INCIDENT RESPONSE IN THE CLOUD

Foggy with a ray of sunshine

Jeroen Vandeleur

Objective of Today

Can you automate incident response in Azure ?

WHO AM I ?

Jeroen Vandeleur

Service line Manager @ NVISO Cyber Architecture and Cloud Security

‘Always remember to mention Digital Security ’

Other facts:

- *Consume 216 Chickens / year*
  *150 grams protein daily = ((1x 250gr + 1x 370 gr chicken filet) x (18 * 12))/ 620g*
- *6 Days per week (skipped leg day in the beginning*

1 Once Upon a Time

2 Security Monitoring in Cloud

3 Automation within the SOC

4 Demo Time

Once Upon a Time …

Migration towards cloud environments

How do we intergate security into our new cloud environment ?

We want to migrate our infrastructure towards Azure (IaaS). Could you perform a security review and provide recommendations ?

Sure, lets do an azure security design review based on the CIS Benchmarks & Microsoft/NIST Blueprint model.

Nice! Involve security before migration

In total we found 12 issues within the proposed design and provided 9 high prio recommendations to resolve these issues. A subset of the recommendations:

1. Multi factor authentication (especially for priviliged accounts)
2. Use network security groups to filter traffic
3. Use Role Based Access Controls (RBAC)
4. Enable Azure logging (activity logs, NSG Flow Logs, SQL Server logs)

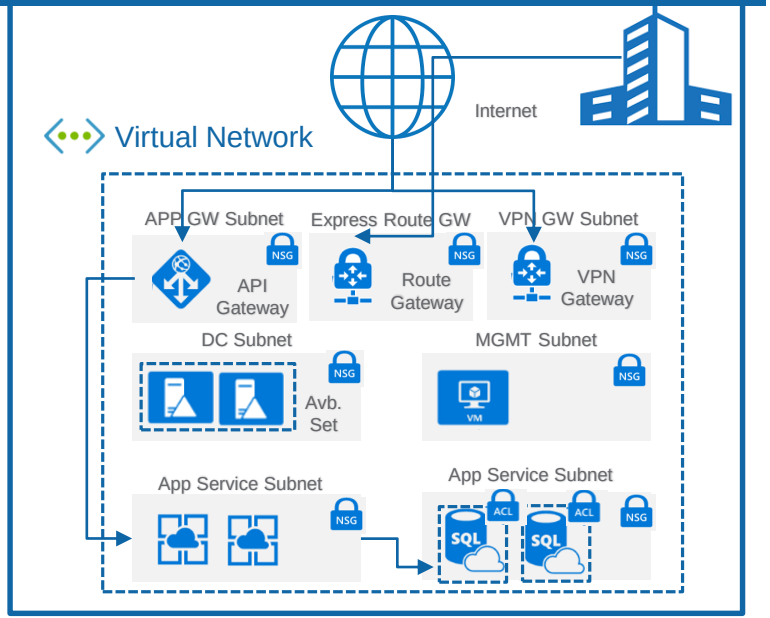
2 Months later … we got an urgent call

BREACHED

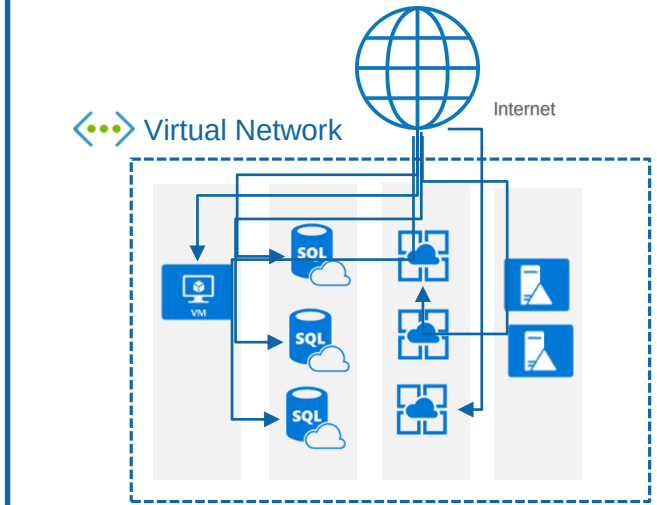
How could this happen??

Find the 7 differences !

Based on our review



Implemented Design



Cloud Security Incident Analysis

Check the logs to see what was going on ?

Take a look at the following logs. Based on these logs we could create a timeline on what happened !

NSG FLOW LOGS	SQL Server Audit	Azure AD Sign Ins	System Logs
Origin and impacted systems?	Sensitive data lost ?	Users Impacted ?	Actions performed ?
No NSG Flow logs	**No SQL Audit Logs**	**No Role Based Access**	**Yes, locally but rotation size**

Conclusion
Assume everything is BREACHED !!!

