



# HAS ANYONE SEEN THE PRINCIPAL?

**Emilian Cebuc & Christian Philipov**

Fwd:CloudSec – 13<sup>th</sup> September 2021

# WHO ARE WE?

- Security consultants @F-Secure Consulting
- Professional ~~Meme Masters~~ Cloud enthusiasts – particularly Microsoft’s Azure platform
- Helping people secure their cloud estate and breaking stuff along the way
  
- Shoutout for the original talk idea to Javan Joshua Mnjama - @JavanMnjama



Emilian Cebuc - @RockBoyEmy



Cristian Philipov - @chrispy\_sec



# CLOUD COMPROMISES IN THE WILD

- Holmium (APT33) attack – full network control in under a week<sup>[1]</sup>
- “Living off the Land” (LoL) attacks – leveraging legitimate functionality<sup>[2]</sup>
- Compromised Azure resources & extensions
- Un-monitored O365 accounts and ADFS
- Password sprays & Phishing
- Lack of MFA



# AGENDA



Azure AD Service Principals



Azure StormSpotter & cypher queries



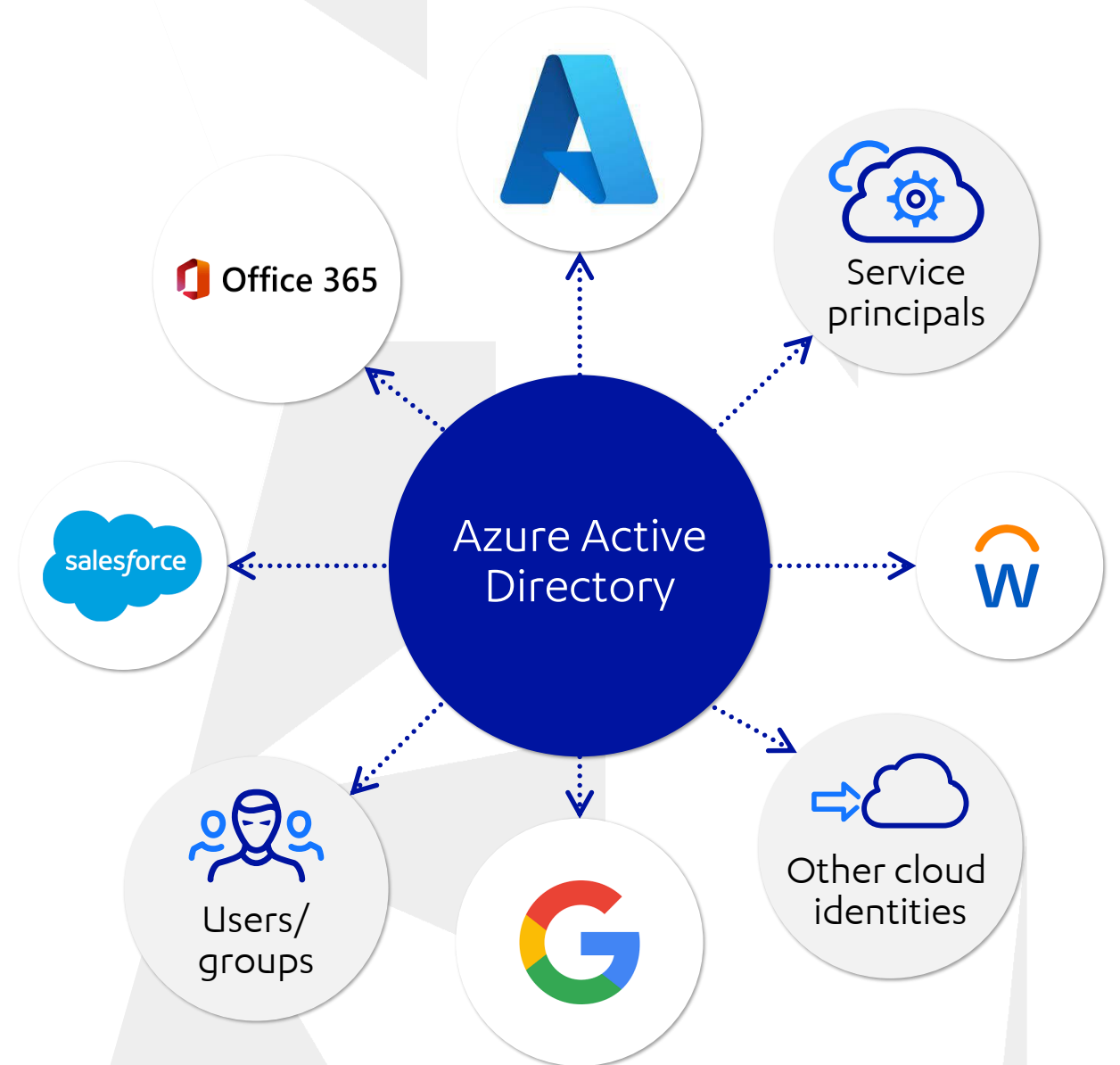
Attack scenarios & exploitation



Detection & prevention

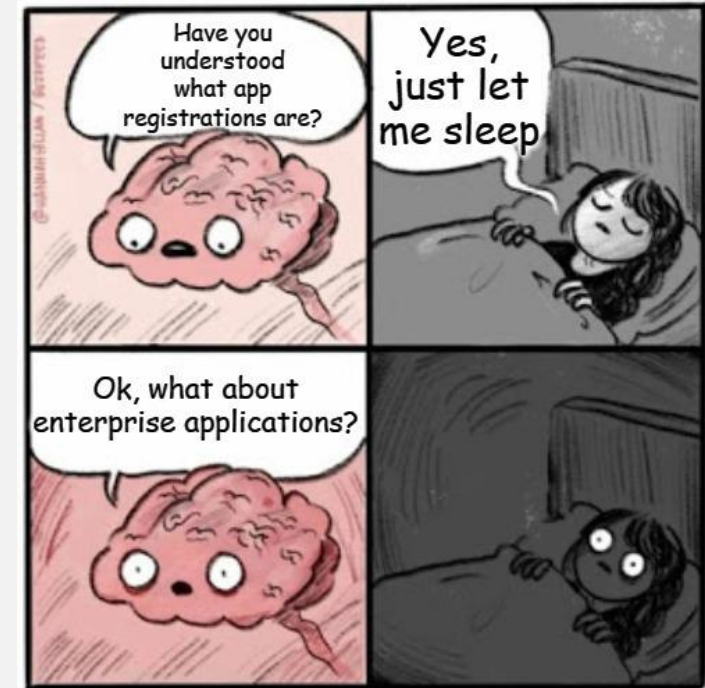
# AZURE AD & SERVICE PRINCIPALS

- An Identity Provider (IdP) & Identity and Access Management (IAM) service, in the cloud
- In Azure, you can have identities
- These can have *roles* assigned to them
- Service Principals are accounts for representing non-user entities



# SERVICE PRINCIPALS AND CLOUD APPS

- Numerous possibilities for applications in the cloud
  - For employees, customers and partners
- AAD Apps can be "registered" – unique definition
  - A *class* if you think of OOP
- "Instantiate" a copy of the app
- A Service Principal account gets created

