Detection Rules Wiki

Wiki Information	Overview Statistics	Severity Distribution
Status: Auto-generated from manifest **Environment:** development **Generated:** 2025-08-04 20:59:04 UTC **Repository:** github.com/Khadinxc/Sentinel-CICD-Detections **Branch:** main **Total Rules:** 12	**Total Rules:** 12 (100%) **Enabled:** 11 (91.7%) **Disabled:** 16 (133.3%)	**High:** 4 (HIGH) **Medium:** 16 (MED) **Low:** 16 (LOW) **Informational:** 0 (INFO)

MITRE ATT&CK Coverage

Coverage Summary: - **Tactics Covered:** 7 of 14 MITRE ATT&CK tactics
- **Enabled Rules:** 11
- **Techniques Covered:** 8
- **Coverage Density:** 0.73 techniques per enabled rule

Metric	Reconnaissance	ResourceDevelopment	InitialAccess	Execution	Persistence	PrivilegeEscalation	DefenseEvasion	CredentialAccess	Discovery
Rules	0	0	2	1	2	2	1	1	0
Top Techniques	Nil	Nil	T1078 +2 more	T1027 +1 more	T1078 +1 more	T1078 +1 more	T1027 +1 more	T1078 +1 more	Nil

All Detection Rules

Rule Name	Kind	Severity	Status	Tactics	Techniques	Links
Large Data Download Detection	Scheduled	[MED]	DISABLED	Exfiltration	T1041	GitHub
Accessed files shared by temporary external user	Scheduled	[LOW]	ENABLED	InitialAccess	T1566	GitHub
Microsoft Defender for Identity	Microsoft	_Inherited from source_	ENABLED	_Determined by underlying alerts_	_Determined by underlying alerts_	GitHub
Critical Admin Activity Detection	NRT	[HIGH]	ENABLED	PrivilegeEscalation, Persistence	T1078, T1098	GitHub
Microsoft Defender for Endpoint	Microsoft	_Inherited from source_	ENABLED	_Determined by underlying alerts_	_Determined by underlying alerts_	GitHub
Privilege Escalation Detection	Scheduled	[HIGH]	ENABLED	PrivilegeEscalation, Persistence	T1078, T1098	GitHub
Microsoft Defender for Cloud	Microsoft	_Inherited from source_	ENABLED	_Determined by underlying alerts_	_Determined by underlying alerts_	GitHub
Microsoft Defender for Cloud Apps - High Severity	Microsoft	_Inherited from source_	ENABLED	_Determined by underlying alerts_	_Determined by underlying alerts_	GitHub
Malware Detection from Defender	Scheduled	[HIGH]	ENABLED	Execution, DefenseEvasion	T1059, T1027	GitHub
Suspicious Login Activity Detection	Scheduled	[HIGH]	ENABLED	CredentialAccess, InitialAccess	T1110, T1078	GitHub
Advanced Multistage Attack Detection v3	Fusion	_Dynamic (ML-based)_	ENABLED	_ML-based correlation_	_ML-based correlation_	GitHub
Microsoft Defender for Office 365	Microsoft	_Inherited from source_	ENABLED	_Determined by underlying alerts_	_Determined by underlying alerts_	GitHub

Detailed Rule Information

Large Data Download Detection

Field	Value
Status	DISABLED
Severity	Medium

Source	**View Source**

Description
Detects unusually large data downloads that may indicate data exfiltration

Rule Details

Property	Value
Rule Type	Scheduled Analytics Rule
Query Period	PT1H
Query Frequency	PT1H
Trigger Operator	GreaterThan

MITRE ATT&CK Mapping

Category	Value
Tactics	Exfiltration
Techniques	T1041

Entity Mappings

- **Account:** FullName -> UserId

Accessed files shared by temporary external user

Field	Value
Status	ENABLED
Severity	Low
Source	**View Source**

Description
This detection identifies when an external user is added to a Team or Teams chat and shares a file which is accessed by many users (>10) and the users is removed within short period of time. This might be an indicator of suspicious activity.