Incident Response in the cloud

What were the main challenges during incident response

Traffic filtering and logs

Default logging available

Log Retention Period

Access management

Insecure host configurations

Identification of the resource owner

Security Monitoring in the Cloud

Security Monitoring toolset

Some of the cloud-native monitoring features available for you

nviso

Microsft Azure

Azure AD Logs

Security Center

NSG Flow Logs

Unified Audit Logs

ATP Logs

Amazon AWS

IAM Policy

CloudWatch

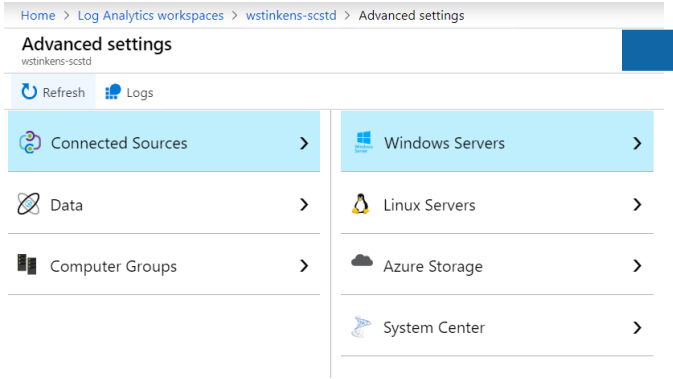
VPCFlow Logs

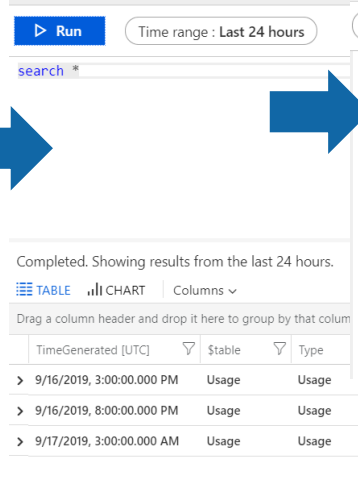
CloudTrail

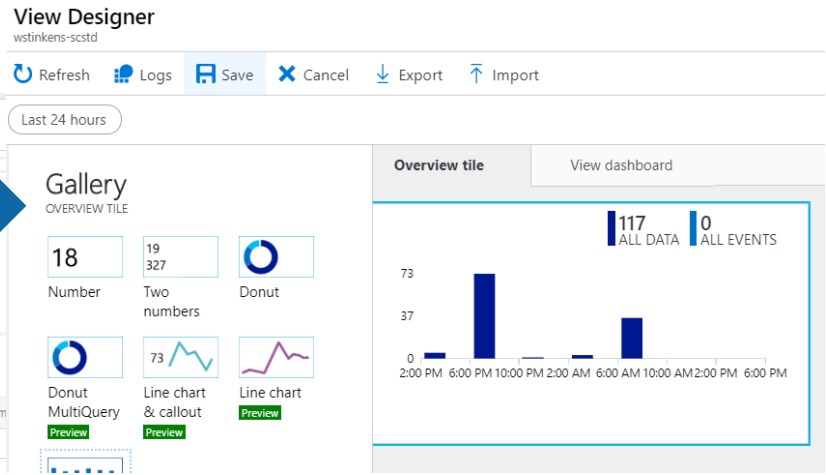
Guardduty

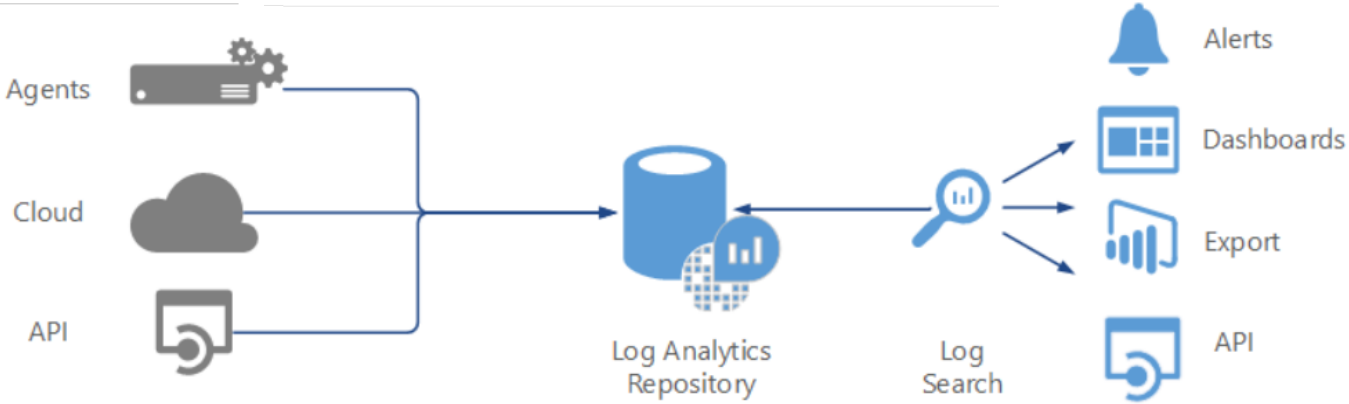
Centralized Cloud Logging Azure

So many logs – how do you manage …



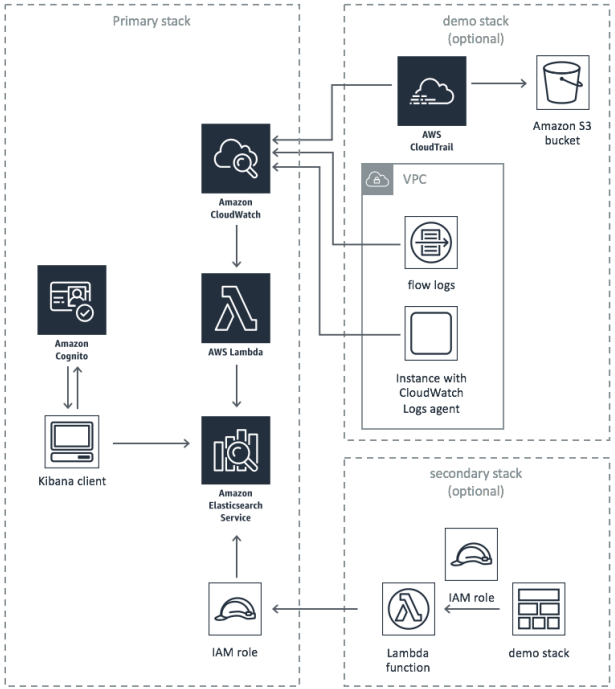


