RSAConference2019
Asia Pacific & Japan
Singapore | 16–18 July | Marina Bay Sands

BETTER.

SESSION ID: CMI-W01

Enemy At The Cloud – Is Your SOC Ready?

Abhishek Kumar

Principal Security Engineering Manager

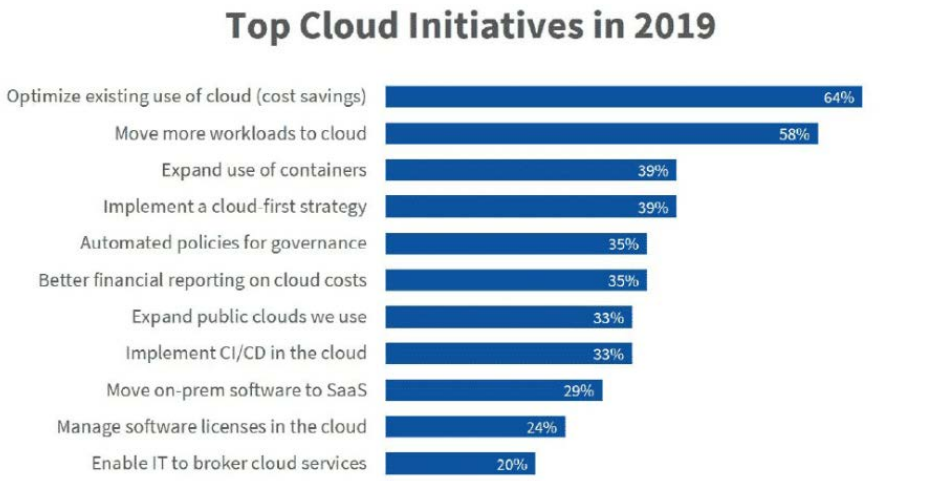
Microsoft

#RSAC

From 'Morris Worm' to 'Hacking Containers' – The Evolution Continues

- Cloud is ever present, ever accessible
  - Can be continuously, relentlessly attacked
- Provides a wide range of computing services, whatever may be your choice
  - A wide surface area to attack
- Enables rapid development and deployment, developers love it
  - Easy to make mistakes, configuration errors
- Cloud consumption is rapidly increasing
  - Makes it a super attractive target

Source: RightScale 2019 State of the Cloud Report from Flexera



Source: RightScale 2019 State of the Cloud Report from Flexera

As Cloud Consumption Increases, The Threats Too

The old ones are still relevant,
Password Brute Force
DDoS
SQL Injection
Phishing
Malware/Ransomware
Credential Stealing

And there are new ones,
Crypto Miners
Harvesting secrets/ Subscription keys
Password Spray
File Less Attacks
Software Supply Chain Hacks
Cloud Configuration Errors

WannaMine Cryptomining: Harmless Nuisance or Disruptive Threat?

January 25, 2018 Ryan McCombs, Jason Barnes, Karan Sood, and Ian Barton From The Front Lines

Yet another AWS config fumble: Time Warner Cable exposes 4 million subscriber records

US cable giant the latest victim of S3 cloud security brain-fart

By Shaun Nichols in San Francisco 5 Sep 2017 at 19:40 28 SHARE ▼

System Shock: How A Cloud Leak Exposed Accenture's Business

Last updated by Dan O'Sullivan on December 12, 2018

Over 100,000 GitHub repos have leaked API or cryptographic keys

Thousands of new API or cryptographic keys leak via GitHub projects every day.

By Catalin Cimpanu for Zero Day | March 21, 2019 -- 23:21 GMT (04:51 IST) | Topic: Security

Cloud Leak: WSJ Parent Company Dow Jones Exposed Customer Data

Last updated by Dan O'Sullivan on December 12, 2018

Microsoft

Microsoft Azure users hit by 300% rise in cyber-attacks

JAMES NUNNS EDITOR

+ INCREASE / DI

But Is The 'SOC' Keeping Up and Ready?