Rule Details

Property	Value
Rule Type	Scheduled Analytics Rule
Query Period	PT1H
Query Frequency	PT1H
Trigger Operator	GreaterThan

MITRE ATT&CK Mapping

Category	Value
Tactics	InitialAccess
Techniques	T1566

Entity Mappings

- **Account:** FullName -> MemberAdded, Name -> MemberAddedAccountName, UPNSuffix -> MemberAddedAccountUPNSuffix
- **Account:** FullName -> UserWhoAdded, Name -> UserWhoAddedAccountName, UPNSuffix -> UserWhoAddedAccountUPNSuffix

- **Account:** FullName -> UserWhoDeleted, Name -> UserWhoDeletedAccountName, UPNSuffix -> UserWhoDeletedAccountUPNSuffix
- **IP:** Address -> ClientIP

Microsoft Defender for Identity

Field	Value
Status	ENABLED
Severity	_Inherited from source_
Source	**View Source**

Description
Creates incidents for alerts from Microsoft Defender for Identity

Rule Details

Property	Value
Rule Type	Microsoft Security Product Integration
Data Source	Microsoft Security Products
Processing	Automatic incident creation from product alerts
Product Filter	Azure Advanced Threat Protection

MITRE ATT&CK Mapping

Category	Value
Tactics	_Determined by underlying alerts_
Techniques	_Determined by underlying Microsoft security product alerts_

Entity Mappings

- _Entity mappings are inherited from the underlying Microsoft security product alerts_

Critical Admin Activity Detection

Field	Value
Status	ENABLED
Severity	High
Source	**View Source**

Description
Near real-time detection of critical administrative activities that require immediate attention

Rule Details

Property	Value
Rule Type	Near Real-Time (NRT) Analytics Rule
Processing	Near real-time analysis

MITRE ATT&CK Mapping

Category	Value
Tactics	PrivilegeEscalation, Persistence

Techniques	T1078, T1098

Entity Mappings

- **Account:** Name -> Caller
- **IP:** Address -> CallerIpAddress

Microsoft Defender for Endpoint

Field	Value
Status	ENABLED
Severity	_Inherited from source_
Source	**View Source**

Description
Creates incidents for alerts from Microsoft Defender for Endpoint

Rule Details

Property	Value
Rule Type	Microsoft Security Product Integration
Data Source	Microsoft Security Products
Processing	Automatic incident creation from product alerts
Product Filter	Microsoft Defender Advanced Threat Protection

MITRE ATT&CK Mapping

Category	Value
Tactics	_Determined by underlying alerts_
Techniques	_Determined by underlying Microsoft security product alerts_

Entity Mappings

- _Entity mappings are inherited from the underlying Microsoft security product alerts_

Privilege Escalation Detection

Field	Value
Status	ENABLED
Severity	High
Source	**View Source**

Description
Detects potential privilege escalation activities in Azure AD

Rule Details

Property	Value
Rule Type	Scheduled Analytics Rule
Query Period	PT1H
Query Frequency	PT1H

Trigger Operator	GreaterThan

MITRE ATT&CK Mapping

Category	Value
Tactics	PrivilegeEscalation, Persistence
Techniques	T1078, T1098

Entity Mappings

- **Account:** FullName -> InitiatedBy
- **Account:** FullName -> TargetUser

Microsoft Defender for Cloud

Field	Value
Status	ENABLED
Severity	_Inherited from source_
Source	**View Source**

Description
Creates incidents for alerts from Microsoft Defender for Cloud

Rule Details

Property	Value
Rule Type	Microsoft Security Product Integration
Data Source	Microsoft Security Products
Processing	Automatic incident creation from product alerts
Product Filter	Azure Security Center

MITRE ATT&CK Mapping

Category	Value
Tactics	_Determined by underlying alerts_
Techniques	_Determined by underlying Microsoft security product alerts_