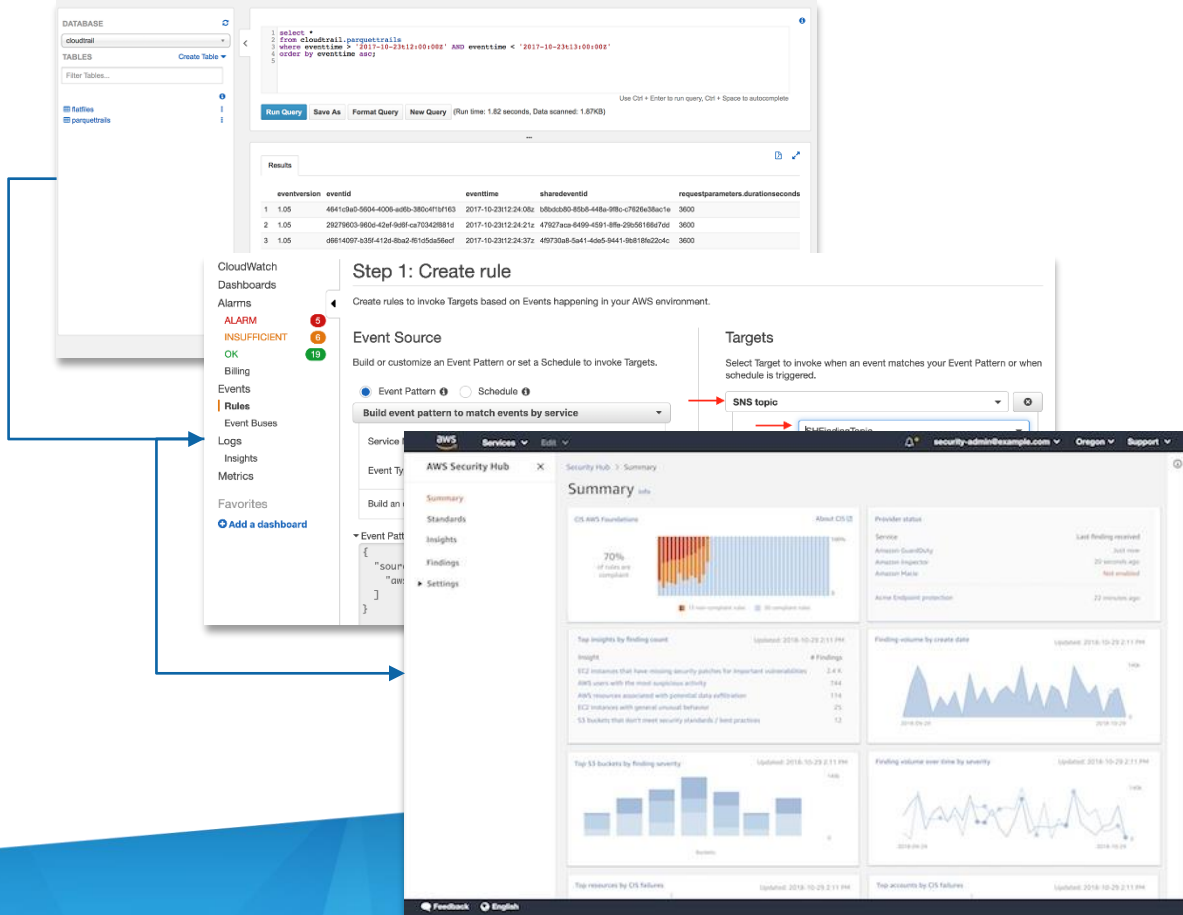




Centralized Cloud Logging AWS

So many logs – how do you manage …





Start with the Basics

Don’t enable all logs at once, in recent incidents most of the following logs were already sufficient to analyze the actual breach:

1. Identity and Access Management logging
2. Network flow logging
3. System logging

Validate, review and move on ...

Automated Incident Response

Challenges related to security monitoring

The Whack-A-Mole approach !

Why do we need a different approach ?

Resources

Resource shortage of 4.7 million security professionals

Tools

The number of products and tools within an environment is increasing

Events

A typical large SOC needs to process 10.000 alerts per day

Static

Independent controls, not agile. Attackers use new techniques; we need to adapt