- Gaining familiarity with Cloud involves a steep learning curve
- Hybrid environment makes detection and investigation complex
- Cloud infrastructure and services are a lot more dynamic
- Tenant and subscription model have created new boundaries
- DevOps and SRE teams make frequent changes to production environment
- Many cloud services, Many attack types
- Rapid release of new features by CSP
- Not to forget, the increasing sophistication of attacks

Let's Start By Looking At Some Cloud Monitoring Use Cases/Attacks

Tenant Level	Subscription Level	IAAS	PAAS	SAAS
1.User elevated to tenant admin 2.MFA (multi factor authentication) settings changed	1.External account added to Subscription 2.Stale account with access to Subscription 3.Attack detection service not configured properly (e.g. ASC)	1.Known hacker/malicious tool/process found 2.Account Password Hash Accessed 3.Antimalware Service Disabled 4.Brute force login attack detected 5.Communication with a malicious IP 6.TOR IP detected 7.File less attack technique detected 8.Outgoing DDoS attacks	1.Malicious Key vault access – keys enumerated 2.Anonymous Storage access 3.Activity from unfamiliar location 4.SQL Injection detected 5.Hadoop YARN exploit 6.Open management ports on Kubernetes nodes 7.Authentication disabled for App/Web services	1.A potentially malicious URL click was detected 2.Unusual volume of external file sharing 3.Password Spray login attack

Most CSP Provide A Set Of Built In Detections

Failed RDP Brute Force Attack

vm1classic

DESCRIPTION	Several Remote Desktop login attempts were detected from Windows7, none of them succeeded. Event logs analysis shows that in the last 4 minutes there were 294 failed attempts. 133 of the failed login attempts aimed at non-existent users. 1 of the failed login attempts aimed at existing users.
DETECTION TIME	Monday, July 11, 2016, 8:41:37 PM
SEVERITY	Medium
STATE	Active
ATTACKED RESOURCE	vm1classic
DETECTED BY	Microsoft
ACTION TAKEN	Detected
SOURCE	Windows7
ALERT START TIME (UTC)	07/12/2016 01:37:32
NON-EXISTENT USERS	133
EXISTING USERS	1
FAILED ATTEMPTS	294
SUCCESSFUL LOGINS	0
ATTACK DURATION	4 minutes
FAILED USER LOGONS	quest

Potential SQL Injection

samplecrmwedemo

Learn more

General information

DESCRIPTION	Potential SQL Injection was detected on your database samplecrmwedemo on server ronmatwedemo
DETECTION TIME	Sunday, 13 May 2018, 3:09:12 pm
SEVERITY	High
STATE	Active
ATTACKED RESOURCE	samplecrmwedemo
SUBSCRIPTION	
DETECTED BY	Microsoft
ACTION TAKEN	Detected
ENVIRONMENT	Azure
RESOURCE TYPE	SQL Server
SERVER	
DATABASE	
IP ADDRESS	
PRINCIPAL NAME	dev1
APPLICATION	.Net SqlClient Data Provider
VULNERABLE STATEMENT	SELECT * FROM sqli_users WHERE username = '' OR 1 = 1 --' AND password = 'dfdfdfdfdf'
THREAT ID	1

Alert

- **Mass download** — 198.51.100.113 — Charley
- **Impossible travel activity** — Charley (charley@test...
- **Activity from a Tor IP address** — 203.0.113.22 — Charley

2 apps	OPEN	Low
Microsoft Cl...	OPEN	Medium

Exposed Docker daemon detected

DOCKER-DEMO-2

Learn more

General information

DESCRIPTION	Machine logs indicate that your Docker daemon (dockerd) exposes a TCP socket. By default, Docker configuration, does not use encryption or authentication when a TCP socket is enabled. This enables full access to the Docker daemon, by anyone with access to the relevant port.
ACTIVITY TIME	Thursday, November 29, 2018, 11:01:11 AM
SEVERITY	Medium
STATE	Active
ATTACKED RESOURCE	DOCKER-DEMO-2
SUBSCRIPTION	ASC Demo (00000000-0000-0000-0000-000000000000)
DETECTED BY	Microsoft
ENVIRONMENT	Azure
RESOURCE TYPE	Virtual Machine
COMPROMISED HOST	DOCKER-DEMO-2
USER NAME	root
SUSPICIOUS PROCESS	/usr/bin/dockerd
SUSPICIOUS COMMAND LINE	/usr/bin/dockerd -H unix://var/run/docker.sock -H tcp://0.0.0.0:2375
SUSPICIOUS PROCESS ID	0x1205e

