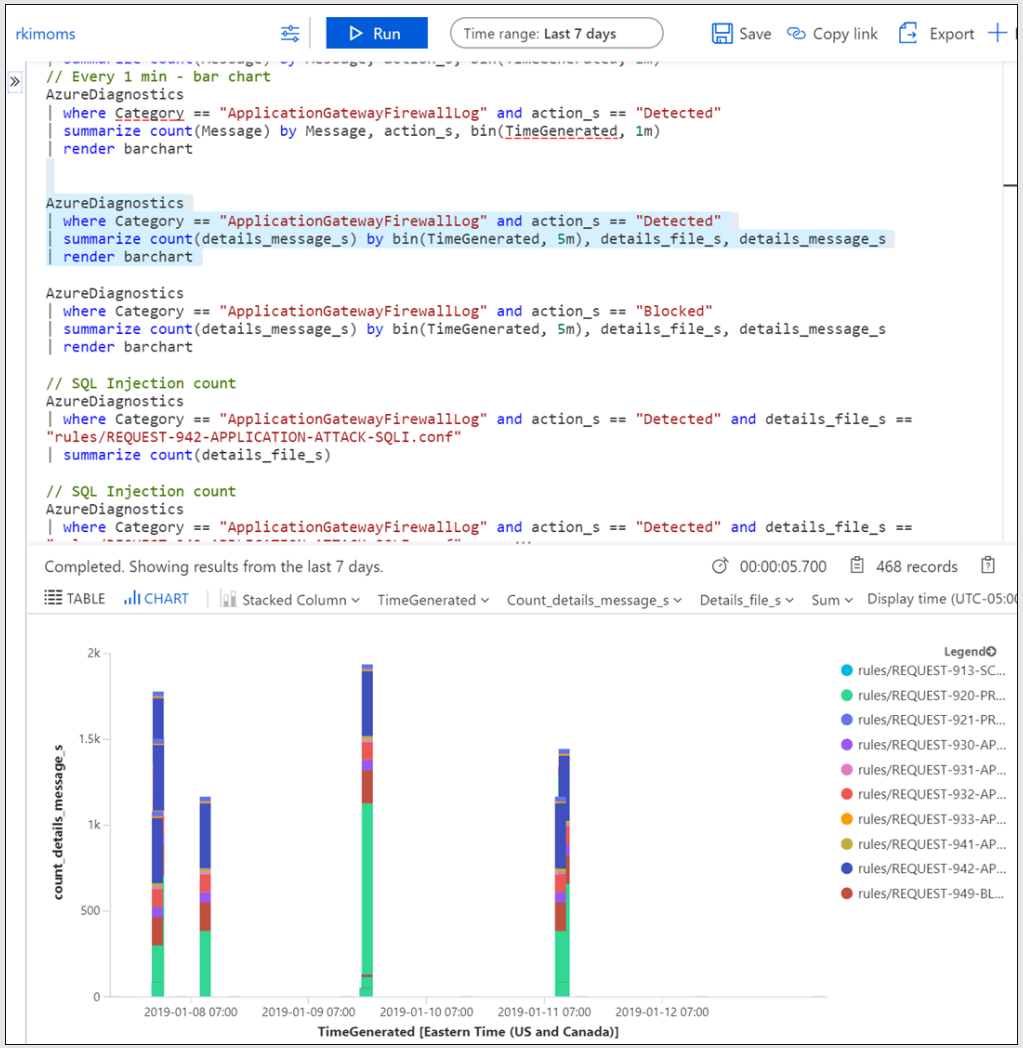
Appendix – Demo screen shots

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



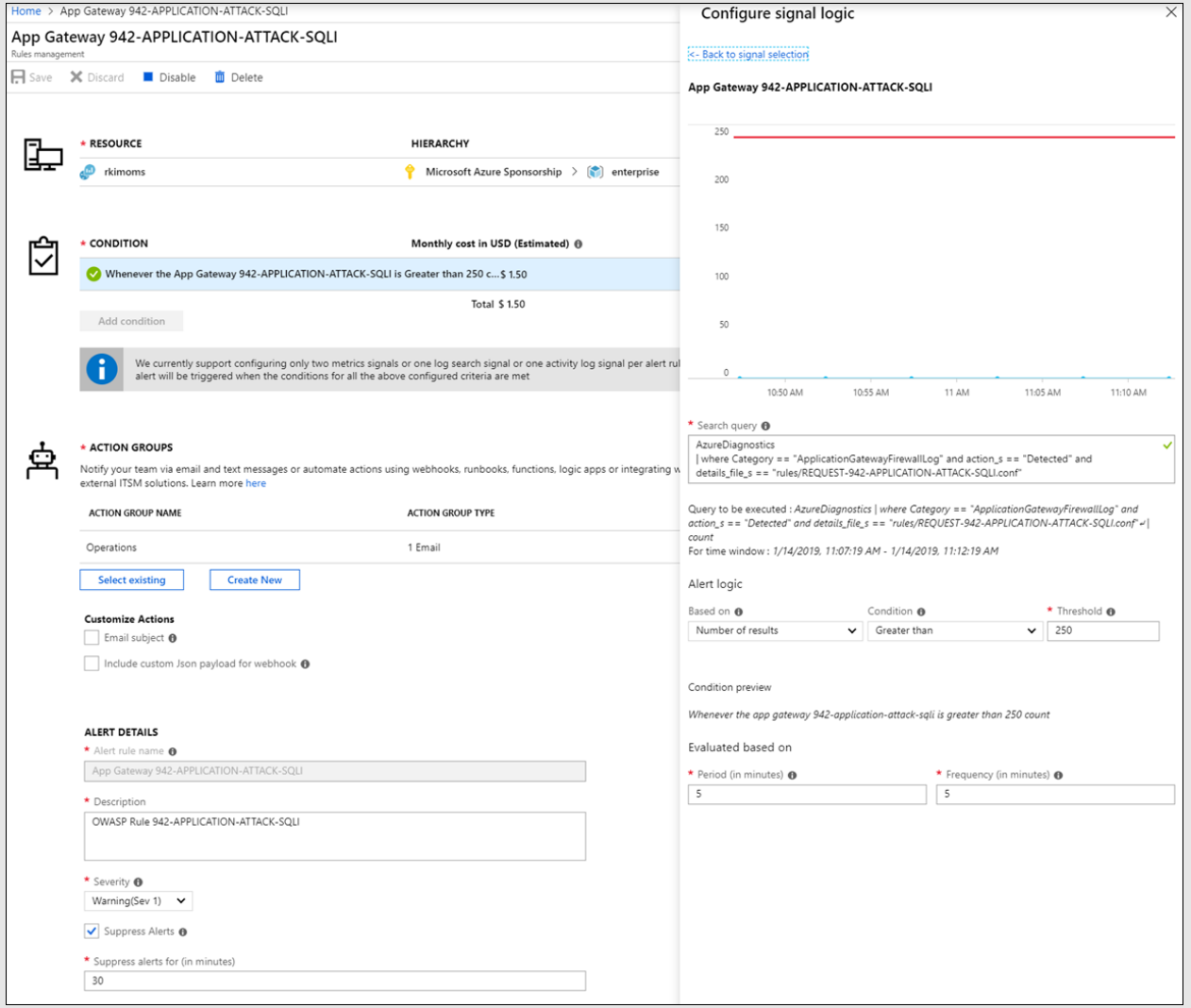
Appendix – Demo screen shots

Alert configuration using Log Analytics Query



Appendix – Demo screen shots

Alert configuration using Log Analytics Query



Appendix – Demo screen shots

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