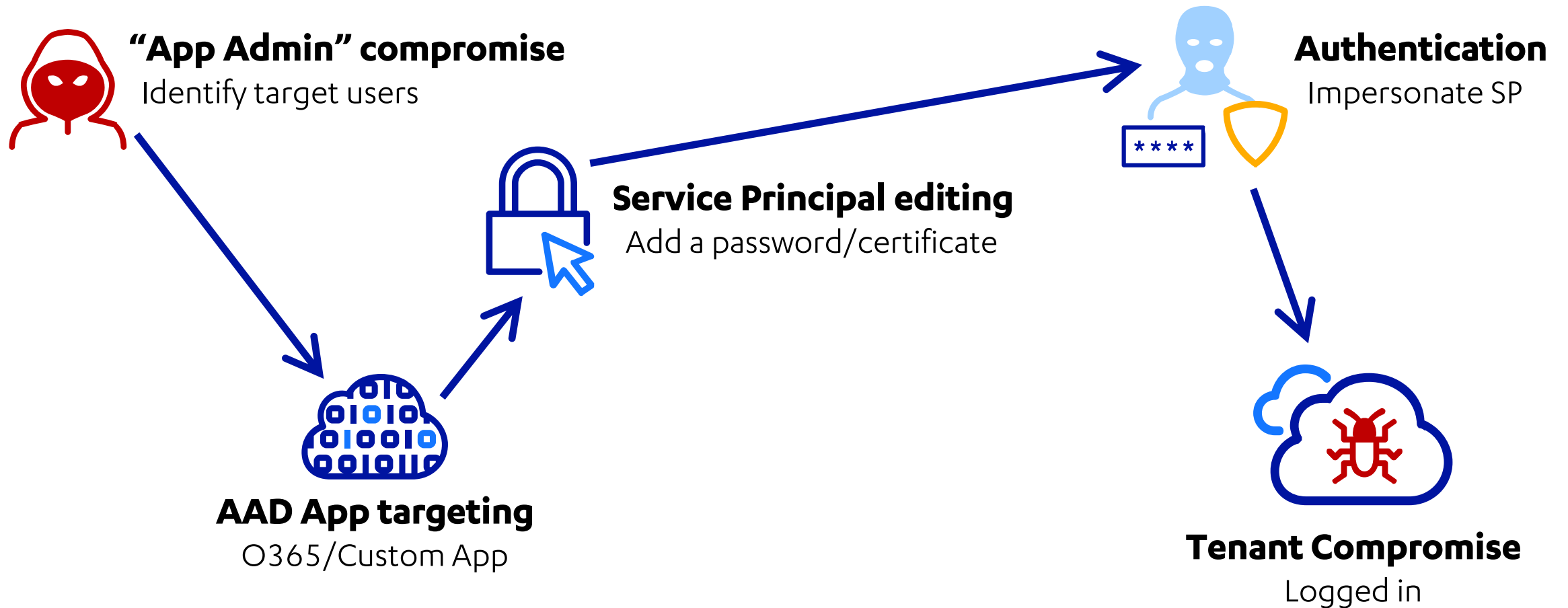


# WHY DO WE CARE?

- SPs tend to be overlooked
  - During development
  - Security assessments
- 300+ Apps onboarded with an O365 E3 or E5 tenant license
  - Research in 2019 by Dirkjan<sup>[3]</sup>
  - However, 2 years later, the situation is not quite the same anymore

We need to restrict access	 Panik
We only have 4 Global Admins	 Kalm
Wait, what permissions do our service principals have?	 Panik

# ATTACK PATH 1



# ATTACK PATH 2

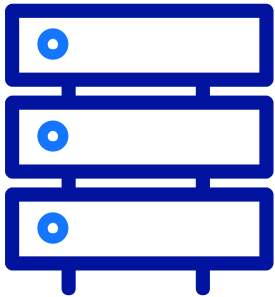
Benign AAD Application



Azure AD tenant identities



"Contributor" Access



Azure Resources

# STORMSPOTTER

- Tool for identifying infrastructure and AD components in Azure<sup>[4]</sup>
- Made by the Azure peeps – neo4j, graphing capabilities
- Cypher queries - creation of visual links among components