Speed

Speed of detection is too slow; the average time to identify is 206 days

Let’s OODA this SOC

OBSERVE

Data Collection, collecting logs in hybrid mode.

ORIENT

Data Analysis, integrate capabilities such as threat hunting, intelligence and custom

DECIDE

Playbooks, provide azure logic apps and playbooks to support the SOC .

ACT

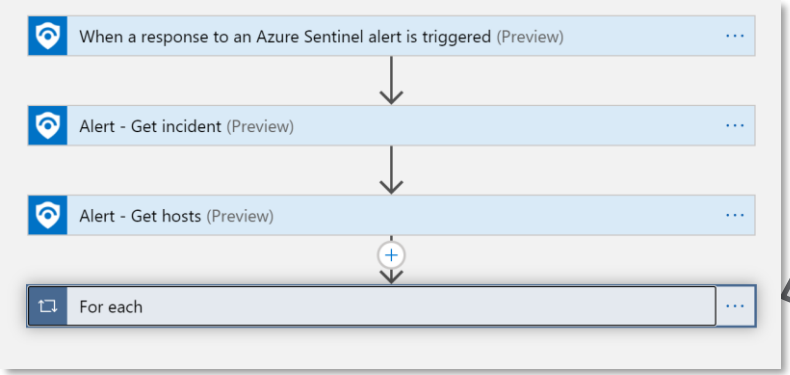
Define and validate the controls with technical teams and automate common tasks.

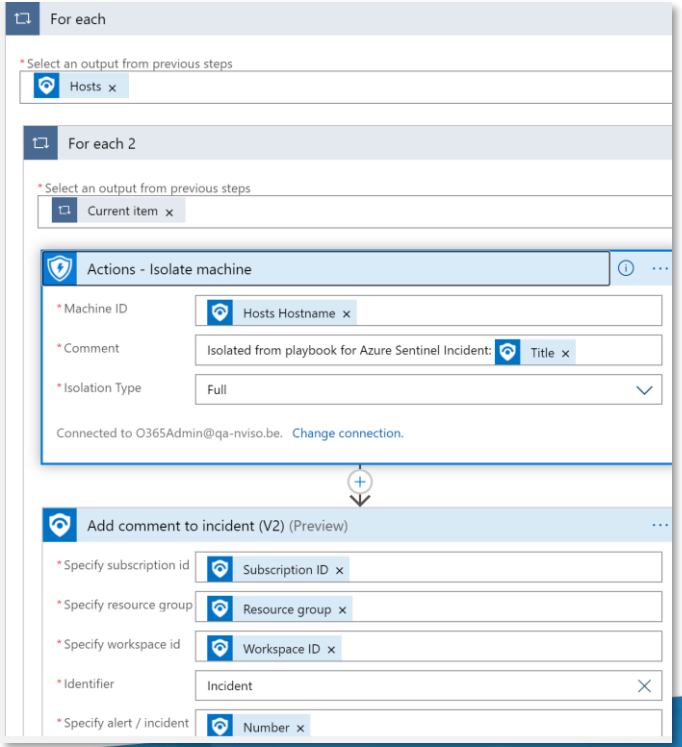
Decide – transform common incidents into playbooks

90% of the time analysts were investigating risky sign-ins & malware

EXAMPLE OF AUTOMING DECISION

This logic app will immediately isolate several hosts where the Sentinel detects malware or suspicious behavior. Result: Immediate containment and more time for the analyst!





