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 integrate 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, let's do an Azure security design review based on the CIS Benchmarks & Microsoft/NIST Blueprint model.

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

1. Multi-factor authentication (especially for privileged 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)

Nice! Involve security before migration.
2 Months later ... we got an urgent call

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**
  - Origin and impacted systems?
  - No NSG Flow logs

- **SQL Server Audit**
  - Sensitive data lost?
  - No SQL Audit Logs

- **Azure AD Sign Ins**
  - Users Impacted?
  - No Role Based Access

- **System Logs**
  - Actions performed?
  - 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
WE NEED TO DO BETTER

YOU PROMISED
A RAY OF SUNSHINE

Security Monitoring in the Cloud
## Security Monitoring toolset

Some of the cloud-native monitoring features available for you

<table>
<thead>
<tr>
<th>Microsoft Azure</th>
<th>Amazon AWS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Azure AD Logs</td>
<td>IAM Policy</td>
</tr>
<tr>
<td>Security Center</td>
<td>CloudWatch</td>
</tr>
<tr>
<td>NSG Flow Logs</td>
<td>VPCFlow Logs</td>
</tr>
<tr>
<td>Unified Audit Logs</td>
<td>CloudTrail</td>
</tr>
<tr>
<td>ATP Logs</td>
<td>Guardduty</td>
</tr>
</tbody>
</table>
Centralized Cloud Logging Azure

So many logs – how do you manage …
Centralized Cloud Logging AWS

So many logs – how do you manage ...
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 ...
YOU DETECT?

RESPOND FASTER

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 indicators.

**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!

![Diagram of logic app flow](image)

When a response to an Azure Sentinel alert is triggered (Preview) → Alert - Get incident (Preview) → Alert - Get hosts (Preview) → For each

Add comment to incident (V2) (Preview)

*Specify subscription id
*Specify resource group
*Specify workspace id
*Identifier
*Specify alert / incident

Actions - Isolate machine

*Machine ID
*Comment
*Isolation Type

Isolated from playbook for Azure Sentinel Incident: Title x

Connected to O365Admin@qa-nviso.be. Change connection.
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
- Add malicious IP Or domain to firewall
- Take snapshot of the system
- Isolate machine
- Send teams' message to SOC or helpdesk
- Add signature to security controls
I PITY THE DEMO GODS

I HAVE A VIDEO

Demo Time
Automated incident response in Azure

Why Azure?

https://www.youtube.com/watch?v=f_EcwmmXkXk
Automated incident response in Azure

Demo design – current state

Corporate Network

Front Gateway

Application Gateway

Web

vSOC

Log Analytics Workspace

Automation Runbook

PowerShell

IR Subnet

Azure Firewall

Compromised Systems

NSG FLOW LOGS

NSG

NSG

NSG

NSG

www.nviso.be | 24
Automated incident response in Azure

What happens & what we expect ...

1. Drops malicious file
2. Server Compromised
3. Alert Triggered
4. Run PS Runbook
5. Move System to IR Subnet

Increased monitoring & isolate from production
Automated incident Response

The automation toolsets we tested!

**Automation Runbooks**
- Trigger: Azure Monitoring Alert
- Action: Execute Powershell runbook
- Result: Successful

**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: Successful

**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.
<table>
<thead>
<tr>
<th>NAME</th>
<th>TYPE</th>
<th>LOCATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityautomation-main-ng</td>
<td>Network security group</td>
<td>West Europe</td>
</tr>
<tr>
<td>securityautomation-main-vnet</td>
<td>Virtual network</td>
<td>West Europe</td>
</tr>
<tr>
<td>securityautomation-vm01</td>
<td>Virtual machine</td>
<td>West Europe</td>
</tr>
<tr>
<td>securityautomation-vm01_OSDISK</td>
<td>Disk</td>
<td>West Europe</td>
</tr>
<tr>
<td>securityautomation-vm01-nic</td>
<td>Network interface</td>
<td>West Europe</td>
</tr>
<tr>
<td>securityautomation-vm01-pip</td>
<td>Public IP address</td>
<td>West Europe</td>
</tr>
</tbody>
</table>
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 hundreds of 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