Suspicious process executed

ASCATTACKSIMU

Learn more

General information

DESCRIPTION	Machine logs indicate that the suspicious process: 'c:\users\labadmin\downloads\mimikatz_trunk\x64\mimikatz.exe' was running on the machine, often associated with attacker attempts to access credentials.'
ACTIVITY TIME	Thursday, December 6, 2018, 7:58:42 PM
SEVERITY	High
STATE	Active
ATTACKED RESOURCE	ASCATTACKSIMU
SUBSCRIPTION	[illegible]f31c-8a08-4add-bdc9-614cea92734b)
DETECTED BY	Microsoft
ENVIRONMENT	Azure
RESOURCE TYPE	Virtual Machine
COMPROMISED HOST	ASCATTACKSIMU

Logon from an unusual location

SQLITEST

Learn more

General information

DESCRIPTION	Someone logged on to your SQL server 'sqlitestlobappserver' from an unusual location.
ACTIVITY TIME	Thursday, March 21, 2019, 2:48:39 PM
SEVERITY	Medium
STATE	Active
ATTACKED RESOURCE	SQLITEST
SUBSCRIPTION	[illegible]-8a08-4add-bdc9-614cea92734b)
DETECTED BY	Microsoft
ENVIRONMENT	Azure
RESOURCE TYPE	SQL Database
CLIENT IP ADDRESS	167.220.238.70
CLIENT HOSTNAME	ANKI-LAPTOP
CLIENT PRINCIPAL NAME	anknar@microsoft.com
CLIENT APPLICATION	Microsoft SQL Server Management Studio
CLIENT IP LOCATION	Hyderabad, India
SERVICE TAG	N/A
POTENTIAL CAUSES	Unauthorized access that exploits an opening in the firewall; legitimate access from a new location.

Effective Monitoring Depends On A Deep Understanding Of Cloud Logs/Events

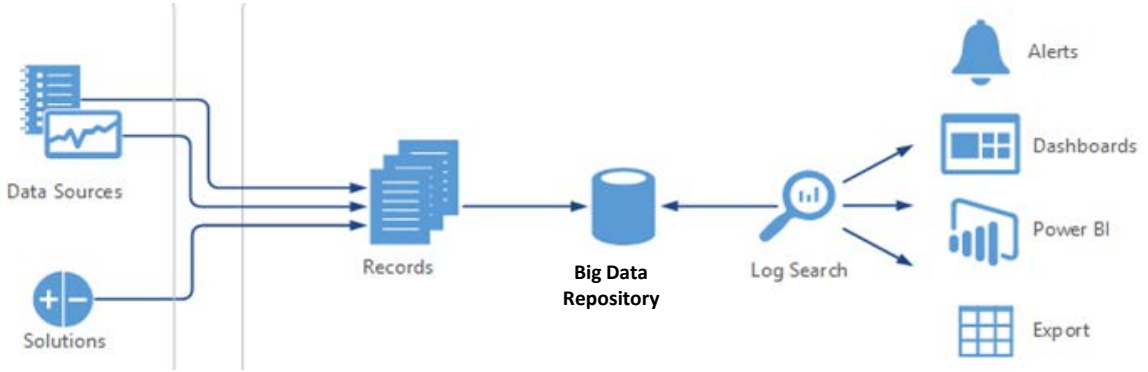
- **Control plane logs**
  - Create, Update, Delete operations for Cloud resources
- **Data plane logs**
  - Events logged as part Cloud resource usage, Windows events in a VM, SQL audit logs etc.
- **Identity related logs**
  - AuthN, AuthZ events, AAD logs etc.
- **Baked Alerts**
  - Ready to consume security alerts, ASC, CASB etc.