Act – transform common incidents into playbooks

Several built-in connectors are used to act upon an incident !

Disable or Block
User access

Add or adjust network
security groups

Send email to user,
SOC or helpdesk

Send teams' message
to SOC or helpdesk

Isolate machine

Add malicious IP
Or domain to firewall

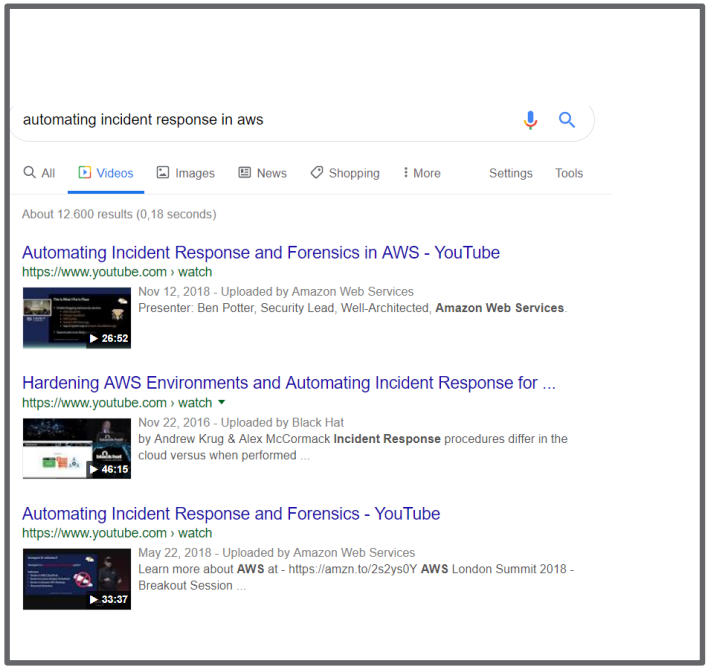
Take snapshot
of the system

Add signature
to security controls

Demo Time

Automated incident response in Azure

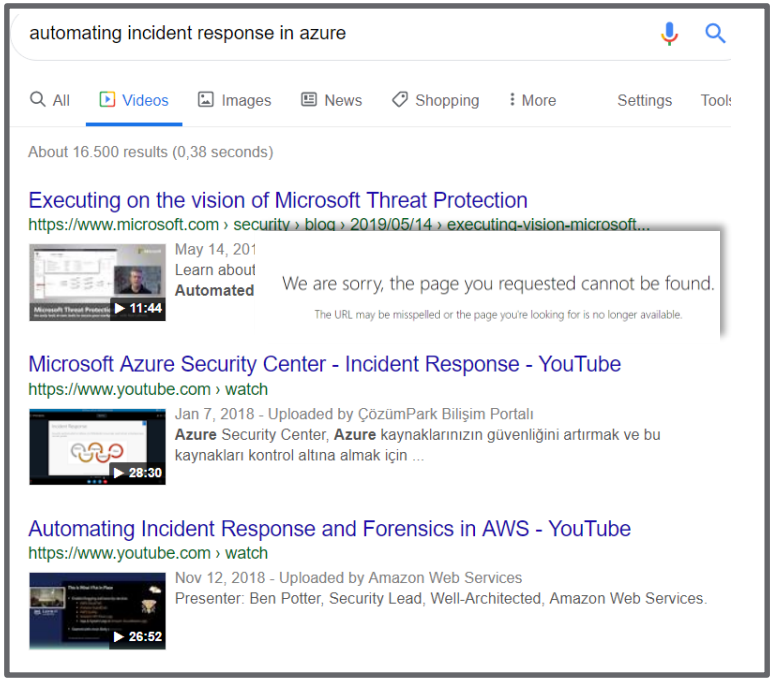
Why Azure ?



Page Not Found ?

Automation ?

