Securing IaC with Microsoft tooling

Craig Forshaw

Craig Forshaw

- Cloud architect @ Crayon
- Azure, Security, Terraform & Bicep
- Organiser – Microsoft Security User Group
- Hobbies; Football, Cycling, Skiing
- Terrible at gaming!

Microsoft Security
USER GROUP

The evolving landscape of an infrastructure engineer

Microsoft security – practices and tooling

- Securing Infrastructure as code (IaC) using Bicep
- Using Github Copilot as your secure code adviser
- Security in Github and Azure DevOps
- Using Defender for DevOps to monitor your repositories

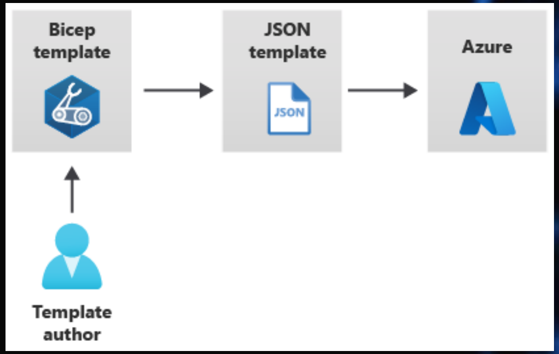
Best practices - Securing IaC (Bicep) code

Azure Resource Manager (ARM) Templates

- Introduced in 2014
- JSON based

Bicep

- Launched August 31, 2020
- Domain specific IaC language



Securing Parameters

ARM

- ARM templates provide ‘secureString’ & ‘secureObject’ data types

Bicep

- *@secure()*
  param password string
- *@secure()*
  param configValues object

Secret management

Avoid secrets where possible

Use managed identities both system assigned and user assigned

Use service managed certificates for handling certificates and private key pairs

Use dynamic secret lookup from another resource

Access key from one resource to another

existing = { name: storageAccountName }

var storageAccountConnectionString =

Store secrets in Azure KeyVault

For use with modules –

keyVaultName.getSecret(secretName)

For use with .bicepparam file -

param secureUserName = az.getSecret('<subscriptionId>', '<resourceGroupName>', '<keyVaultName>', '<secretName>', '<secretVersion>')

Other considerations

Avoid outputs

Secret management

Adding, rotating, deleting

State management

- ARM & Bicep does not store state like Terraform
  - Bicep uses an incremental deployment method
  - No security requirements for state storage, such as Disk encryption, RBAC
- State storage in clear text can reveal secrets and information associated with your tenant, subscriptions ID's etc.
  - Encrypt by default
  - Use RBAC
- Out of band changes are a challenge and often overlooked
  - Drift detection alerting should be planned

Azure resource security with Bicep

What can we do to secure resources?

- Policy as code
  - Azure Security baseline for azure policy
- Managed service identities
- Role assignments
- Privileged access management
- Access reviews
- Resource locks…but be careful Protect your Azure resources with a lock - Azure Resource Manager | Microsoft Learn

Microsoft Security
USER GROUP

Azure resource security with Bicep

Managed service identities

Policy as code

- Azure Security baseline for azure policy

Role assignments

Privileged access management

Access reviews

Resource locks…but be careful

Microsoft Security USER GROUP

Github Copilot

- AI code completion tool by GitHub and OpenAI to assist developers with coding
- Can also be used to help find security vunerabilties in code

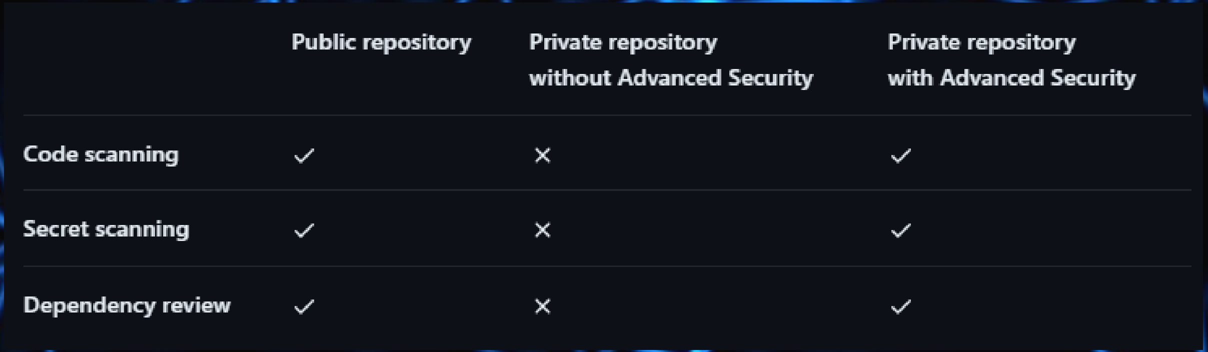
Github Copilot Chat (Public Beta)

