Product Solutions Resources Open Source Enterprise Pricing Sign in Sign up

elastic / detection-rules Public

Notifications Fork 498 Star 2k

Code Issues 144 Pull requests 28 Actions Security Insights

Files

065bf48

Go to file

- .github
- detection_rules
- docs
- etc
- kibana
- kql
- rta
- rules
  - _deprecated
  - apm
  - cross-platform
  - integrations
    - aws
    - azure
      - collection_update_event_hub...
      - credential_access_key_vault_...
      - credential_access_storage_acc...
      - defense_evasion_azure_applic...
      - defense_evasion_azure_diagn...
      - defense_evasion_azure_servic...
      - defense_evasion_event_hub_...
      - defense_evasion_firewall_polic...
      - defense_evasion_network_wa...
      - discovery_blob_container_acc...
      - execution_command_virtual_...
      - impact_azure_automation_ru...
      - impact_azure_service_principa...
      - impact_kubernetes_pod_delet...
      - impact_resource_group_deleti...
      - initial_access_azure_active_dir...
      - initial_access_azure_active_dir...
      - initial_access_consent_grant_...
      - initial_access_external_guest_...
      - persistence_azure_automatio...
      - persistence_azure_automatio...
      - persistence_azure_automatio...

detection-rules / rules / integrations / azure / impact_kubernetes_pod_deleted.toml

⚠ This commit does not belong to any branch on this repository, and may belong to a fork outside of the repository.

austinsonger Update 065bf48 · 3 years ago History

Code Blame 48 lines (42 loc) · 1.51 KB Raw

```
[metadata]
creation_date = "2021/06/24"
maturity = "production"
updated_date = "2021/06/24"

[rule]
author = ["Austin Songer"]
description = """
Identifies the deletion of Azure Kubernetes Pods.
"""
false_positives = [
    """
    Pods may be deleted by a system administrator. Verify whether the user identity, us
    should be making changes in your environment. Pods deletions from unfamiliar users
    investigated. If known behavior is causing false positives, it can be exempted from
    """,
]
from = "now-25m"
index = ["filebeat-*", "logs-azure*"]
language = "kuery"
license = "Elastic License v2"
name = "Azure Kubernetes Pods Deleted"
note = """## Config

The Azure Fleet integration, Filebeat module, or similarly structured data is required
references = [
    "https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider
]
risk_score = 47
rule_id = "83a1931d-8136-46fc-b7b9-2db4f639e014"
severity = "medium"
tags = ["Elastic", "Cloud", "Azure", "Continuous Monitoring", "SecOps", "Asset Visibili
timestamp_override = "event.ingested"
type = "query"

query = '''
event.dataset:azure.activitylogs and azure.activitylogs.operation_name:MICROSOFT.KUBERN
event.outcome:(Success or success)
'''


[[rule.threat]]
framework = "MITRE ATT&CK"

[rule.threat.tactic]
id = "TA0040"
name = "Impact"
reference = "https://attack.mitre.org/tactics/TA0040/"
```

- persistence_azure_conditional...
- persistence_azure_pim_user_a...
- persistence_azure_privileged_i...
- persistence_mfa_disabled_for...
- persistence_user_added_as_o...
- persistence_user_added_as_o...