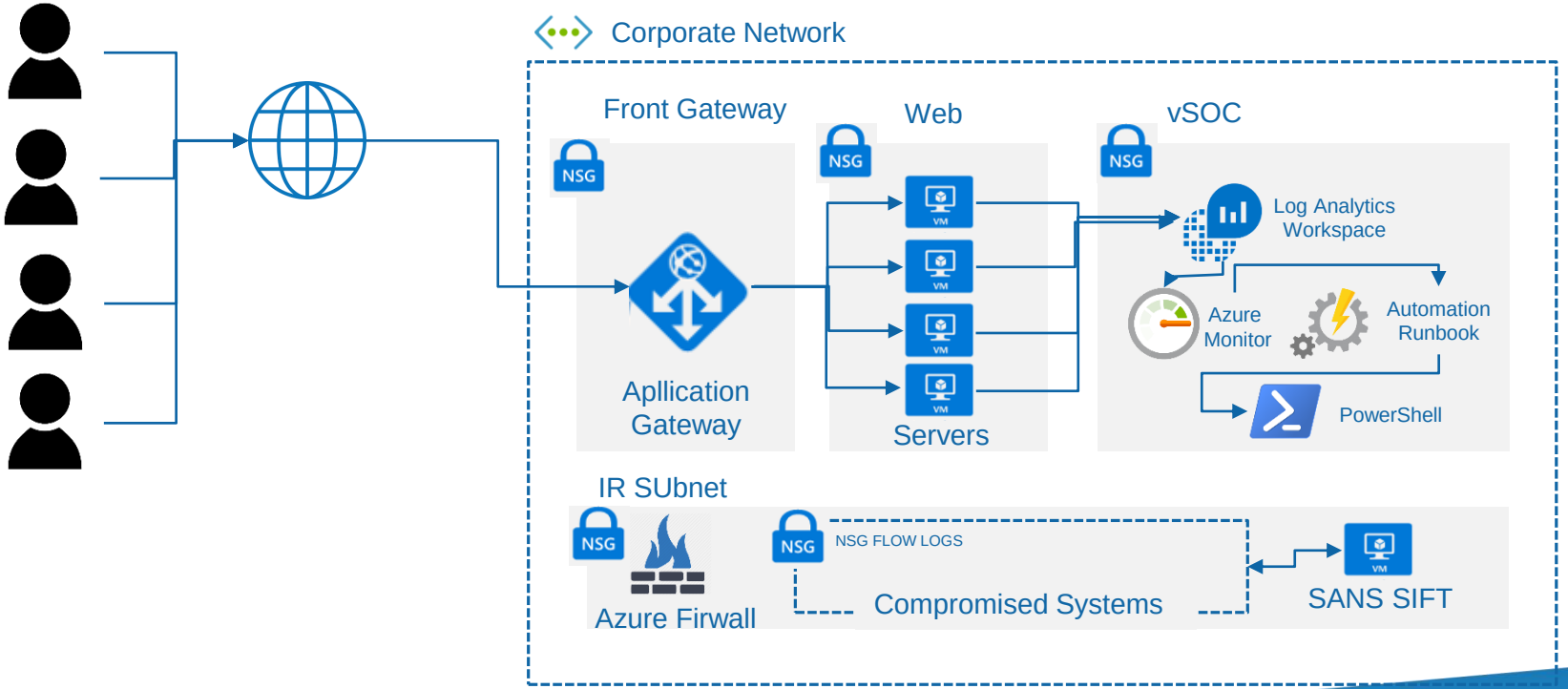
AWS ??



