AWS Security Automation Framework:

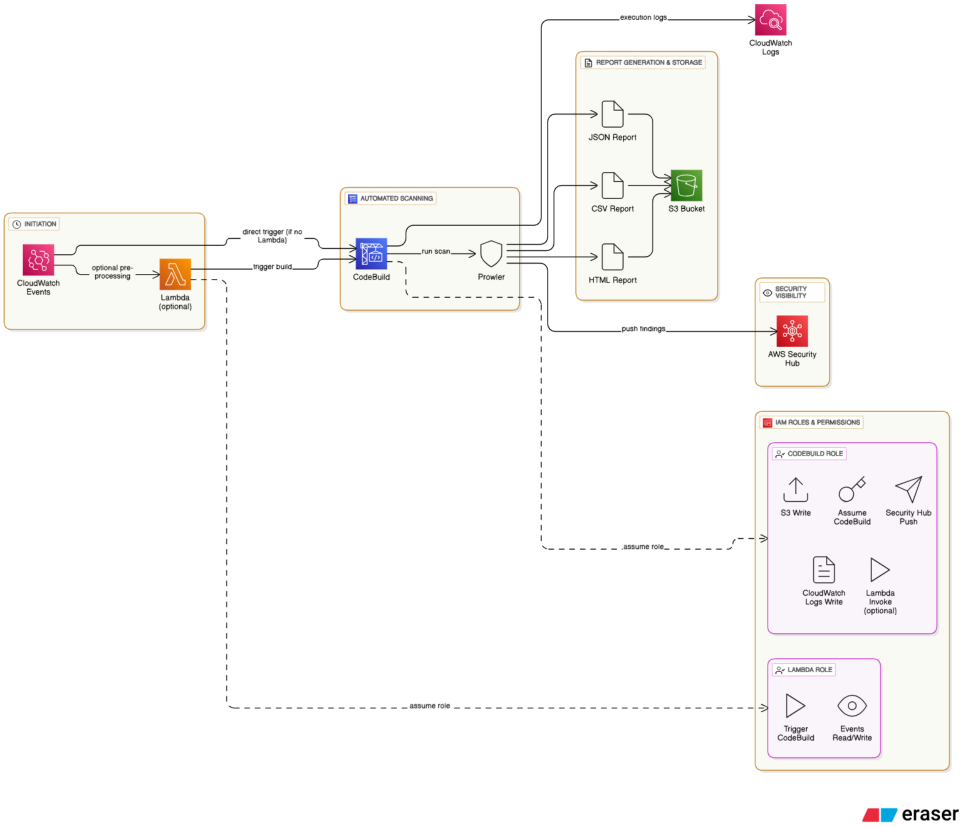
By: Ritvik Indupuri

Abstract

This document details the implementation of an automated security framework within Amazon Web Services (AWS). The framework leverages **Prowler**, **AWS CodeBuild**, and **AWS Security Hub** to enable continuous security posture assessment, identify vulnerabilities, ensure compliance, and streamline reporting across AWS cloud environments.

Solution Architecture

The framework is designed for continuous, automated security assessments against defined benchmarks. **Prowler scans**, the core assessment component, are orchestrated for daily execution via **AWS CodeBuild** projects. The generated scan reports are securely stored in designated **Amazon S3 buckets**, providing a centralized and auditable repository for historical data. All identified findings are then ingested into **AWS Security Hub**, which acts as a central dashboard for aggregated visibility and streamlined vulnerability management. **AWS CloudWatch** is integral for real-time monitoring and logging of the automation pipeline's execution. Meticulously configured **IAM roles** ensure least privilege access and secure operation of all components.