Sample Cloud Log

Event ID	Event Name	Subscription ID	Resource Name	Resource ID	Event Time
25185421582 63961279_fc 313bff	Malicious SQL Activity	bc9ef31c-8a08-4add-bdc9	/subscriptio ns/MINTDB	a367-527d396151 e5	6/14/2019 9:21:18 AM

Data Center	Meta Data	Prod or Dev	Owner ID	User ID	Success or Failure
WEST-US	process, command, parameters etc.	Prod	95734324-823b	Haddock	Success

- It helps to have a Raw event repository, e.g. Log Analytics
  - Can help build your custom monitoring scenarios
  - Can help SOC run investigation
  - Most cloud services provide it



Here Is A GitHub Project With Sample Cloud Detections

Why GitHub? Enterprise Explore Marketplace Pricing Search

Azure / Azure-Sentinel Watch

Code | Issues 6 | Pull requests 5 | Projects 0 | Security | Insights

Branch: master Azure-Sentinel / Detections /

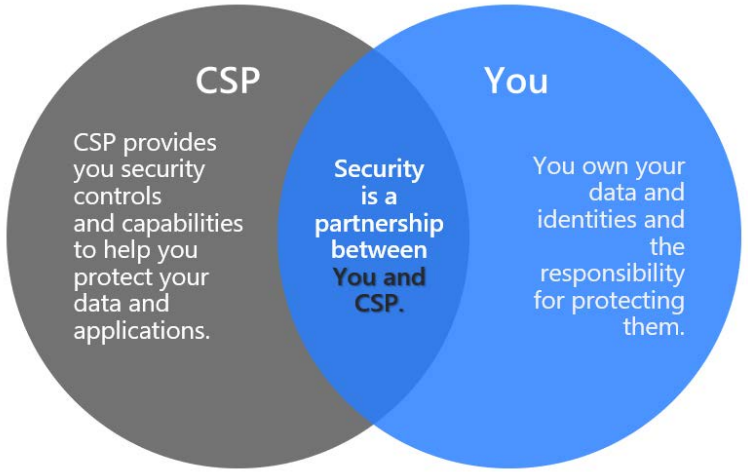
shainw Merge pull request #169 from Azure/may2019-timeseries_and_networkbeac... ...

