Secure Emergency Access Strategies: Zero Trust Break the Glass Solutions

WORKPLACEDUDES SUMMIT 2024

DANK AAN ONZE SPONSORS

infinity

PATCH MY PC

LIQUIT

Part of RECAST SOFTWARE

venéco

Moving you *forward*

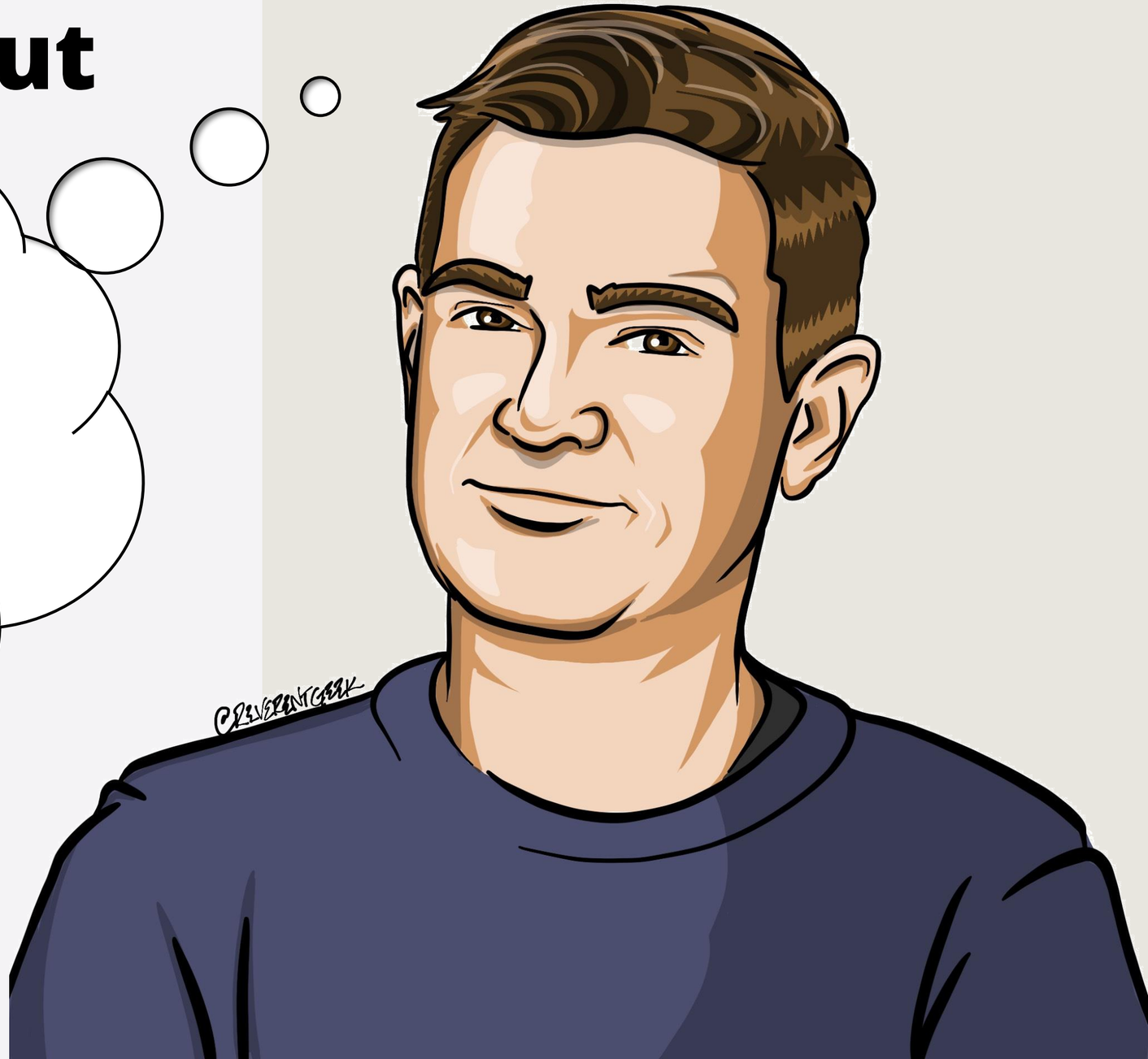
?

Break the glass

Jeroen Burgerhout

- 🍺 Modern Workplace Brewer
- 👨‍🏫 Microsoft Certified Trainer

- 📰 burgerhout.org
- 🔗 burgerhou.tj/connect



Who is Sander

Creative Cloud Developer

Hobbies
- Play around with technology
- Blog @ rozemuller.com
- Athletics
- Gardening, brewing and BBQ

Microsoft Most Valuable Professional

Enterprise Mobility & Security

Stands for Automation first & everything


RAW
LINSEED
OIL
NAILS

What do we need?