- Released 20th Sept
- Chat interface to engage with Copilot
- Ask for code suggestions, fixes, explanation

- Individual license ($10) and business license ($19)

Github Advanced Security

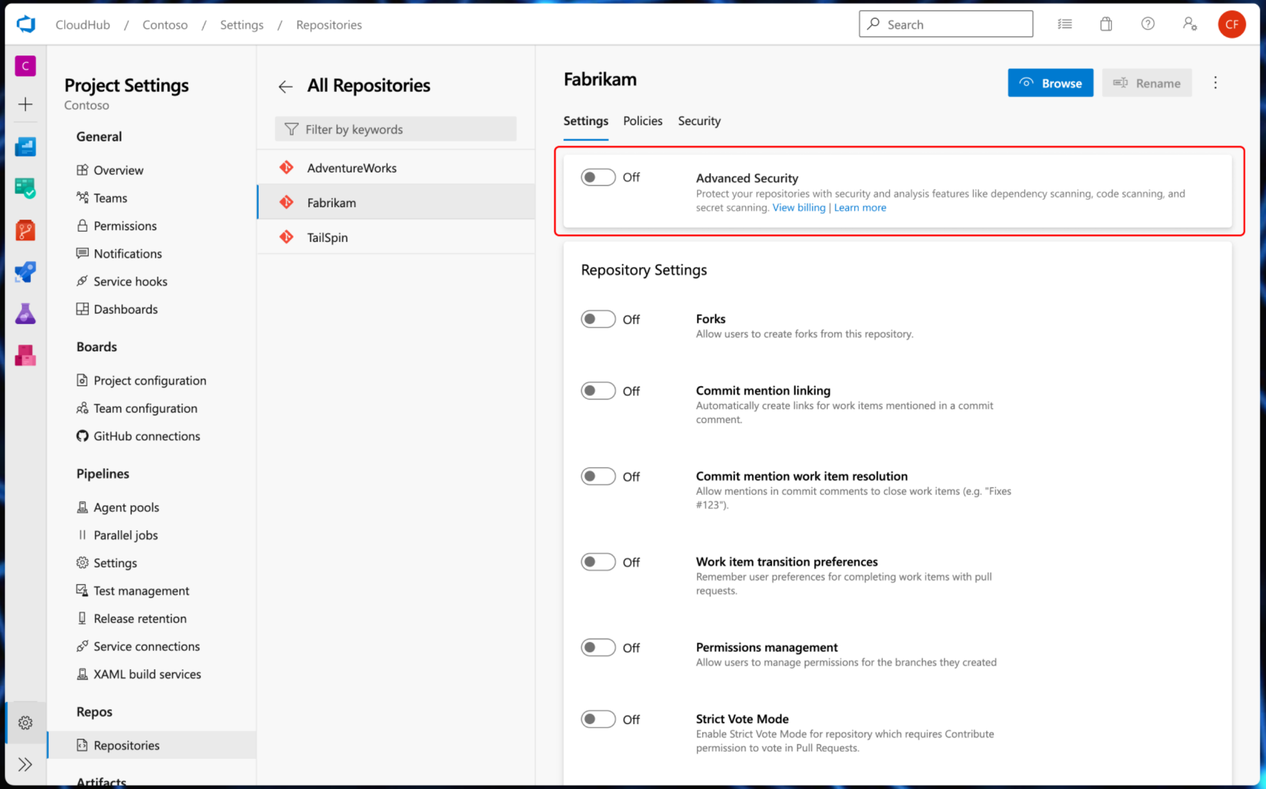
- Code scanning - Search for potential security vulnerabilities in your code however codeQL is not supporting IaC tools just yet
- Secret scanning - Detect secrets, for example keys and tokens, that have been checked into the repository.
- Dependency review
- Starter workflows for advanced security