Caption: Architectural diagram for the Security Automation Project

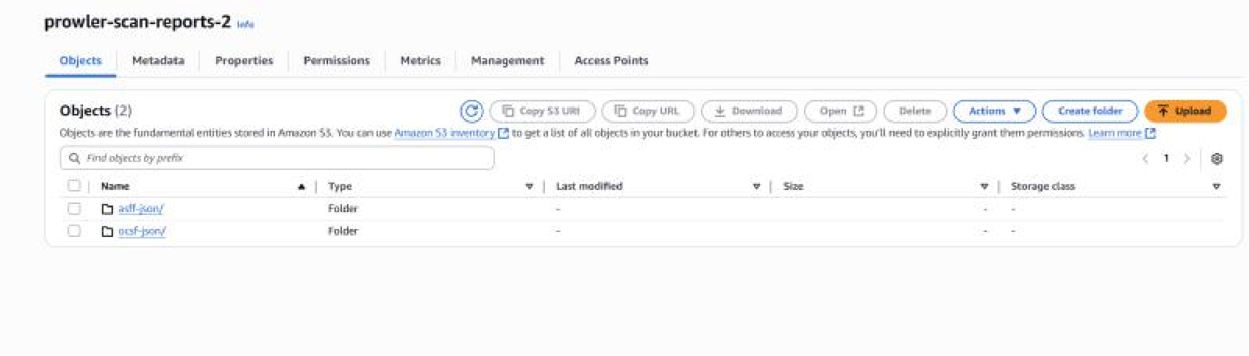
Implementation Details

Automated Scanning Pipeline

Prowler was configured to perform comprehensive security assessments across multiple AWS services. AWS CodeBuild projects were set up with a daily schedule to execute these Prowler scans automatically. This ensures consistent and up-to-date security posture evaluations.

Report Storage and Logging

Two dedicated Amazon S3 buckets were configured for storing both raw and processed Prowler scan results. This provides a secure and organized location for historical data, crucial for auditing and trend analysis.



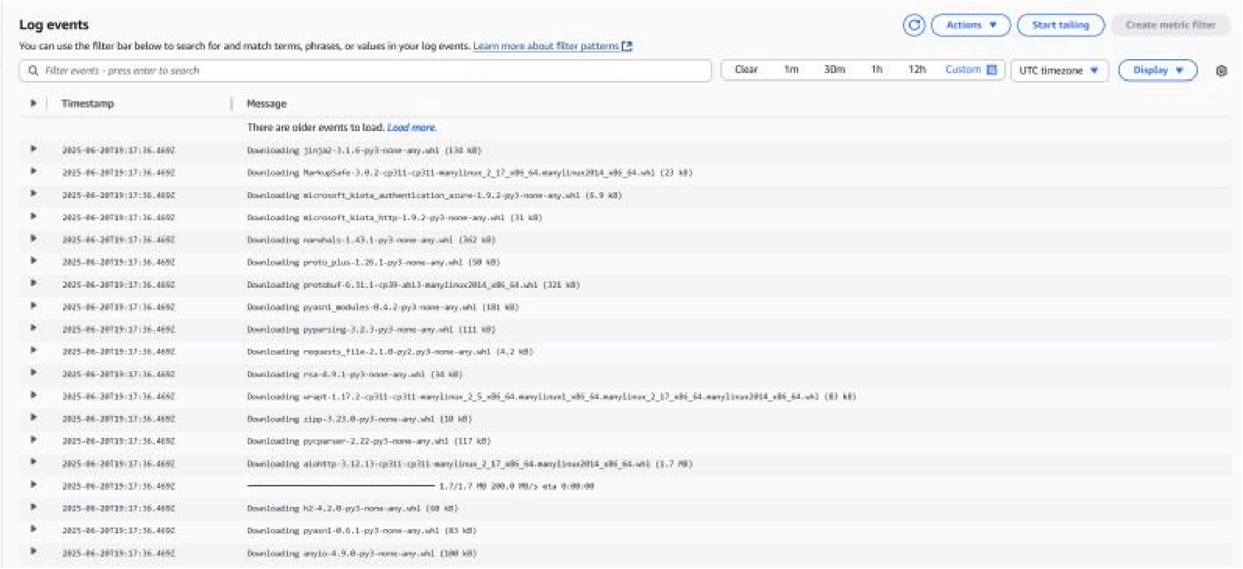
Objects (2)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

□	Name	Type	Last modified	Size	Storage class
□	asff-json/	Folder	-	-	-
□	ocsf-json/	Folder	-	-	-

Caption: Shows the Amazon S3 bucket configured specifically for storing the raw and processed scan reports generated by Prowler, ensuring organized and accessible historical data.

