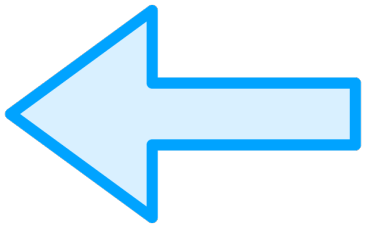
Automate Security and Compliance Scanning

John Savill
Chief Architect

@ntfaqguy | onboardtoazure.com

Common Security and Privacy Challenges with Repositories

Shifting Security Left



Security is top of mind for every organization

The earlier threats can be identified and mitigated the better

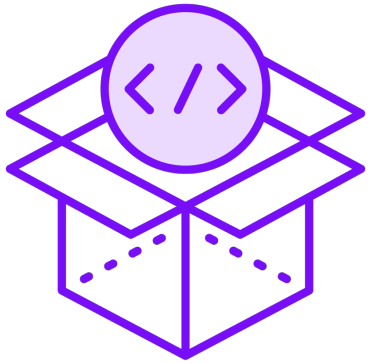
Shifting lefts moves security early in our processes

DevSecOps integrates DevOps and Security

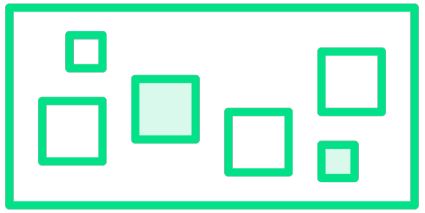
Common Sources of Vulnerability

Code

Secrets



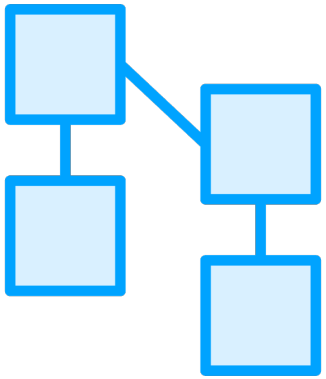
Dependencies



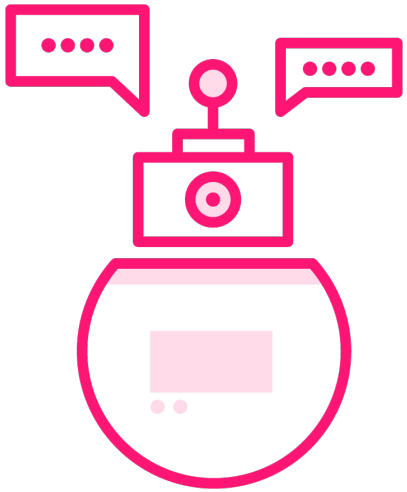
Container images

Using GitHub Advanced Security

Features for All Plans



Dependency graph



Dependabot alerts

GitHub Advanced Security License Features

Code scanning	CodeQL CLI	Secret scanning
Custom auto-triage rules	Dependency review	Security advisories

Licensing for GitHub

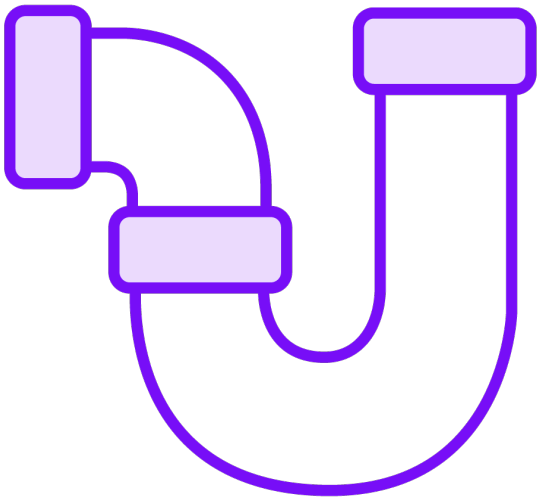
FREE

Public Repos

GitHub Advanced Security license

Private/Internal Repos

GitHub Advanced Security for Azure DevOps



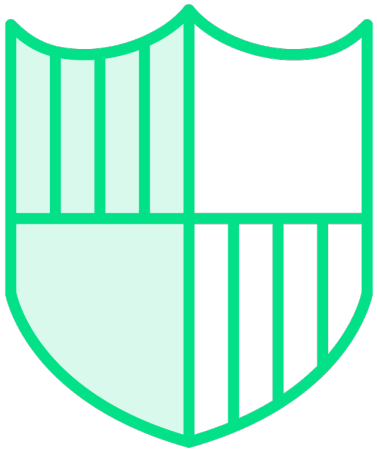
The key features are also available for Azure DevOps

The implementation is different

Secret, dependency, and code scanning are part of the pipeline flow

Requires GitHub Advanced Security for Azure DevOps license

GitHub Integration with Defender for Cloud



GitHub organizations can be connected to Defender for Cloud

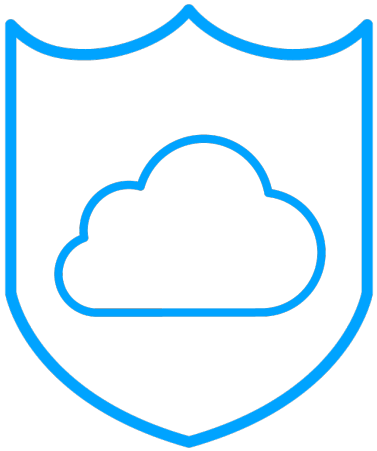
This enables advanced DevOps posture capabilities