	Public repository	Private repository without Advanced Security	Private repository with Advanced Security
Code scanning	✓	✕	✓
Secret scanning	✓	✕	✓
Dependency review	✓	✕	✓

Azure DevOps

- Github advanced security feature launched 20th september
  - Enable per org, project or repo level
- Billing: $49 per active committer per month and enables usage and invoice management through your Azure subscription.
  - Active user is someone who commits within a 90-day period



Off — **Advanced Security**
Protect your repositories with security and analysis features like dependency scanning, code scanning, and secret scanning. View billing | Learn more

Repository Settings

Off — **Forks**
Allow users to create forks from this repository.

Off — **Commit mention linking**
Automatically create links for work items mentioned in a commit comment.

Off — **Commit mention work item resolution**
Allow mentions in commit comments to close work items (e.g. "Fixes #123").

Off — **Work item transition preferences**
Remember user preferences for completing work items with pull requests.

Off — **Permissions management**
Allow users to manage permissions for the branches they created

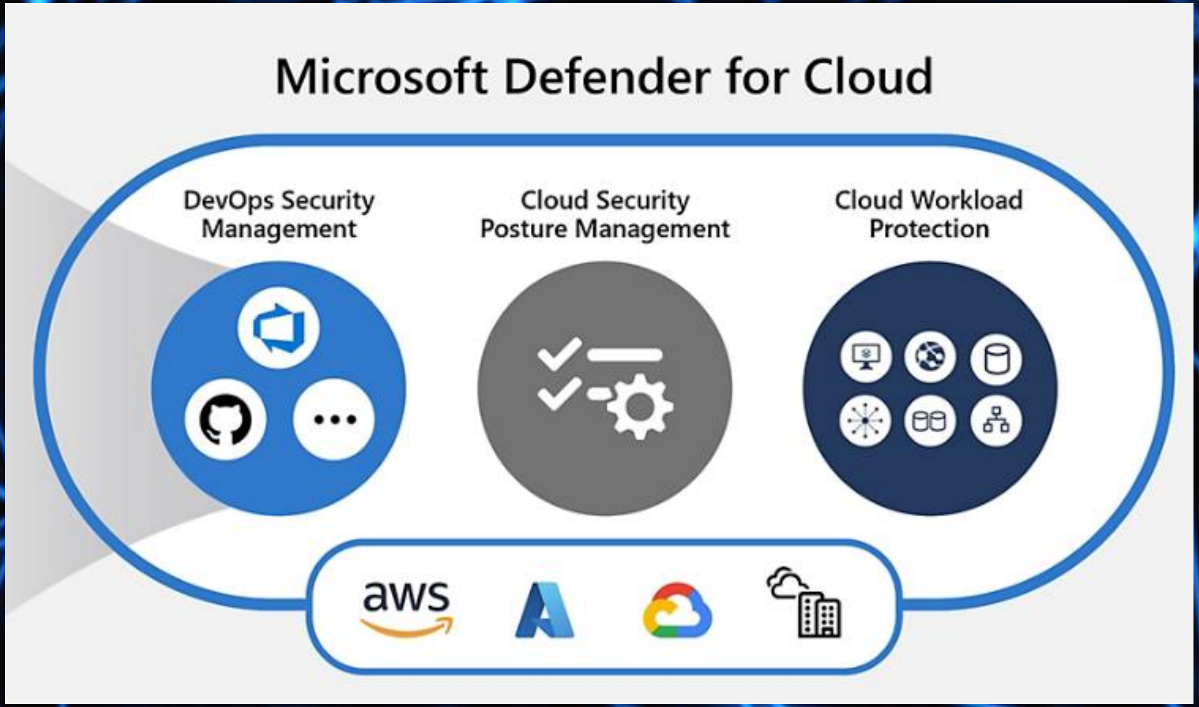
Off — **Strict Vote Mode**
Enable Strict Vote Mode for repository which requires Contribute permission to vote in Pull Requests.