AWS CloudWatch was utilized to capture and review execution logs from the AWS CodeBuild runs. This provided real-time visibility into the automation pipeline's status, ensuring smooth operation and aiding in quick troubleshooting of any issues.


Log events
You can use the filter bar below to search for and match terms, phrases, or values in your log events. Learn more about filter patterns
Filter events - press enter to search
Actions
Start tailing
Create metric filter
Clear
1m
30m
1h
12h
Custom
UTC timezone
Display

```
Timestamp                   Message
                            There are older events to load. Load more.
2025-06-20T19:17:36.469Z    Downloading jinja2-3.1.6-py3-none-any.whl (134 kB)
2025-06-20T19:17:36.469Z    Downloading MarkupSafe-3.0.2-cp311-cp311-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (23 kB)
2025-06-20T19:17:36.469Z    Downloading microsoft_kiota_authentication_azure-1.9.2-py3-none-any.whl (6.9 kB)
2025-06-20T19:17:36.469Z    Downloading microsoft_kiota_http-1.9.2-py3-none-any.whl (31 kB)
2025-06-20T19:17:36.469Z    Downloading narwhals-1.43.1-py3-none-any.whl (362 kB)
2025-06-20T19:17:36.469Z    Downloading proto_plus-1.26.1-py3-none-any.whl (50 kB)
2025-06-20T19:17:36.469Z    Downloading protobuf-6.31.1-cp39-abi3-manylinux2014_x86_64.whl (321 kB)
2025-06-20T19:17:36.469Z    Downloading pyasn1_modules-0.4.2-py3-none-any.whl (181 kB)
2025-06-20T19:17:36.469Z    Downloading pyparsing-3.2.3-py3-none-any.whl (111 kB)
2025-06-20T19:17:36.469Z    Downloading requests_file-2.1.0-py2.py3-none-any.whl (4.2 kB)
2025-06-20T19:17:36.469Z    Downloading rsa-4.9.1-py3-none-any.whl (34 kB)
2025-06-20T19:17:36.469Z    Downloading wrapt-1.17.2-cp311-cp311-manylinux_2_5_x86_64.manylinux1_x86_64.manylinux_2_17_x86_64.manylinux2014_x86_64.whl (83 kB)
2025-06-20T19:17:36.469Z    Downloading zipp-3.23.0-py3-none-any.whl (10 kB)
2025-06-20T19:17:36.469Z    Downloading pycparser-2.22-py3-none-any.whl (117 kB)
2025-06-20T19:17:36.469Z    Downloading aiohttp-3.12.13-cp311-cp311-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (1.7 MB)
2025-06-20T19:17:36.469Z    ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 1.7/1.7 MB 200.0 MB/s eta 0:00:00
2025-06-20T19:17:36.469Z    Downloading h2-4.2.0-py3-none-any.whl (60 kB)
2025-06-20T19:17:36.469Z    Downloading pyasn1-0.6.1-py3-none-any.whl (83 kB)
2025-06-20T19:17:36.469Z    Downloading anyio-4.9.0-py3-none-any.whl (100 kB)
```

Caption: Illustrates real-time execution logs of the automated Prowler scans within AWS CodeBuild, as viewed through CloudWatch Logs, confirming the successful operation of the automated pipeline.