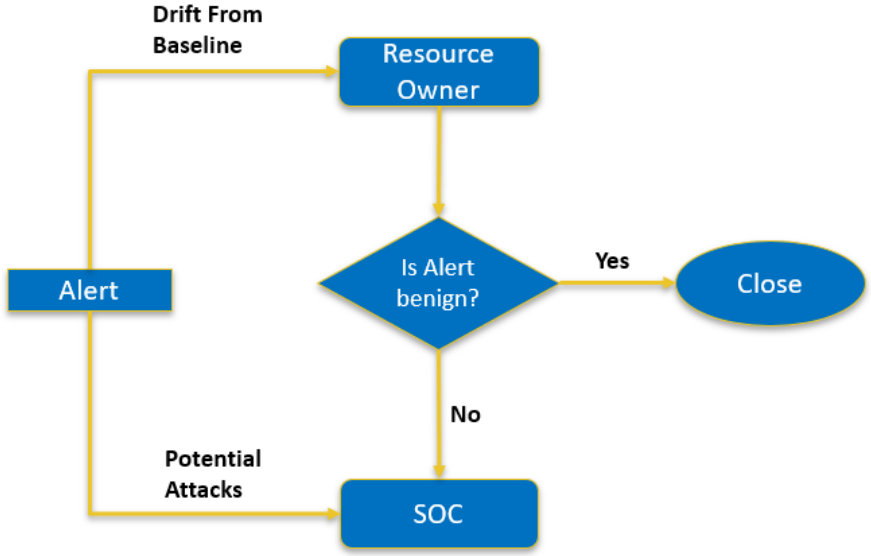
..	
AWSCloudTrail	change technique to tactic
AzureActivity	change technique to tactic
CommonSecurityLog	changing alerttriggerthreshold with scorethreshold
DnsEvents	change technique to tactic
MultipleDataSources	Merge pull request #169 from Azure/may2019-timeseries_and_networkbeac...
OfficeActivity	OfficeActivity detections and hunting from ashwin (#141)
SecurityEvent	Added missing fields for detections
SigninLogs	Azure portal brute foce (#136)
Syslog	change technique to tactic
VMConnection	Adding a couple of interesting queries I threw together while doing r... (
W3CIISLog	pushing initial version of PrivAccountTracking and some minor fixes
readme.md	Updating Detections Readme

```
// Name: brute force attack against Azure Portal
// Id: 28b42356-45af-40a6-a0b4-a554cdfd5d8a
//
// Description: This query looks for evidence of brute force activity against the Azure Portal
// by highlighting multiple authentication failures and a successful authentication within
// a given time window. (The query does not enforce any sequence - eg requiring the successful
// authentication to occur last.)
//
// We consider anything other than the following result types as authentication failures:
// 0 - successful logon
// 50125 - Sign-in was interrupted due to a password reset or password registration entry.
// 50140 - This error occurred due to 'Keep me signed in' interrupt when the user was signing-in
//
// DataSource: #SigninLogs
//
// Severity: Medium
//
// QueryFrequency: 24h
//
// QueryPeriod: 24h
//
// AlertTriggerOperator: gt
//
// AlertTriggerThreshold: 0
//
// Tactics: #InitialAccess
//
// Evidence of Azure Portal brute force attack in SigninLogs:
// This query returns results if there are more than 5 authentication failures and a successful authentication
// within a 20-minute window.
let failureCountThreshold = 5;
let successCountThreshold = 1;
let timeRange = ago(1d);
let authenticationWindow = 20m;
SigninLogs
| where TimeGenerated >= timeRange
| extend OS = DeviceDetail.operatingSystem, Browser = DeviceDetail.browser
| extend StatusCode = tostring(Status.errorCode), StatusDetails = tostring(Status.additionalDetails)
| extend State = tostring(LocationDetails.state), City = tostring(LocationDetails.city)
| where AppDisplayName contains "Azure Portal"
// Split out failure versus non-failure types
```

Incident Triage Is A Little Different In The Cloud

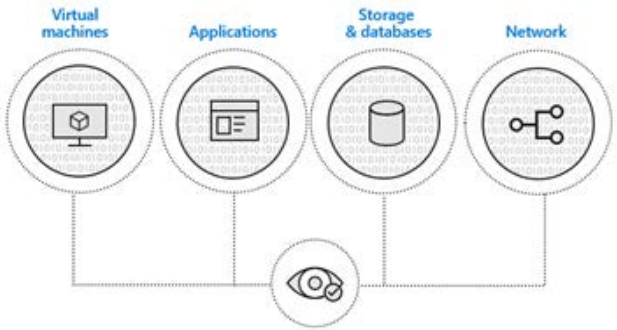
- Monitoring in cloud is about **partnership**
  - Between SOC Analysts, Cloud Resource Owners, Subscription Owners, as well as Cloud Service Provider
- SOC Analysts may sometimes need intervention from cloud resource owners
  - For getting required events for investigation
    - E.g. SQL Audit Logs etc.
  - For implementing remediation steps
    - E.g. Making changes to virtual network, disabling account etc.
- SOC Playbooks needs to be designed accordingly
- It makes sense to route 'certain' Alerts directly to 'resource owners' to reduce unnecessary load on SOC
  - They can always escalate to SOC if it is not benign