Signals from GitHub Advanced Security are fed into Defender for Cloud

Microsoft Security DevOps GitHub action is available

Using Microsoft Defender for Cloud DevOps Security

Defender for Cloud Overview



Defender for Cloud is Microsoft's full suite of security solutions

This solution works across the entire lifecycle

Works across clouds and operating systems

Has many different offerings

Posture management is at its core

Defender for Cloud DevOps Security

Works across Azure DevOps, GitHub and GitLab

Provides unified posture management and threat protection

Recommendations are given

Exact features vary based on free vs paid and the DevOps solution

Enabling Code and Container Scanning

Code Scanning

Code scanning looks for vulnerabilities in your code

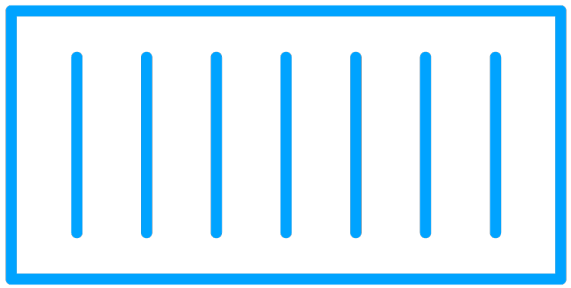
This includes security flaws and coding errors

GitHub CodeQL enables code to be queryable like data

This enables standard and custom queries to identify the vulnerabilities

Often these queries will be run as part of your CICD

Container Scanning



There are two types of container scanning

- Runtime containerized application scanning
- Container image scanning

There are numerous solutions that support different aspects and platforms

- Security posture
- Vulnerability assessment
- Run-time threat protection
- Deployment & monitoring

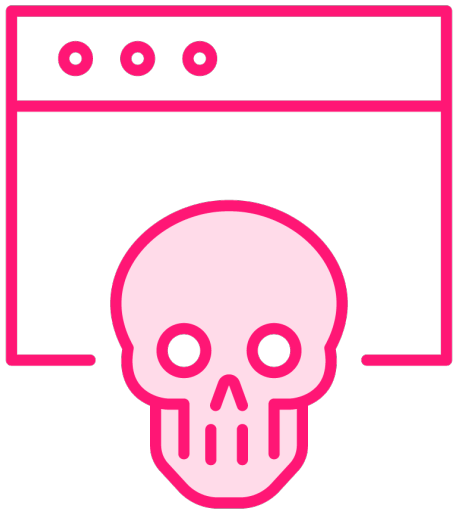
Microsoft Defender for Containers

Azure, AWS, GCP and Arc-enabled K8S clusters

Container runtime and image scanning

Azure Policy for Kubernetes

Microsoft Defender for Vulnerability Management



Container image vulnerability scanning is performed via Defender for Vulnerability Management

This is agentless

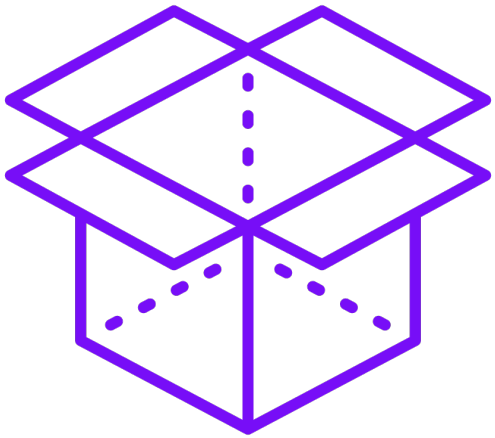
Images are scanned shortly after addition

24 hour rescan cadence for in-scope images

Searches for known CVEs

Open-source Component Capabilities

Where Is Open-source Used?



Very few applications are written from scratch

Most applications use existing components for the majority of functionality

Often open-source software is utilized

It can be used during development, release and operations

Therefore, the answer is “everywhere”

What Are Open-source Challenges?

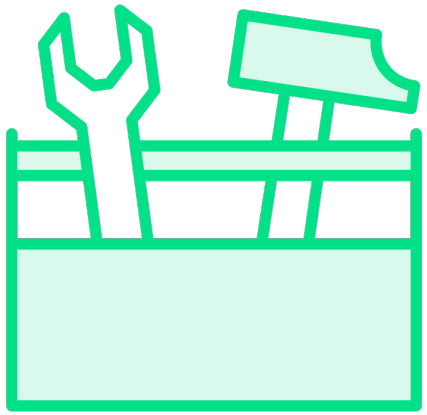
Quality

Security risks & vulnerabilities

Support & maintenance

License restrictions

Software Composition Analysis



As an organization it's critical to understand where open-source is used

Companies often want to control package management

Azure Artifacts enables complete control over packages utilized

Also use GitHub dependency graph and dependabot alerts