Findings Integration and Access Control

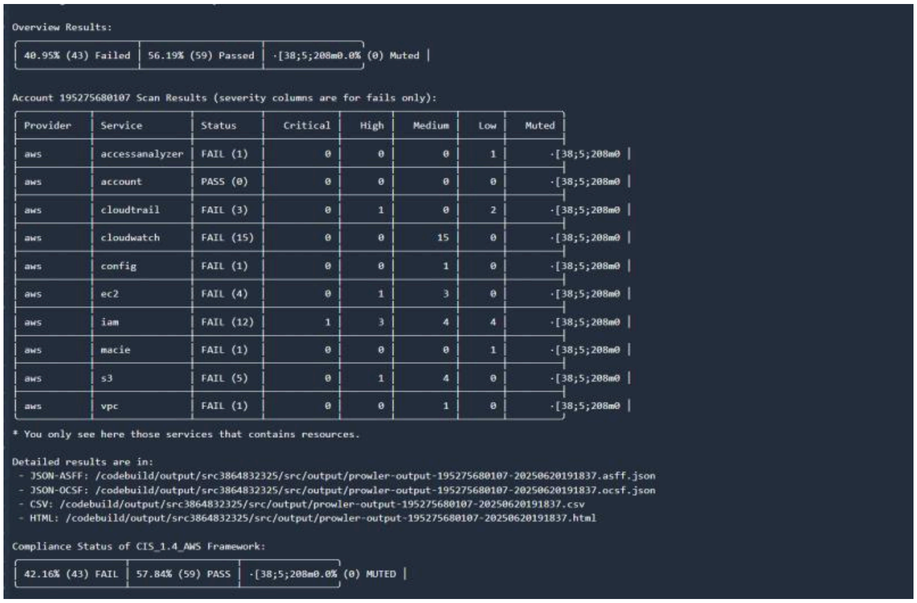
Scan outputs were integrated with AWS Security Hub, consolidating findings from Prowler with other security services for unified management and reporting. Specific IAM roles were created and configured with the minimum necessary permissions to allow CodeBuild to execute Prowler scans and interact securely with required AWS services (S3, Security Hub).

Results and Impact

The implementation of this automated security framework yielded significant improvements in the AWS environment's security posture and compliance visibility. It successfully transitioned the organization towards a more proactive and continuous security assessment model, providing actionable intelligence for risk mitigation.

Overall Compliance and Vulnerability Detection

The framework achieved a **56.19% compliance rate**, with **59 out of 105 checks passed** against defined security standards. It successfully detected **43 vulnerabilities** across 7 key AWS services, including S3, IAM, and CloudTrail, providing a clear baseline for improvement.