SIEM For The Cloud, or Cloud For The SIEM

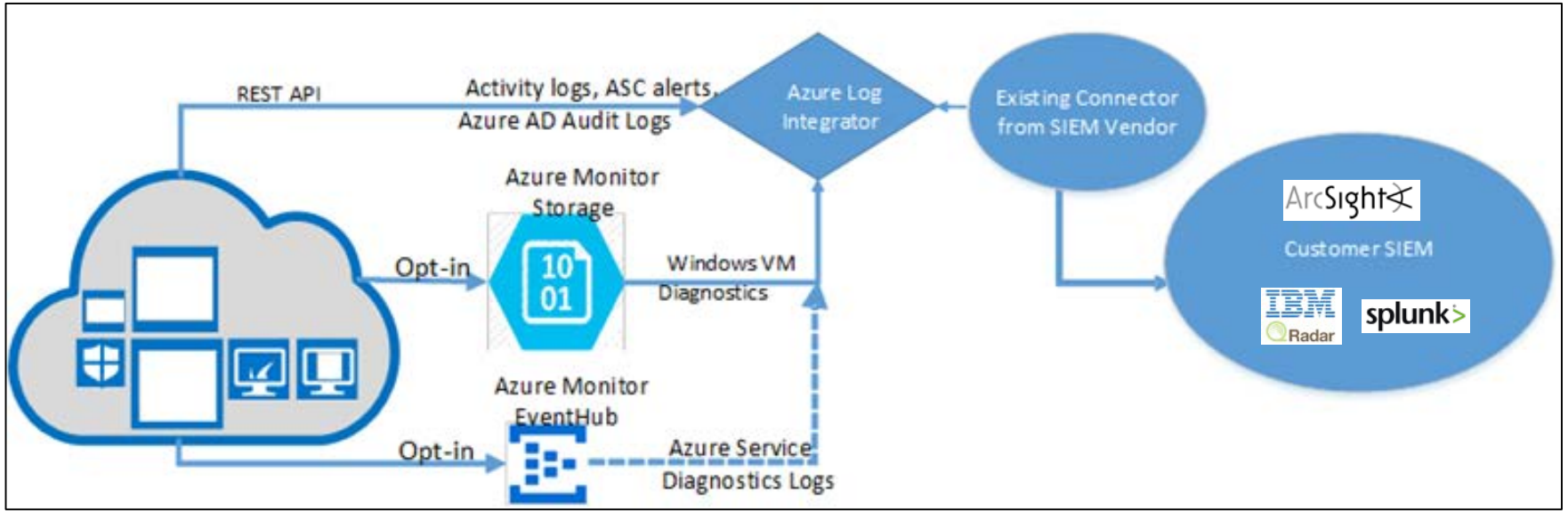
- SIEM design and architecture is evolving too
- You can start with bringing cloud events to an on-prem SIEM
  - Continue to leverage investments in existing SIEM setup
  - Major Cloud providers have connectors for popular SIEM
- Over time you can move to a Cloud based SIEM
  - Take on-prem events to cloud SIEM
  - This is undergoing rapid development, but there are early adopters
- Or you can also build your own
  - Leverage big data platform, flexible and allows for great hunt experience
  - Useful for large enterprises which generate high volume and variety of events
- It is better to first start with native cloud alerting, understand the use cases, develop skills, then transition to SIEM integration.



Challenges

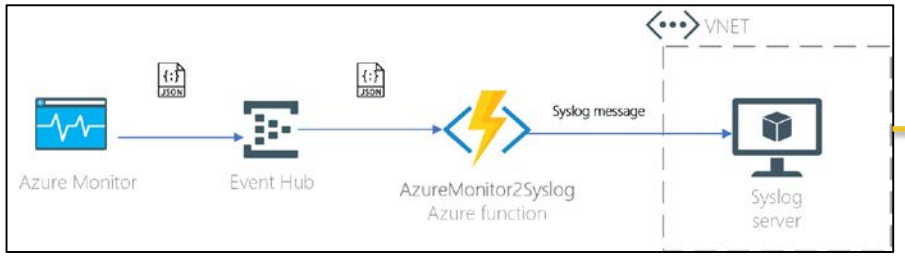
- Inadequate connectors for existing SIEM platforms
- Multi Cloud environment
- Skill deficit
- Limited access to events from across subscriptions
- Large volume & variety of events
- Poor correlation of events