- Object ID from the emergency account
- A custom logs alert rule

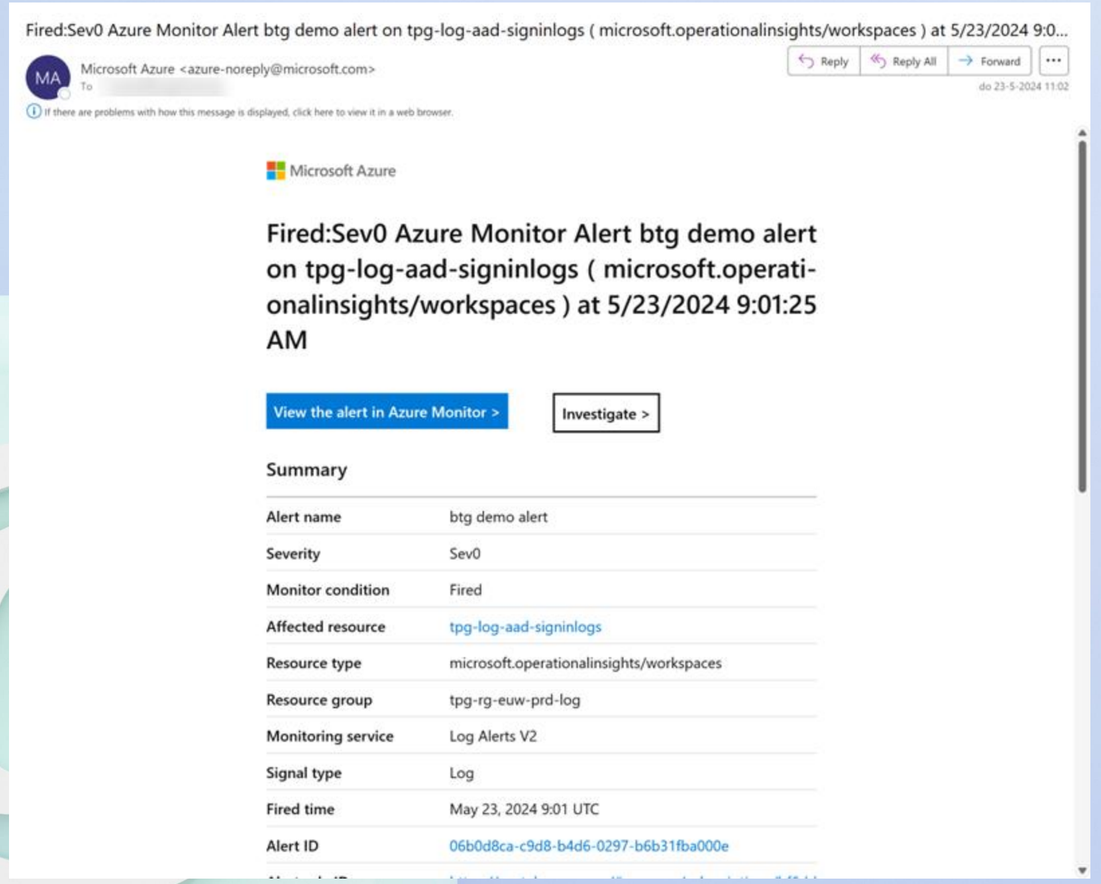
```
SigninLogs
| where UserId contains "object-id"
```

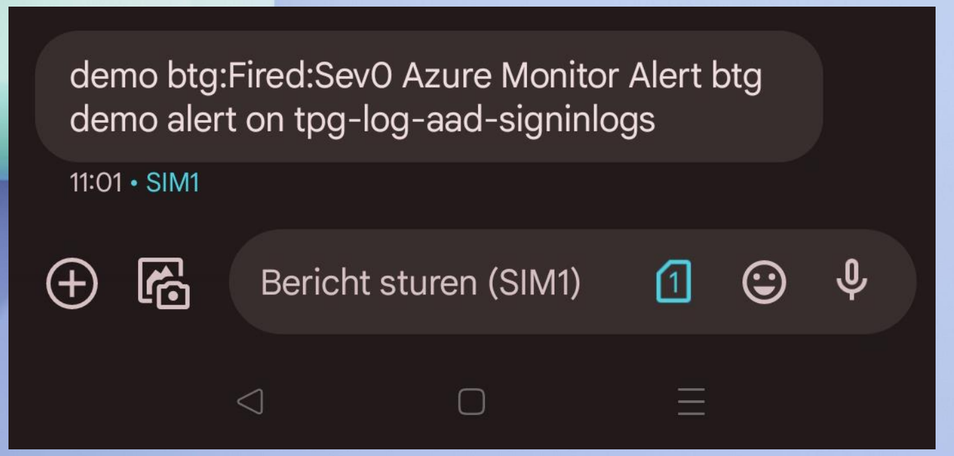
- Action Group
- Logic App that monitors the certificate