Microsoft Security
USER GROUP

@MsSecUG
#MSUG

Defender for DevOps

- Service in Defender for Cloud for DevOps security posture management of code repositories
- Includes code scanning capabilities for IaC in an action/pipeline run
- Connects to Azure DevOps & Github as well as GCP and AWS
- Requires github advanced security features enabled
- Public preview since October 2022


Microsoft Defender for Cloud
DevOps Security Management
Cloud Security Posture Management
Cloud Workload Protection
aws

Microsoft security github action

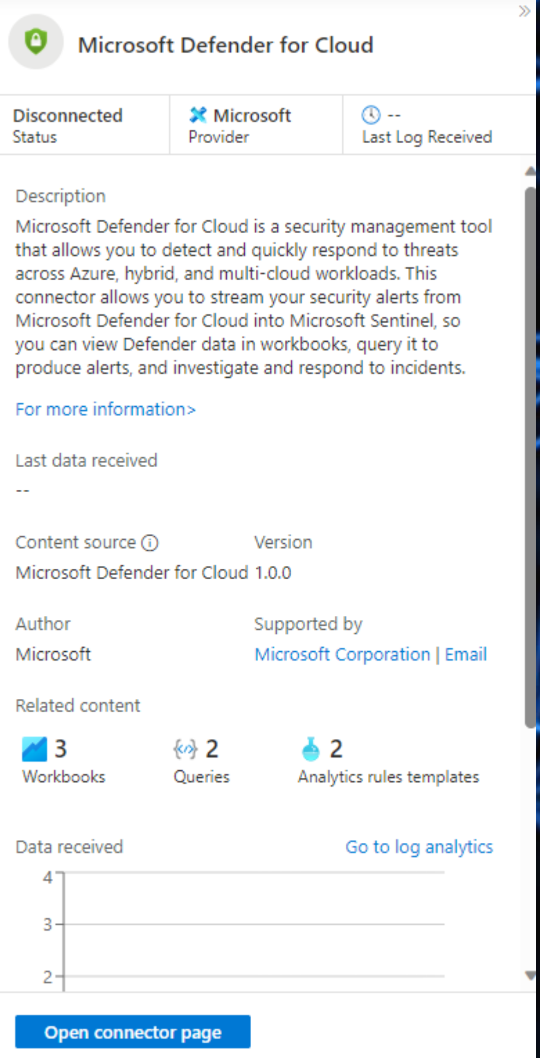
- Action template that scans repositories for known vunerabilities
- Uses the following open source tools

Name	Language	License
AntiMalware	AntiMalware protection in Windows from Microsoft Defender for Endpoint, that scans for malware and breaks the build if malware has been found. This tool scans by default on windows-latest agent.	Not Open Source
Bandit	Python	Apache License 2.0
BinSkim	Binary--Windows, ELF	MIT License
ESlint	JavaScript	MIT License
Template Analyzer	ARM template, Bicep file	MIT License
Terrascan	Terraform (HCL2), Kubernetes (JSON/YAML), Helm v3, Kustomize, Dockerfiles, Cloud Formation	Apache License 2.0
Trivy	container images, file systems, git repositories	Apache License 2.0

Monitoring with Sentinel

Connectors

- Continuous threat monitoring for GitHub
- Microsoft Defender for Cloud – stream security alerts to sentinel



Microsoft Defender for Cloud

Disconnected
Status

Microsoft
Provider

--
Last Log Received

Description

Microsoft Defender for Cloud is a security management tool that allows you to detect and quickly respond to threats across Azure, hybrid, and multi-cloud workloads. This connector allows you to stream your security alerts from Microsoft Defender for Cloud into Microsoft Sentinel, so you can view Defender data in workbooks, query it to produce alerts, and investigate and respond to incidents.