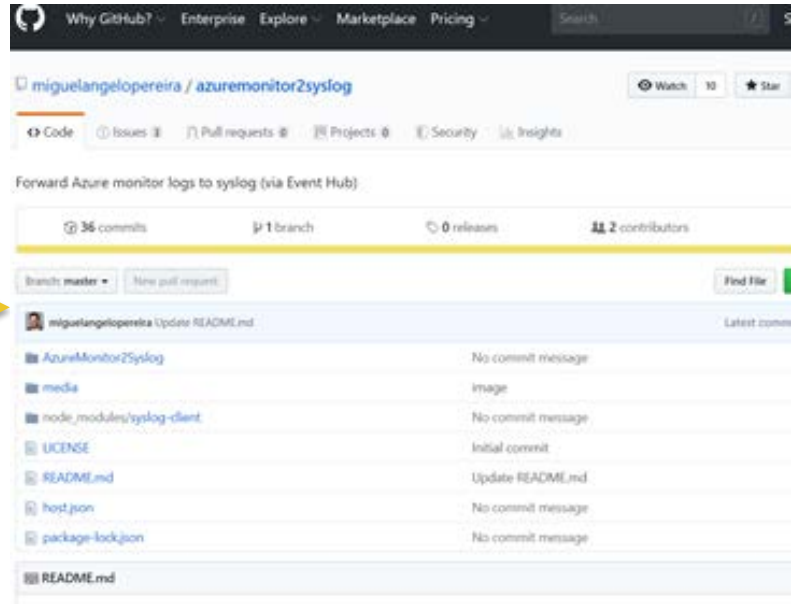
Connecting Cloud Events to On-prem SIEM - Reference Architecture



Various mechanism to fetch events

- REST API calls
- Connectors by SIEM vendors
- Conversion to standard Syslog format

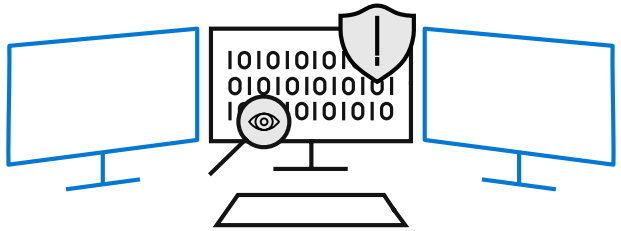




Here's a project on GitHub which you can refer to convert Cloud events to Syslog format

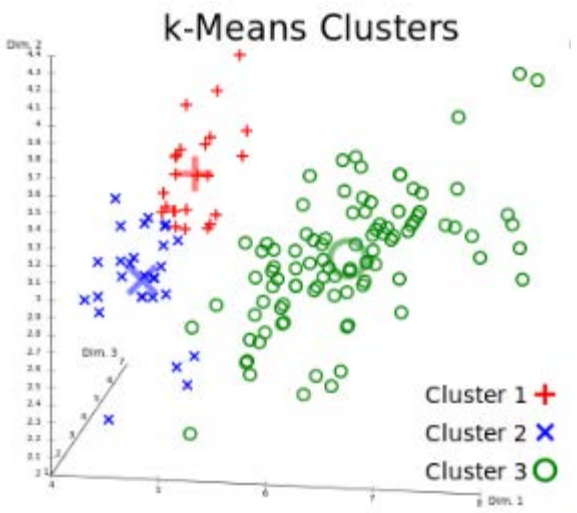
Skilling Up Your Analysts/Engineers Is Key to Success

1. Start by developing familiarity with Cloud concepts
2. Tackle IAAS first, familiar turf, easier for analysts to use their existing skills
3. Then move on to PAAS services being used within the org
4. Hire for fungible skills, not limited to product skills
   - Adaptability to evolving technologies is important
5. Analysts will deal with 'lots' of events
   - An ability to plumb data between repositories, and query data to create insights is important
6. Focus on understanding cloud attack TTPs
7. Get familiarity with your organizations DevOps and SRE practices
8. Design mechanism to keep Analysts updated on evolving cloud features