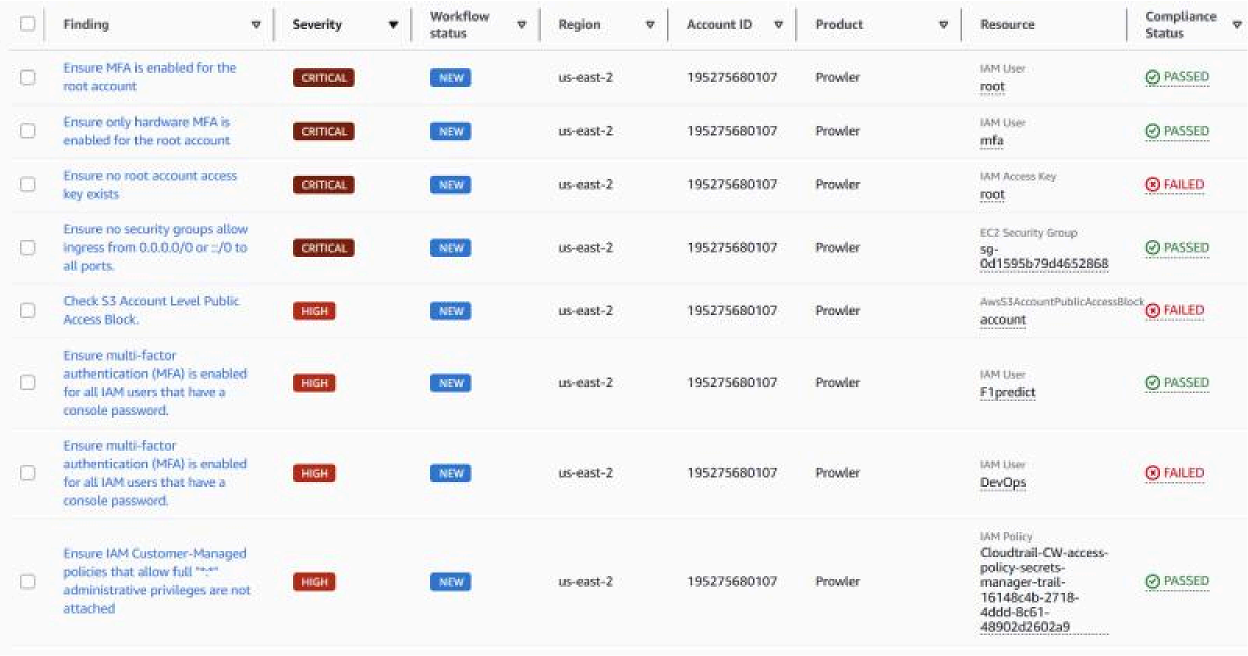
```
Overview Results:
| 40.95% (43) Failed | 56.19% (59) Passed | ·[38;5;208m0.0% (0) Muted |

Account 195275680107 Scan Results (severity columns are for fails only):
| Provider | Service         | Status    | Critical | High | Medium | Low | Muted
| aws      | accessanalyzer  | FAIL (1)  |        0 |    0 |      0 |   1 |    ·[38;5;208m0 |
| aws      | account         | PASS (0)  |        0 |    0 |      0 |   0 |    ·[38;5;208m0 |
| aws      | cloudtrail      | FAIL (3)  |        0 |    1 |      0 |   2 |    ·[38;5;208m0 |
| aws      | cloudwatch      | FAIL (15) |        0 |    0 |     15 |   0 |    ·[38;5;208m0 |
| aws      | config          | FAIL (1)  |        0 |    0 |      1 |   0 |    ·[38;5;208m0 |
| aws      | ec2             | FAIL (4)  |        0 |    1 |      3 |   0 |    ·[38;5;208m0 |
| aws      | iam             | FAIL (12) |        1 |    3 |      4 |   4 |    ·[38;5;208m0 |
| aws      | macie           | FAIL (1)  |        0 |    0 |      0 |   1 |    ·[38;5;208m0 |
| aws      | s3              | FAIL (5)  |        0 |    1 |      4 |   0 |    ·[38;5;208m0 |
| aws      | vpc             | FAIL (1)  |        0 |    0 |      1 |   0 |    ·[38;5;208m0 |
* You only see here those services that contains resources.

Detailed results are in:
 - JSON-ASFF: /codebuild/output/src3864832325/src/output/prowler-output-195275680107-20250620191837.asff.json
 - JSON-OCSF: /codebuild/output/src3864832325/src/output/prowler-output-195275680107-20250620191837.ocsf.json
 - CSV: /codebuild/output/src3864832325/src/output/prowler-output-195275680107-20250620191837.csv
 - HTML: /codebuild/output/src3864832325/src/output/prowler-output-195275680107-20250620191837.html

Compliance Status of CIS_1.4_AWS Framework:
| 42.16% (43) FAIL | 57.84% (59) PASS | ·[38;5;208m0.0% (0) MUTED |
```

Caption: Displays the overall compliance status, highlighting the 56.19% compliance rate and the distribution of 43 identified vulnerabilities across various AWS services.

Detailed Risk Identification

The automated scans identified a range of security findings categorized by severity:

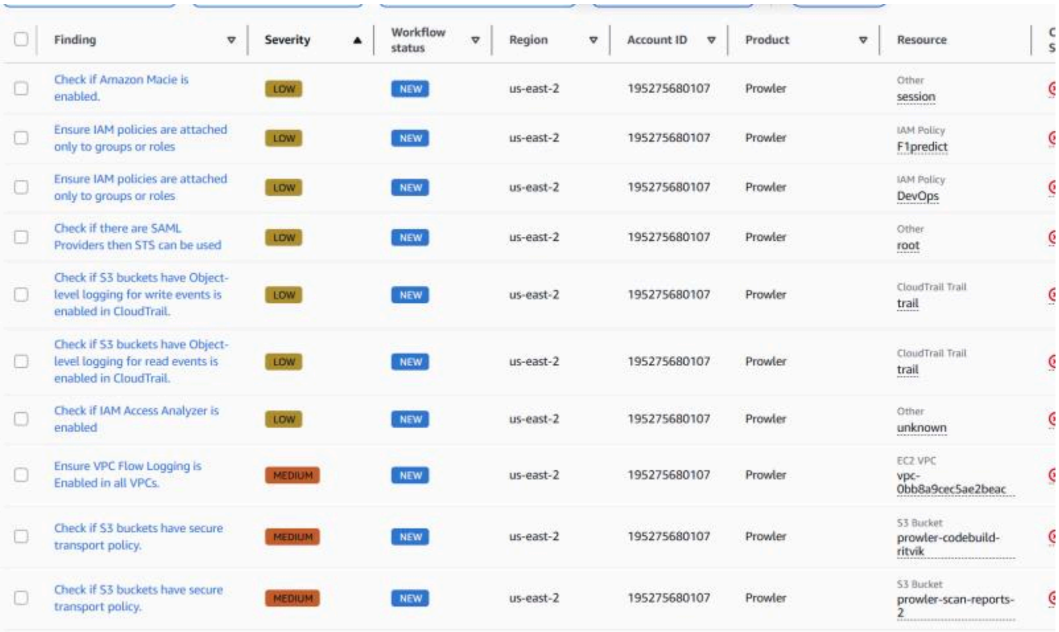
- **Critical & High Severity Findings:** Examples include alerts for missing Multi-Factor Authentication (MFA) for root accounts, unblocked S3 public access, and overly permissive IAM policies, demonstrating the framework's ability to detect significant risks.



