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 x 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 ...
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

Facts and Figures

19% Unauthorized access
SANS Cloud Security Survey

9 cases Cloud Security Incidents investigated by NVISO in the last 2 months
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

**Microsoft 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 ...
Incident response automation

Why should we automate?

Automating incident response activities improves the **efficiency and effectiveness** of incident response efforts and increases the number of incidents that a team may handle.

- Focus on the people area, most companies have several technologies and processes in place.
- SOC is always limited in resources and time, automation should allow you to detect and respond faster.
- Security analysts want to do the more advanced stuff instead of repetitive and unproductive tasks.
- Incident response playbook = procedural description on how to handle incidents. Can’t we automate this for common incidents?
Where should we automate

Incident response phases

Preparation → Identification → Containment → Eradication → Recovery → Lessons Learned

Our automation focuses on **Identification** and **containment**, to have less repetitive tasks and speed up the containment.

Other phases we still need to have manual power to fully understand the security incident.

Most organizations are already doing automated IR – Sandboxing or detonation services.
I Pitty the Demo Gods

I Have a Video
Automated incident response in Azure

Why Azure?

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

Page Not Found?

Automation?

AWS ??

autamating incident response in aws

About 12,600 results (0.18 seconds)

Automating Incident Response and Forensics in AWS - YouTube
https://www.youtube.com/watch
Nov 12, 2016 - Uploaded by Amazon Web Services
Presenter: Ben Potter, Security Lead, Well-Architected, Amazon Web Services

Hardening AWS Environments and Automating Incident Response for ...
https://www.youtube.com/watch
Nov 22, 2016 - Uploaded by Black Hat
by Andrew Kug & Alex McCormack Incident Response procedures differ in the cloud versus when performed...

Automating Incident Response and Forensics - YouTube
https://www.youtube.com/watch
May 22, 2015 - Uploaded by Amazon Web Services
Learn more about AWS at: https://aws.amazon.com/AWS London Summit 2015 - Breakout Session...

executing the vision of microsoft threat protection
https://www.microsoft.com/security/blog/2018/05/14/executing-vision-microsoft

Microsoft Azure Security Center - Incident Response - YouTube
https://www.youtube.com/watch
Jan 7, 2018 - Uploaded by ÇözümPark Bilişim Platformi
Azure Security Center, Azure kaynaklarınızı güvenliği artırmak ve bu kaynakları kontrol altına almak için...

Automating Incident Response and Forensics in AWS - YouTube
https://www.youtube.com/watch
Nov 12, 2016 - Uploaded by Amazon Web Services
Automated incident response in Azure

Demo design – current state
Automated incident response in Azure

What happens & what we expect ...

1. Drops malicious file

Increased monitoring & isolate from production

2. Server Compromised

3. Alert Triggered

4. Run PS Runbook

5. Move System to IR Subnet

Corporate Network

Front Gateway

Web Servers

vSOC

Application Gateway

Servers

IR Subnet

Azure Firewall

Log Analytics Workspace

Automation Runbook

Runbook

NSG FLOW LOGS

Systems for investigation

SANS SIFT

Increased monitoring & isolate from production

www.nviso.be | 28
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.
Conclusion and Lessons Learned

- Multiple Toolsets
- Read Best Practices
- Train for Automation
- Extra Costs
- Limitations related to toolset
- Preview mode means bugs

Series of blogpost: https://blog.nviso.eu
Scripts will be published on our Github
Thank you