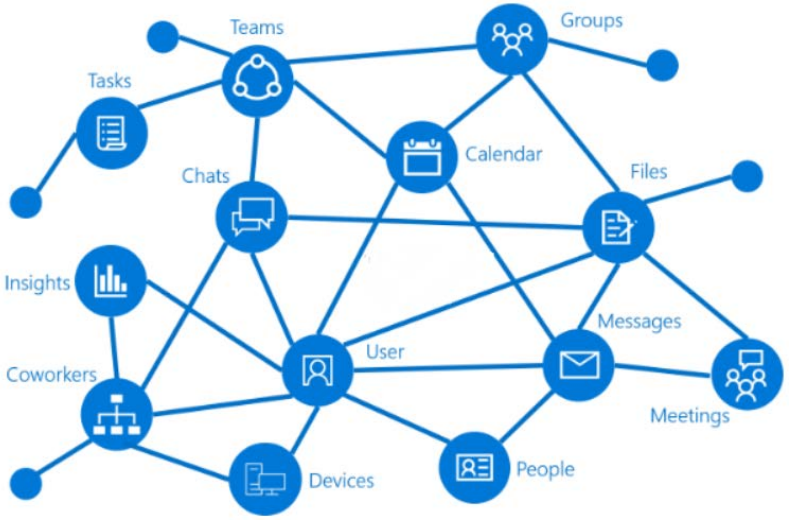


Up The Game by Leveraging 'Analytics' And 'Graph DB'

- Analytics when used right can help.
  - Cloud gives ability to analyze large volumes of events
  - Analytics/ML can uncover Anomalies and Outliers
    - Suspicious process execution, Suspicious login pattern, Suspicious Cloud Resource/ Service usage etc.
  - The Hunt team can then go after them



- Graph DB
  - Still evolving
  - But can help in complex investigation, especially in cloud
  - Great to investigate blended, multistage attacks



Top 6 Essentials For Success

1. It all starts with configuring it right, hygiene matters
   - E.g. CIS benchmark for Azure, CIS benchmark for AWS, CIS benchmark for Google Cloud
2. Prioritization is super critical
   - Use threat modelling to prioritize monitoring scenarios, cut the noise
3. Nurture Cloud skills within engineering and SOC team
4. Tweak playbooks for a ‘partnered’ investigation and remediation model
5. Design the right SIEM architecture
6. Establish a mechanism to keep up with new features in the cloud

Apply What You Have Learned Today

30 Days

Lay The Foundation

- Identify and implement security controls for Cloud
- Identify Cloud monitoring use cases
- Develop a framework for use case prioritization
- Develop a training plan for SOC analysts & engineers
- Define a workflow for incident handling for Cloud services

60 Days

Implement

- Conduct training for skill development
- Implement enhancements to your SIEM to handle Cloud events
- Develop & deploy use cases
- Develop SOC playbooks
- Conduct table-top exercise

90 Days

Measure & Finetune

- Measure fidelity of alerts
- Track new Cloud security features
- Run ongoing skill enhancement programs
- Conduct root cause analysis of Cloud incidents
- Fine tune use cases, playbooks

References

- *2019 State of the cloud report from Flexera - https://info.flexerasoftware.com/SLO-WP-State-of-the-Cloud-2019*
- *Gartner's annual forecast of worldwide public cloud service revenue - https://www.gartner.com/en/newsroom/press-releases/2019-04-02-gartner-forecasts-worldwide-public-cloud-revenue-to-g*
- *Detections on Github - https://github.com/Azure/Azure-Sentinel/tree/master/Detections*
- *Sample SIEM integration architecture - https://docs.microsoft.com/en-us/azure/security/security-azure-log-integration-overview*
- *Sample Cloud Logging - https://docs.microsoft.com/en-us/azure/security/azure-log-audit*
- *Kusto Big Data - https://docs.microsoft.com/en-us/azure/kusto/concepts/*
- *K-Means Clustering - https://en.wikipedia.org/wiki/K-means_clustering*
- *Graph DB - https://en.wikipedia.org/wiki/Graph_database & https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-graph-api*
- *Audit Logs - https://docs.microsoft.com/en-us/azure/security/azure-log-audit*
- *Security Alerts - https://docs.microsoft.com/en-us/azure/security-center/security-center-alerts-type*

RSAConference2019
Asia Pacific & Japan

Thank You!