☐	Finding	Severity	Workflow status	Region	Account ID	Product	Resource	Compliance Status
☐	Ensure MFA is enabled for the root account	CRITICAL	NEW	us-east-2	195275680107	Prowler	IAM User root	✓ PASSED
☐	Ensure only hardware MFA is enabled for the root account	CRITICAL	NEW	us-east-2	195275680107	Prowler	IAM User mfa	✓ PASSED
☐	Ensure no root account access key exists	CRITICAL	NEW	us-east-2	195275680107	Prowler	IAM Access Key root	☒ FAILED
☐	Ensure no security groups allow ingress from 0.0.0.0/0 or ::/0 to all ports.	CRITICAL	NEW	us-east-2	195275680107	Prowler	EC2 Security Group sg-0d1595b79d4652868	✓ PASSED
☐	Check S3 Account Level Public Access Block.	HIGH	NEW	us-east-2	195275680107	Prowler	AwsS3AccountPublicAccessBlock account	☒ FAILED
☐	Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password.	HIGH	NEW	us-east-2	195275680107	Prowler	IAM User F1predict	✓ PASSED
☐	Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password.	HIGH	NEW	us-east-2	195275680107	Prowler	IAM User DevOps	☒ FAILED
☐	Ensure IAM Customer-Managed policies that allow full "*:*" administrative privileges are not attached	HIGH	NEW	us-east-2	195275680107	Prowler	IAM Policy Cloudtrail-CW-access-policy-secrets-manager-trail-16148c4b-2718-4ddd-8c61-48902d2602a9	✓ PASSED

Caption: Detailed view of specific critical and high-severity security findings identified by Prowler in AWS Security Hub, such as missing MFA for root accounts and over-permissive S3 bucket policies.)

- **Low & Medium Severity Findings:** Included checks for AWS Macie enablement, proper IAM policy attachments, S3 object-level logging, and VPC Flow Logging configuration, showcasing the comprehensive nature of the vulnerability assessment.



☐	Finding	Severity	Workflow status	Region	Account ID	Product	Resource
☐	Check if Amazon Macie is enabled.	LOW	NEW	us-east-2	195275680107	Prowler	Other session
☐	Ensure IAM policies are attached only to groups or roles	LOW	NEW	us-east-2	195275680107	Prowler	IAM Policy F1predict
☐	Ensure IAM policies are attached only to groups or roles	LOW	NEW	us-east-2	195275680107	Prowler	IAM Policy DevOps
☐	Check if there are SAML Providers then STS can be used	LOW	NEW	us-east-2	195275680107	Prowler	Other root
☐	Check if S3 buckets have Object-level logging for write events is enabled in CloudTrail.	LOW	NEW	us-east-2	195275680107	Prowler	CloudTrail Trail trail
☐	Check if S3 buckets have Object-level logging for read events is enabled in CloudTrail.	LOW	NEW	us-east-2	195275680107	Prowler	CloudTrail Trail trail
☐	Check if IAM Access Analyzer is enabled	LOW	NEW	us-east-2	195275680107	Prowler	Other unknown
☐	Ensure VPC Flow Logging is Enabled in all VPCs.	MEDIUM	NEW	us-east-2	195275680107	Prowler	EC2 VPC vpc-0bb8a9cec5ae2beac
☐	Check if S3 buckets have secure transport policy.	MEDIUM	NEW	us-east-2	195275680107	Prowler	S3 Bucket prowler-codebuild-ritvik
☐	Check if S3 buckets have secure transport policy.	MEDIUM	NEW	us-east-2	195275680107	Prowler	S3 Bucket prowler-scan-reports-2