Activity Details: Sign-ins

Basic info | Location | Device info | Authentication Details | Conditional

Date	5/23/2024, 10:47:37 AM
Request ID	99d160b7-3efa-47fa-91c3-3f6b6c973700
Correlation ID	6f56eb31-2483-4ed8-b4b5-162779bd2764
Authentication requirement	Single-factor authentication
Status	Success
Continuous access evaluation	No
Troubleshoot Event	Follow these steps: Launch the Sign-in Diagnostic. 1. Review the diagnosis and act on suggested fixe
User	demobtg
Username	demobtg@thepeskyghosts.onmicrosoft.com
User ID	bb82aecf-82bf-4c62-b802-d1b69d203ccf





Why?

In case of:
- Natural disaster, like earthquake, flooding
- network issues
- Identity providers outage, like MFA services

Create

- At least, create 2 break the glass accounts
- Cloud-only (*.onmicrosoft.com)
- Global Administrator role

Store it

- In a vault
- Internal and external from office
- Preferable FIDO2 key
- Write it down and keep the u/p separate from each other

Attention

- Exclude from MFA, CA and SSPR
- Exclude from Entra ID Protection

- GA behind PIM activation with auto approval

Monitoring

- Log Analytics Workspace
- Change the Diagnostic settings to forward the Entra ID loggings
- Action Group (SMS/Email)
- Alert Rule KQL query

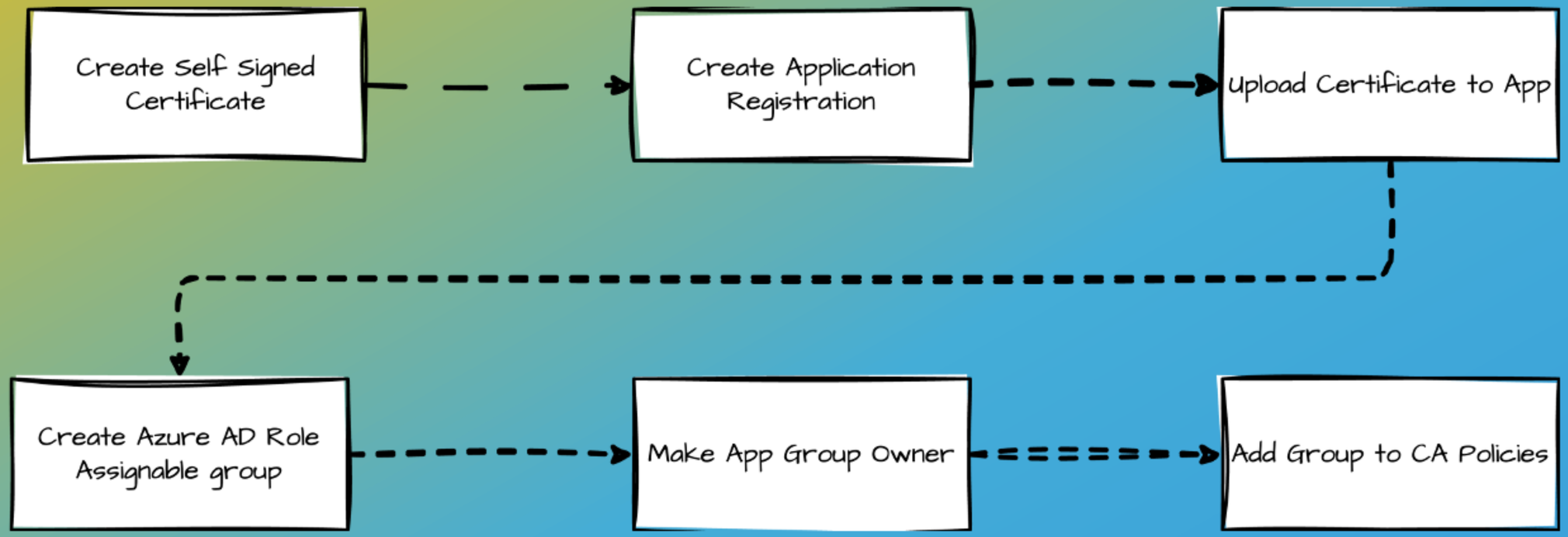
Test / validate it

- at least every 90 days
- Recent change in IT staff
- process to use these accounts is documented and current

And now, from a different angle

What differs this break glass approach?

Deployment process



Login process

CONSIDERATIONS

Emergency account has ONLY GroupMember.ReadWrite.All permissions;

When logged in, The userId as the groupId CAN NOT be craweled by the app;

Add the user to the exclusion group based on user ID and Group ID

The exclusion group is an Azure Role Assignable group

ONLY a Global Admin, Privileged Role Admin or owner can add users

Wrap up