STORMSPOTTER

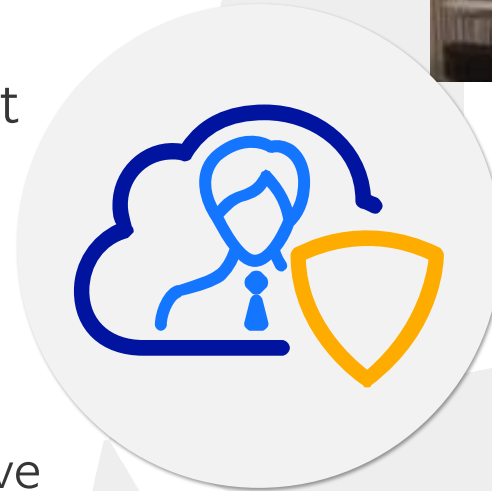
# DEMO

# MICROSOFT SERVICE PRINCIPALS

COMMON NAME	PERMISSIONS
Microsoft Rights Management Services	<u>Directory.Read.All</u> <u>Member.Read.Hidden</u>
Office 365 Exchange Online	<u>Directory.Read.All</u> <u>Group.ReadWrite.All</u> <u>User.Read.All</u>
Office 365 SharePoint Online	<u>Files.ReadWrite.All</u> <u>TeamsActivity.Send</u> <u>TeamsAppInstallation.ReadWriteSelfForUser.All</u>
Yammer	<u>Policy.Read.All</u> <u>Reports.Read.All</u>

# PREVENTION – USER ACCOUNTS

- Custom roles for users managing applications
  - built-in ones can be quite permissive
  - tailor very specifically
- Disable any AD user's ability to register and consent applications
- Assign "App/Cloud App Admin" and/or "App Developer" accordingly
  - Can still bypass the previous two security toggles above
- PIM, MFA, and CAs (when available for SPs) if possible



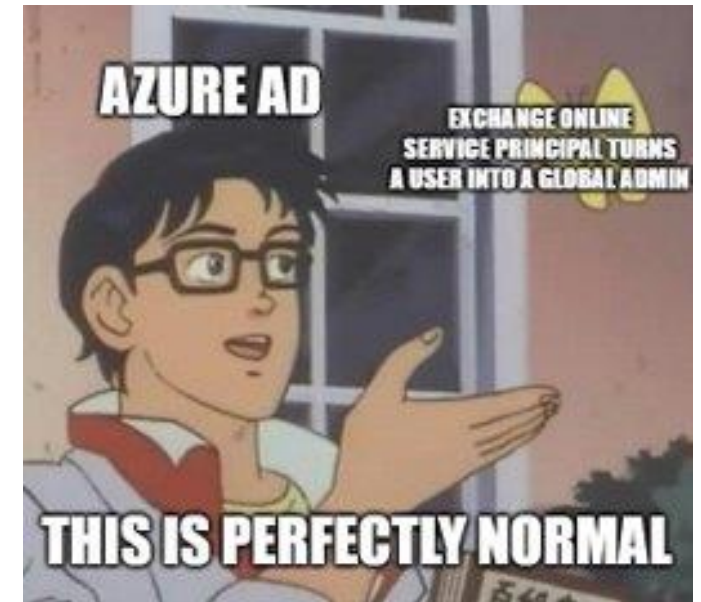
# PREVENTION – SERVICE PRINCIPALS

- Principle of least privilege - Assign only needed Graph permissions
  - Particularly for admin privileges
- Restrict role assignments for Azure resources
  - "Contributor" by default
  - Remove passwords, if added for any reason
- Perform regular reviews SPs login events
  - Any left with passwords?



# DETECTION AND MONITORING?

- Can be quite difficult specifically for this issue - allowed by design
- Your existing logging/monitoring capabilities can detect *some* things
- A tailored set of alerting policies
  - Focus on critical SP's activity, not just user's
- No sign-in logs for 1<sup>st</sup> party Microsoft Applications