https://www.youtube.com/watch?v=f_EcwmmXkXk

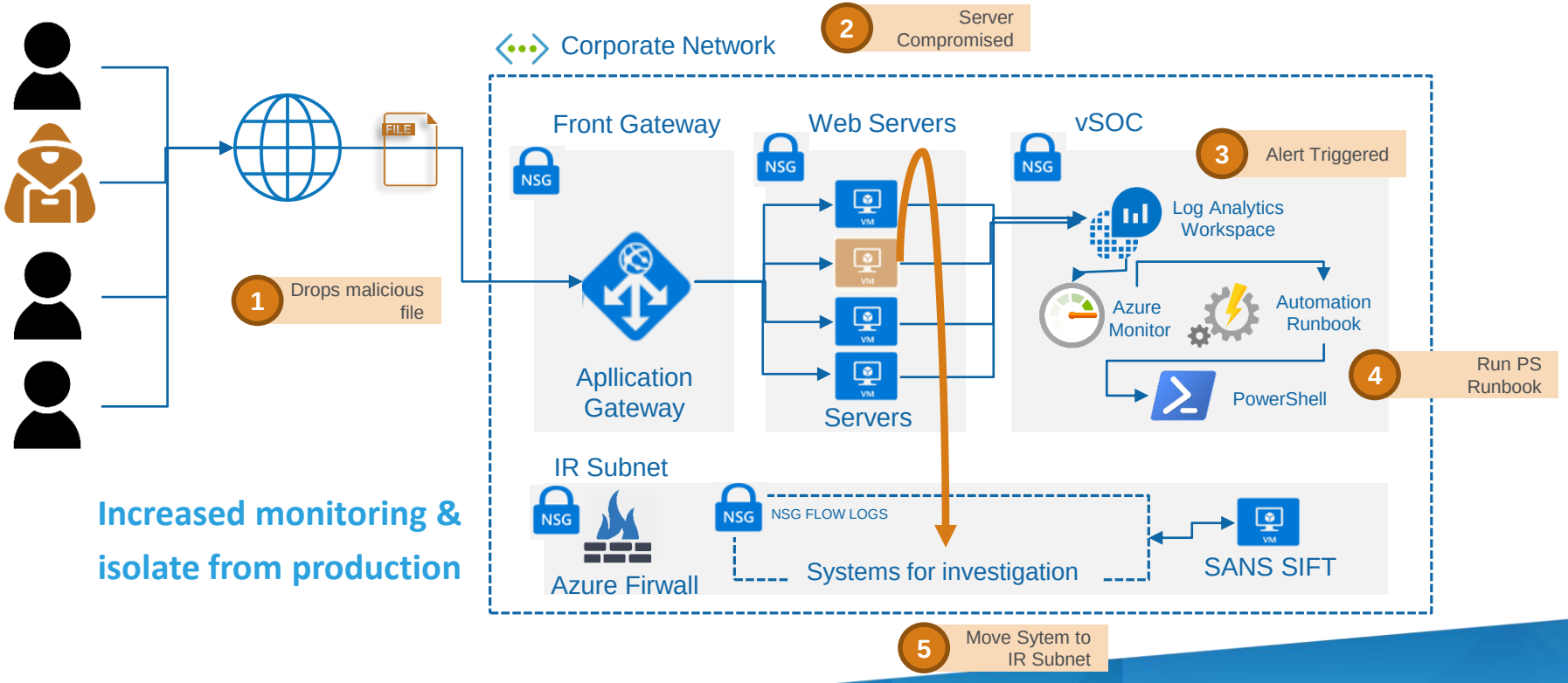
Automated incident response in Azure

Demo design – current state



Automated incident response in Azure

What happens & what we expect …



Increased monitoring & isolate from production

Automated incident Response

The automation toolsets we tested !

Automation Runbooks

- ✓ Trigger: Azure Monitoring Alert
- ✓ Action: Execute Powershell runbook
- ✓ Result: **Succesful**

Constraints:

- ✓ Alert query only executed each 5 minutes
- ✓ Passes all alerts in one scheme format; all alerts need to be parsed in the runbook

Azure Functions

- ✓ Trigger: Azure Monitoring Alert
- ✓ Action: Execute Azure Function
- ✓ Result: **Succesful**

Constraints:

- ✓ Powershell functions in preview
- ✓ Limited documentation

Logic Apps

- ✓ Trigger:Security center alert
- ✓ Action:Execute Runbook
- ✓ Result: **Failed**

Reason:

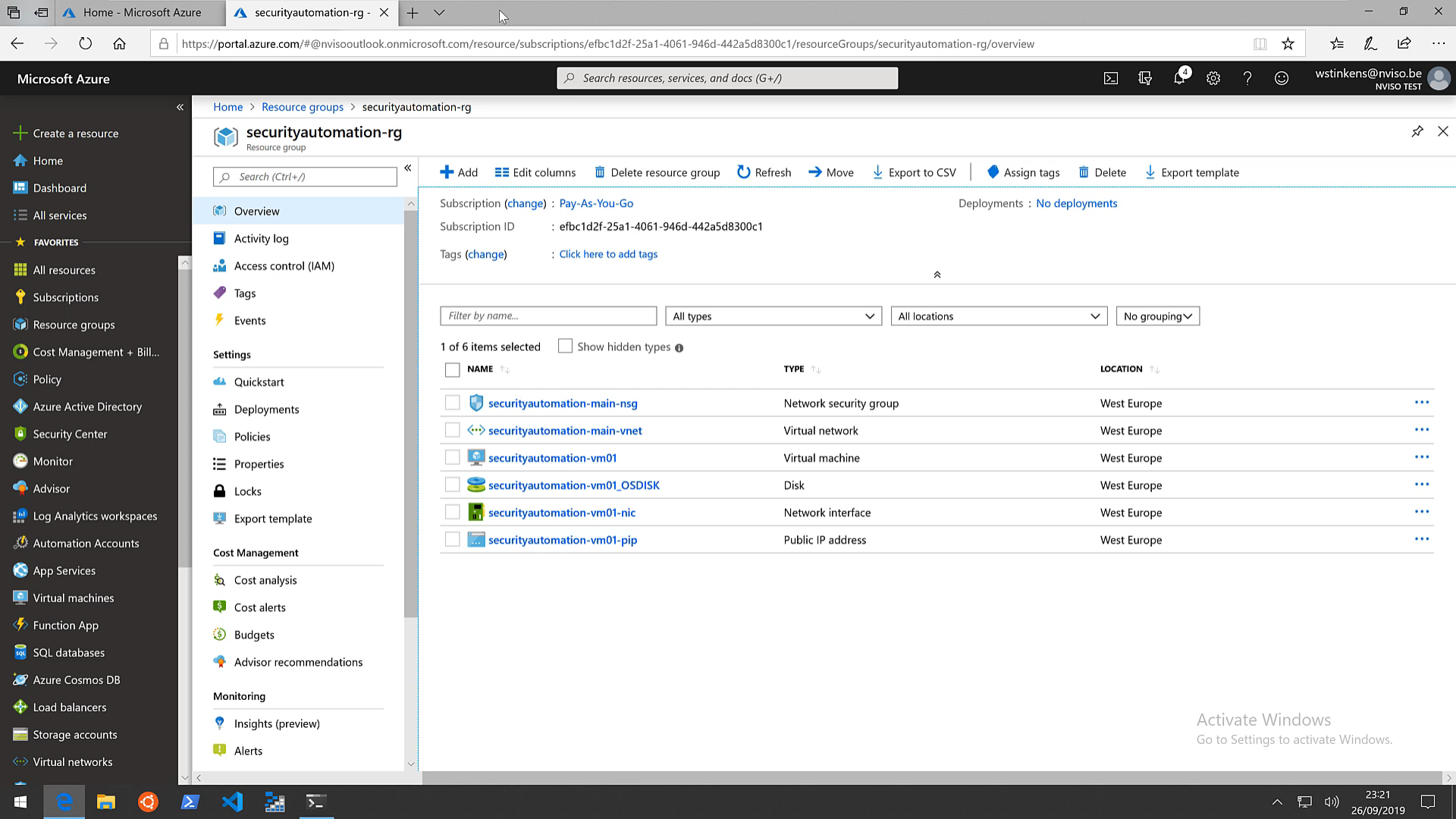
- ✓ Run is on demand
- ✓ Detailed parameters not in the alert to run our runbook such as system ID