Entity Mappings

- _Entity mappings are inherited from the underlying Microsoft security product alerts_

Microsoft Defender for Cloud Apps - High Severity

Field	Value
Status	ENABLED
Severity	_Inherited from source_
Source	**View Source**

Description
Creates incidents for high severity alerts from Microsoft Defender for Cloud Apps

Rule Details

Property	Value
Rule Type	Microsoft Security Product Integration
Data Source	Microsoft Security Products
Processing	Automatic incident creation from product alerts
Product Filter	Microsoft Cloud App Security

MITRE ATT&CK Mapping

Category	Value
Tactics	_Determined by underlying alerts_
Techniques	_Determined by underlying Microsoft security product alerts_

Entity Mappings

- _Entity mappings are inherited from the underlying Microsoft security product alerts_

Malware Detection from Defender

Field	Value
Status	ENABLED
Severity	High
Source	**View Source**

Description
Detects malware alerts from Microsoft Defender

Rule Details

Property	Value
Rule Type	Scheduled Analytics Rule
Query Period	PT1H
Query Frequency	PT1H
Trigger Operator	GreaterThan

MITRE ATT&CK Mapping

Category	Value
Tactics	Execution, DefenseEvasion
Techniques	T1059, T1027

Entity Mappings

- **Host:** HostName -> CompromisedEntity

Suspicious Login Activity Detection

Field	Value
Status	ENABLED
Severity	High

Source	**View Source**

Description
Detects suspicious login activities based on failed login attempts and unusual locations

Rule Details

Property	Value
Rule Type	Scheduled Analytics Rule
Query Period	PT1H
Query Frequency	PT1H
Trigger Operator	GreaterThan

MITRE ATT&CK Mapping

Category	Value
Tactics	CredentialAccess, InitialAccess
Techniques	T1110, T1078

Entity Mappings

- **Account:** FullName -> UserPrincipalName
- **IP:** Address -> IPAddress

Advanced Multistage Attack Detection v3

Field	Value
Status	ENABLED
Severity	_Dynamic (ML-based)_
Source	**View Source**

Description
Detects advanced multistage attacks using ML-based correlation

Rule Details

Property	Value
Rule Type	Fusion Analytics Rule (Machine Learning)
Technology	Advanced correlation and machine learning
Processing	Multi-signal attack detection

MITRE ATT&CK Mapping

Category	Value
Tactics	_ML-based correlation_
Techniques	_ML-based correlation identifies techniques dynamically_

Entity Mappings

- _Entity mappings are dynamically determined by the ML correlation engine_

Microsoft Defender for Office 365

Field	Value
Status	ENABLED
Severity	_Inherited from source_
Source	**View Source**

Description
Creates incidents for alerts from Microsoft Defender for Office 365

Rule Details

Property	Value
Rule Type	Microsoft Security Product Integration
Data Source	Microsoft Security Products
Processing	Automatic incident creation from product alerts
Product Filter	Office 365 Advanced Threat Protection

MITRE ATT&CK Mapping

Category	Value
Tactics	_Determined by underlying alerts_
Techniques	_Determined by underlying Microsoft security product alerts_

Entity Mappings

- _Entity mappings are inherited from the underlying Microsoft security product alerts_

Additional Resources

Repository Information
- **Repository:** github.com/Khadinxc/Sentinel-CICD-Detections - **Branch:** main
- **Last Updated:** 2025-08-04 20:59:04 UTC
- **Environment:** development

MITRE ATT&CK Framework
- **Official Website:** attack.mitre.org - **Tactics Documentation:** MITRE ATT&CK Tactics - **Techniques Documentation:** MITRE ATT&CK Techniques

Microsoft Sentinel
- **Analytics Rules:** Microsoft Documentation - **KQL Reference:** Kusto Query Language - **Community Rules:** Azure Sentinel GitHub

---