# ATTACK PATH IDENTIFICATION CYPHER QUERIES

- MATCH (a:AADRole)-[r]-(t:AADUser) WHERE (a.name = 'Application Administrator' OR a.name = 'Cloud Application Administrator') RETURN \*
- MATCH (a:AADRole) WHERE a.name = 'Application Developer' RETURN \*
- MATCH (a:AADRole)-[r]-(t) WHERE r.roleName = 'Contributor' AND a.objectType = 'ServicePrincipal' OR a.objectType = 'Application' RETURN \*
- MATCH (a)-[r]-(t) WHERE (r.roleName = 'Contributor' OR r.roleName = 'Owner') AND (a.objectType = 'ServicePrincipal' OR a.objectType = 'Application') RETURN \*
- MATCH (a) WHERE a.objectType = "ServicePrincipal" AND (a.passwordCredentialCount > 0 OR a.keyCredentialCount > 0) RETURN \*
- MATCH (w:ResourceGroup)-[p]-(s:Subscription)-[y]-(a:AADUser)-[r]-(g:AADGroup)-[d:MemberOf]-(AADRole) WHERE (y.roleName = "Contributor" OR y.roleName = "Owner") RETURN \*

# SP ACTIVITY KQL DETECTION QUERIES

```
// Most active Service Principals (Custom Apps)
```

```
AADServicePrincipalSignInLogs
```

```
| where TimeGenerated > ago(7d)
```

```
| summarize CountPerServicePrincipal = count() by ServicePrincipalName,  
ServicePrincipalId, AppId, IPAddress
```

```
| order by CountPerServicePrincipal desc
```

```
//TimeGenerated
```

```
// Most active AAD Applications (MS Apps)
```

```
AADNonInteractiveUserSignInLogs
```

```
| where TimeGenerated > ago(7d)
```

```
| summarize CountPerServicePrincipal = count() by AppDisplayName, AppId, Identity,  
IPAddress, TimeGenerated
```

```
//| order by CountPerServicePrincipal desc
```

# SP ACTIVITY KQL DETECTION QUERIES

```
// Suspicious activity by SPs
```

```
// Look for audit logs in the last x days as needed
```

```
// Filter by SP OperationName of interest for these attacks
```

```
// Filter by escalation-related OperationName and AAD App Identity
```

## **AuditLogs**

```
| where TimeGenerated > ago(7d)
```

```
| where OperationName == "Add service principal credentials"
```

```
or OperationName == "Remove service principal credentials"
```

```
or OperationName == "Add app role assignment to service principal"
```

```
or OperationName == "Update service principal"
```

```
|| where OperationName == "Add member to group" and Identity == "Office 365 Exchange Online"
```

```
| summarize CountPerServicePrincipal = count() by Identity, OperationName
```

```
//TimeGenerated
```

# TAKEAWAYS

Service principals are an equally interesting attack vector as privileged users

- Aim at identifying anomalous behavior indicating human intervention

Proactively identify potential targets of compromise

- Admin users, Apps deployed, sensitive Azure resources
- Tools such as StormSpotter and cypher queries can be of great help

Prevention of these issues is no easy task

- Build layered defenses <sup>[5]</sup>
- Set up detection around eventual compromise

# REFERENCES

1. <https://www.microsoft.com/security/blog/2020/06/18/inside-microsoft-threat-protection-mapping-attack-chains-from-cloud-to-endpoint/>
2. <https://www.microsoft.com/security/blog/2021/03/09/azure-lolbins-protecting-against-the-dual-use-of-virtual-machine-extensions/>
3. <https://dirkjanm.io/azure-ad-privilege-escalation-application-admin/>
4. <https://github.com/Azure/Stormspotter>
5. <https://lnkd.in/e7RPappr>
6. Follow us on Twitter for news on the tool release



# THE END – THANK YOU!

Questions?