For more information>

Last data received
--

Content source	Version
Microsoft Defender for Cloud	1.0.0

Author	Supported by
Microsoft	Microsoft Corporation | Email

Related content

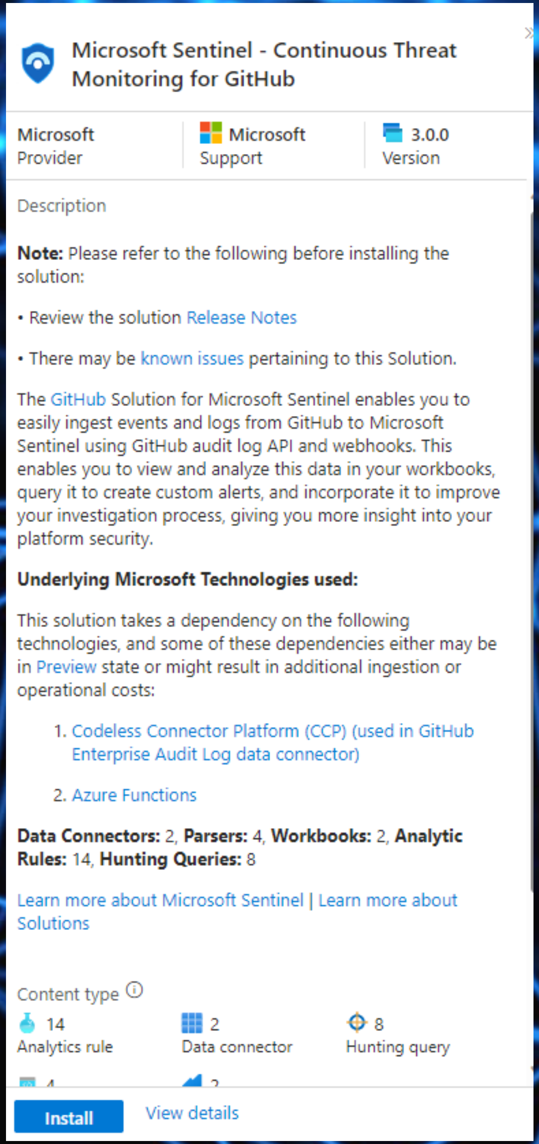
3 Workbooks

2 Queries

2 Analytics rules templates

Data received

Go to log analytics



Microsoft Sentinel - Continuous Threat Monitoring for GitHub

Microsoft
Provider

Microsoft
Support

3.0.0
Version

Description

Note: Please refer to the following before installing the solution:

- Review the solution Release Notes
- There may be known issues pertaining to this Solution.

The GitHub Solution for Microsoft Sentinel enables you to easily ingest events and logs from GitHub to Microsoft Sentinel using GitHub audit log API and webhooks. This enables you to view and analyze this data in your workbooks, query it to create custom alerts, and incorporate it to improve your investigation process, giving you more insight into your platform security.

Underlying Microsoft Technologies used:

This solution takes a dependency on the following technologies, and some of these dependencies either may be in Preview state or might result in additional ingestion or operational costs:

1. Codeless Connector Platform (CCP) (used in GitHub Enterprise Audit Log data connector)
2. Azure Functions

Data Connectors: 2, **Parsers:** 4, **Workbooks:** 2, **Analytic Rules:** 14, **Hunting Queries:** 8

Learn more about Microsoft Sentinel | Learn more about Solutions

Content type

14 Analytics rule

2 Data connector

8 Hunting query

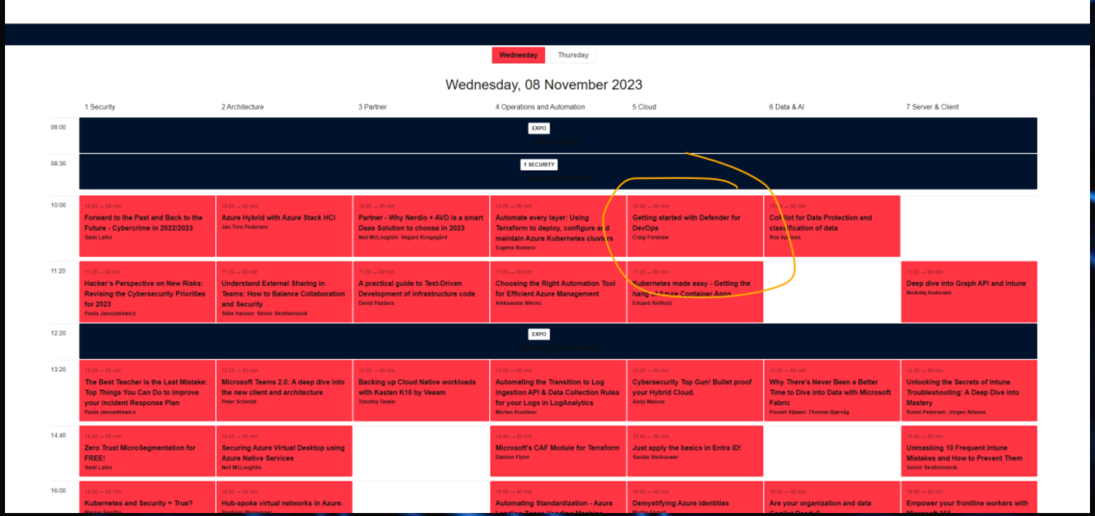
Summary

- Microsoft improving security tooling geared toward IaC with DevSecOps
- Best practices are the best way to secure code
- Github advanced security is a key component to securing code
- Defender for DevOps for monitoring code repositories
- Future is tighter integration between all areas copilot, github advanced security, Defender for DevOps & Sentinel

