Files

main

Go to file

- .github
- detection_rules
- docs
- hunting
- lib
- rta
- rules
  - _deprecated
  - apm
  - cross-platform
  - integrations
    - aws
      - NOTICE.txt
      - collection_cloudtrail_logging_...
      - credential_access_aws_getpas...
      - credential_access_aws_iam_as...
      - credential_access_iam_compr...
      - credential_access_iam_user_a...
      - credential_access_new_terms_...
      - credential_access_rapid_secre...
      - credential_access_retrieve_sec...
      - credential_access_root_consol...
      - defense_evasion_cloudtrail_lo...
      - defense_evasion_cloudtrail_lo...
      - defense_evasion_cloudwatch_...
      - defense_evasion_config_servi...
      - defense_evasion_configuratio...
      - defense_evasion_ec2_flow_lo...
      - defense_evasion_ec2_networ...
      - defense_evasion_elasticache_...
      - defense_evasion_elasticache_...
      - defense_evasion_guardduty_...
      - defense_evasion_rds_instance...
      - defense_evasion_route53_dn...
      - defense_evasion_s3_bucket_c...
      - defense_evasion_s3_bucket_li...

detection-rules / rules / integrations / aws / initial_access_via_system_manager.toml

shashank-elastic Back-porting Version Trimming (#3704) ✓ 63e91c2 · 6 months ago History

Code Blame 114 lines (95 loc) · 5.96 KB Raw

```
[metadata]
creation_date = "2020/07/06"
integration = ["aws"]
maturity = "production"
updated_date = "2024/05/21"

[rule]
author = ["Elastic"]
description = """
Identifies the execution of commands and scripts via System Manager. Execution methods
RunPowerShellScript, and alike can be abused by an authenticated attacker to install a
compromised instance via reverse-shell using system only commands.
"""
false_positives = [
    """
    Verify whether the user identity, user agent, and/or hostname should be making chan
    Suspicious commands from unfamiliar users or hosts should be investigated. If known
    positives, it can be exempted from the rule.
    """,
]
from = "now-60m"
index = ["filebeat-*", "logs-aws.cloudtrail-*"]
interval = "10m"
language = "kuery"
license = "Elastic License v2"
name = "AWS Execution via System Manager"
note = """## Triage and analysis

### Investigating AWS Execution via System Manager

Amazon EC2 Systems Manager is a management service designed to help users automatically

This rule looks for the execution of commands and scripts using System Manager. Note th

#### Possible investigation steps

- Identify the user account that performed the action and whether it should perform thi
- Investigate other alerts associated with the user account during the past 48 hours.
- Validate that the activity is not related to planned patches, updates, network admini
- Investigate the commands or scripts using host-level visibility.
- Considering the source IP address and geolocation of the user who issued the command:
    - Do they look normal for the calling user?
    - If the source is an EC2 IP address, is it associated with an EC2 instance in one
    - If it is an authorized EC2 instance, is the activity associated with normal behav
- Assess whether this behavior is prevalent in the environment by looking for similar o
- Contact the account owner and confirm whether they are aware of this activity.
- Check if this operation was approved and performed according to the organization's ch
- If you suspect the account has been compromised, scope potentially compromised assets

### False positive analysis

- If this rule is noisy in your environment due to expected activity, consider adding e

### Response and remediation

- Initiate the incident response process based on the outcome of the triage.
- Disable or limit the account during the investigation and response.
```

- defense_evasion_s3_bucket_s...
- defense_evasion_sts_get_fede...
- defense_evasion_vpc_security...
- defense_evasion_waf_acl_dele...
- defense_evasion_waf_rule_or_...
- discovery_ec2_multi_region_d...

```
- Disable or limit the account during the investigation and response.
- Identify the possible impact of the incident and prioritize accordingly; the followin
    - Identify the account role in the cloud environment.
    - Assess the criticality of affected services and servers.
    - Work with your IT team to identify and minimize the impact on users.
    - Identify if the attacker is moving laterally and compromising other accounts, ser
    - Identify any regulatory or legal ramifications related to this activity.
- Investigate credential exposure on systems compromised or used by the attacker to ens
- Check if unauthorized new users were created, remove unauthorized new accounts, and r
- Consider enabling multi-factor authentication for users.
- Review the permissions assigned to the implicated user to ensure that the least privi
- Implement security best practices [outlined](https://aws.amazon.com/premiumsupport/kn
- Take the actions needed to return affected systems, data, or services to their normal
- Identify the initial vector abused by the attacker and take action to prevent reinfec
- Using the incident response data, update logging and audit policies to improve the me

## Setup

The AWS Fleet integration, Filebeat module, or similarly structured data is required to
references = ["https://docs.aws.amazon.com/systems-manager/latest/userguide/ssm-plugins
risk_score = 21
rule_id = "37b211e8-4e2f-440f-86d8-06cc8f158cfa"
severity = "low"
tags = [
    "Domain: Cloud",
    "Data Source: AWS",
    "Data Source: Amazon Web Services",
    "Data Source: AWS SSM",
    "Use Case: Log Auditing",
    "Tactic: Initial Access",
    "Resources: Investigation Guide",
]
timestamp_override = "event.ingested"
type = "query"

query = '''
event.dataset:aws.cloudtrail and event.provider:ssm.amazonaws.com and event.action:Send
'''


[[rule.threat]]
framework = "MITRE ATT&CK"
[[rule.threat.technique]]
id = "T1566"
name = "Phishing"
reference = "https://attack.mitre.org/techniques/T1566/"
[[rule.threat.technique.subtechnique]]
id = "T1566.002"
name = "Spearphishing Link"
reference = "https://attack.mitre.org/techniques/T1566/002/"



[rule.threat.tactic]
id = "TA0001"
name = "Initial Access"
reference = "https://attack.mitre.org/tactics/TA0001/"
```