<p><b>INCIDENT</b></p> <p><b>PRINCIPLE: COLLABORATION</b> <b>SECURITY ANALYSTS FORM A CAPABLE TEAM</b></p> <p>The "assume breach" model requires that attackers will eventually attain privileged access within your organization. As your organization increases its security posture, the need to monitor for and respond to incidents grows. This is why it is essential to have a team of security analysts who can monitor for and respond to incidents in real-time. This is why it is essential to have a team of security analysts who can monitor for and respond to incidents in real-time.</p>	<p><b>CONTINUOUS IMPROVEMENT</b></p> <p><b>PRINCIPLE: CONTINUOUS IMPROVEMENT</b> <b>IMPLEMENTING SECURITY DETECTION AND RESPONSE</b></p> <p>Log management is a continuous process. It is not a one-time activity. It is a process that evolves over time. It is a process that evolves over time. It is a process that evolves over time.</p>	<p><b>RESOURCES</b></p> <p><b>PRINCIPLE: CONTINUOUS IMPROVEMENT</b> <b>HIGHLIGHT DEFICIENCIES</b></p> <p>Resource governance is essential for ensuring that your Azure environment is secure. It is a process that evolves over time. It is a process that evolves over time. It is a process that evolves over time.</p>	<p><b>POLICIES</b></p> <p><b>PRINCIPLE: EFFECTIVE SECURITY AND COMPLIANCE DEVELOPMENT ACT</b></p> <p>As your Azure environment grows, it becomes more complex. It becomes more complex. It becomes more complex. It becomes more complex. It becomes more complex.</p>	<p><b>LOGGING</b></p> <p><b>PRINCIPLE: COMPREHENSIVE LOGGING</b> <b>CREATES A RELIABLE PERFORMANCE ANALYSIS</b></p> <p>Logging is an essential part of any security program. It is a process that evolves over time. It is a process that evolves over time. It is a process that evolves over time.</p>	<p><b>RBAC</b></p> <p><b>PRINCIPLE: EFFECTIVE SECURITY AND COMPLIANCE DEVELOPMENT ACT</b></p> <p>Role-based access control (RBAC) is a security model that allows you to control access to your Azure resources. It is a process that evolves over time. It is a process that evolves over time. It is a process that evolves over time.</p>	<p><b>IDENTITY</b></p> <p><b>PRINCIPLE: DEFINING IDENTITY</b> <b>THEM CAN LIMIT ACCESS</b></p> <p>Identity is a key component of any security program. It is a process that evolves over time. It is a process that evolves over time. It is a process that evolves over time.</p>	<p><b>BACKUPS</b></p> <p><b>PRINCIPLE: BACKUP DATA</b> <b>IN THE EVENT OF A DISASTER</b></p> <p>Disasters do happen and loss of data is a real possibility. It is a process that evolves over time. It is a process that evolves over time. It is a process that evolves over time.</p>	<p><b>RESOURCES</b></p> <p><b>PRINCIPLE: ISOLATE RADIUS</b> <b>OF A CYBER INCIDENT</b></p> <p>If one resource is compromised, it can affect other resources. It is a process that evolves over time. It is a process that evolves over time. It is a process that evolves over time.</p>	<p><b>INVENTORY</b></p> <p><b>PRINCIPLE: UNDERSTAND YOUR SURFACE</b></p> <p>Correctly managing the resources in your Azure environment is an essential part of any security program. It is a process that evolves over time. It is a process that evolves over time. It is a process that evolves over time.</p>	<p><b>SECURITY</b></p> <p><b>PRINCIPLE: UNDERSTAND YOUR SURFACE</b></p> <p>Although 95% of Fortune 500 companies use Microsoft Azure, there is still a significant security gap. It is a process that evolves over time. It is a process that evolves over time. It is a process that evolves over time.</p>
---	--	---	--	--	--	--	---	--	--	--

## MICROSOFT AZURE SECURITY FRAMEWORK

A roadmap for hardening the security of your Azure environment

An F-Secure Consulting guide  
Authors: Emilian Cebuc and Christian Philippov

**CONTENTS**

- 01 INTRODUCTION
- 02 INVENTORY
- 04 RESOURCE
- 06 BACKUP
- 07 IDENTIFY
- 11 LOGGING
- 14 POLICIES
- 15 RESOURCE
- 16 CONTINUOUS
- 18 INCIDENT



**F-Secure**®