Check out my blog

Securing infrastructure as code (IaC) with the Microsoft technology stack | by Craig Forshaw | Sep, 2023 | Medium

See you at NIC! Nordic Infrastructure Conference | NIC Cloud Connect (nicconf.com)



Wednesday Thursday

Wednesday, 08 November 2023

	1 Security	2 Architecture	3 Partner	4 Operations and Automation	5 Cloud	6 Data & AI	7 Server & Client
08:00	EXPO Doors open						
08:30	1 SECURITY Opening Keynote						
10:00	10:00 — 60 min Forward to the Past and Back to the Future - Cybercrime in 2022/2023 Sami Laiho	10:00 — 60 min Azure Hybrid with Azure Stack HCI Jan-Tore Pedersen	10:00 — 60 min Partner - Why Nerdio + AVD is a smart Daas Solution to choose in 2023 Neil McLoughlin Vegard Kongsgård	10:00 — 60 min Automate every layer: Using Terraform to deploy, configure and maintain Azure Kubernetes clusters Eugene Romero	10:00 — 60 min Getting started with Defender for DevOps Craig Forshaw	10:00 — 60 min CoPilot for Data Protection and classification of data Roy Apalnes	
11:20	11:20 — 60 min Hacker's Perspective on New Risks: Revising the Cybersecurity Priorities for 2023 Paula Januszkiewicz	11:20 — 60 min Understand External Sharing in Teams: How to Balance Collaboration and Security Ståle Hansen Simon Skotheimsvik	11:20 — 60 min A practical guide to Test-Driven Development of infrastructure code David Pazdera	11:20 — 60 min Choosing the Right Automation Tool for Efficient Azure Management Aleksandar Nikolic	11:20 — 60 min Kubernetes made easy - Getting the hang of Azure Container Apps Eduard Keilholz		11:20 — 60 min Deep dive into Graph API and Intune Nickolaj Andersen
12:20	EXPO Lunch @ Expo Area						
13:20	13:20 — 60 min The Best Teacher is the Last Mistake: Top Things You Can Do to Improve your Incident Response Plan Paula Januszkiewicz	13:20 — 60 min Microsoft Teams 2.0: A deep dive into the new client and architecture Peter Schmidt	13:20 — 60 min Backing up Cloud Native workloads with Kasten K10 by Veeam Timothy Dewin	13:20 — 60 min Automating the Transition to Log Ingestion API & Data Collection Rules for your Logs in LogAnalytics Morten Knudsen	13:20 — 60 min Cybersecurity Top Gun! Bullet proof your Hybrid Cloud. Andy Malone	13:20 — 60 min Why There's Never Been a Better Time to Dive into Data with Microsoft Fabric Puneet Vijwani Thomas Bjørvåg	13:20 — 60 min Unlocking the Secrets of Intune Troubleshooting: A Deep Dive into Mastery Ronni Pedersen Jörgen Nilsson
14:40	14:40 — 60 min Zero Trust MicroSegmentation for FREE! Sami Laiho	14:40 — 60 min Securing Azure Virtual Desktop using Azure Native Services Neil McLoughlin		14:40 — 60 min Microsoft's CAF Module for Terraform Damian Flynn	14:40 — 60 min Just apply the basics in Entra ID! Sander Berkouwer		14:40 — 60 min Unmasking 10 Frequent Intune Mistakes and How to Prevent Them Simon Skotheimsvik
16:00	16:00 — 60 min Kubernetes and Security = True?	16:00 — 60 min Hub-spoke virtual networks in Azure.		16:00 — 60 min Automating Standardization - Azure	16:00 — 60 min Demystifying Azure identities	16:00 — 60 min Are your organization and data	16:00 — 60 min Empower your frontline workers with

Microsoft Security
USER GROUP