O365 Flows

- ✓ Trigger:Security Graph API alert
- ✓ Action:Execute Runbook
- ✓ Result: **Failed**

Reason:

- ✓ Not all fields are populated in alert.


Home - Microsoft Azure
securityautomation-rg -
https://portal.azure.com/#@nvisooutlook.onmicrosoft.com/resource/subscriptions/efbc1d2f-25a1-4061-946d-442a5d8300c1/resourceGroups/securityautomation-rg/overview
Microsoft Azure
Search resources, services, and docs (G+/)
wstinkens@nviso.be
NVISO TEST
Home > Resource groups > securityautomation-rg
securityautomation-rg
Resource group
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Events
Settings
Quickstart
Deployments
Policies
Properties
Locks
Export template
Cost Management
Cost analysis
Cost alerts
Budgets
Advisor recommendations
Monitoring
Insights (preview)
Alerts
Add
Edit columns
Delete resource group
Refresh
Move
Export to CSV
Assign tags
Delete
Export template
Subscription (change) : Pay-As-You-Go
Deployments : No deployments
Subscription ID : efbc1d2f-25a1-4061-946d-442a5d8300c1
Tags (change) : Click here to add tags
Filter by name...
All types
All locations
No grouping
1 of 6 items selected
Show hidden types
NAME
TYPE
LOCATION
securityautomation-main-nsg
Network security group
West Europe
securityautomation-main-vnet
Virtual network
West Europe
securityautomation-vm01
Virtual machine
West Europe
securityautomation-vm01_OSDISK
Disk
West Europe
securityautomation-vm01-nic
Network interface
West Europe
securityautomation-vm01-pip
Public IP address
West Europe
Activate Windows
Go to Settings to activate Windows.
23:21
26/09/2019

Our response to the current challenges !

How to win the Whack-a-mole Game through Automation

Resources

90% of the time analyst were investigating phishing attacks.

Tools

Increase the visibility in on-prem environments and multi-cloud tools.

Events

The older SIEM was generating hundred alerts per day.

Static

Use case development was static on the previous SIEM

Speed

Investigated account breaches that were older than 3 months.

Automation

Sentinel enabled us to automate phishing and malware detection and response via logic apps or LAMBDA.

API Calls

Sentinel has built-in connects (single click log sources) and API links.

Intelligence

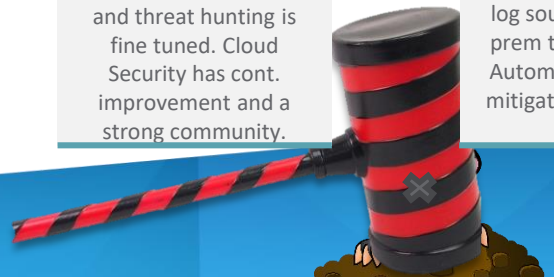
We have on-boarded threat intel MISP and reduced the amount of events to handle.

Community

Use case development and threat hunting is fine tuned. Cloud Security has cont. improvement and a strong community.

Centralized

SIEM can combine the log sources in and on-prem to detect faster. Automation is used to mitigate threats in real time.



Thank you