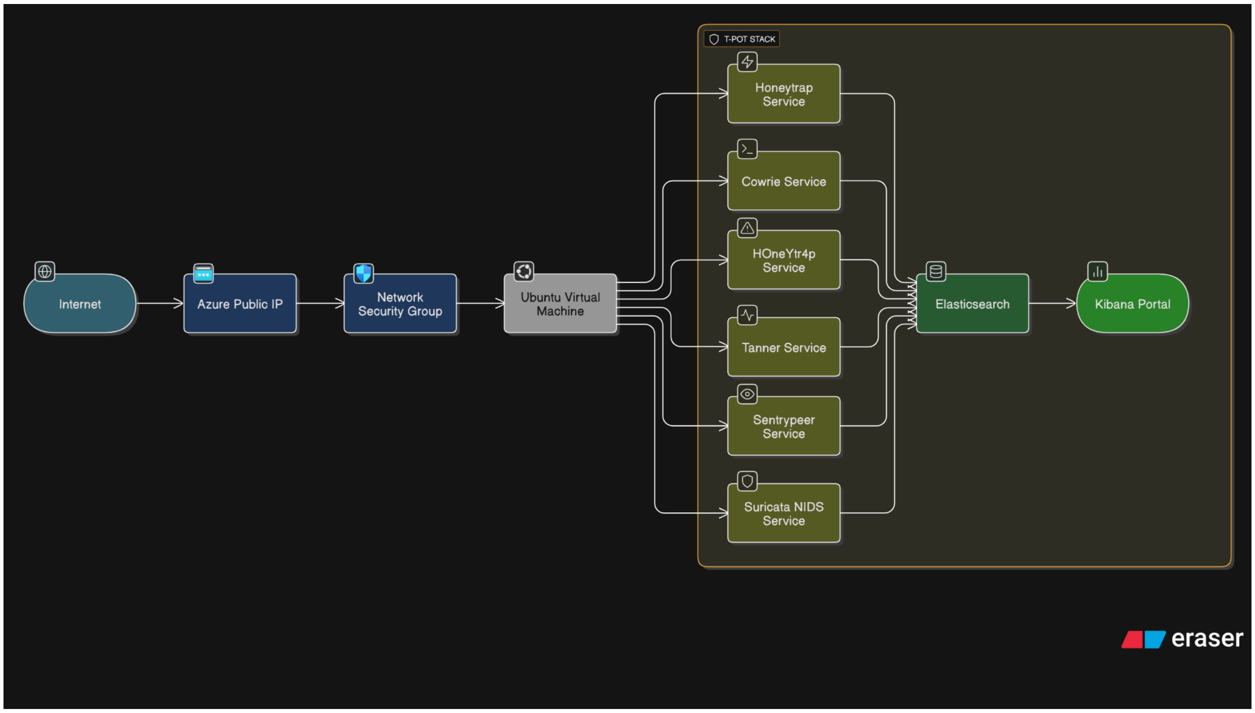
*_(Caption: Presents a detailed view of specific low and medium-severity security findings identified by Prowler, including checks for AWS Macie enablement and proper VPC Flow Logging configuration.)_

Technology Stack

- **Cloud Platform:** Amazon Web Services (AWS)
    - AWS Security Hub
    - AWS CodeBuild
    - Amazon S3
    - AWS CloudWatch
    - AWS IAM
- **Security Tool:** Prowler (Open-source cloud security best practices assessment tool)

Conclusion

This AWS Security Automation Framework successfully establishes a robust, automated pipeline for **continuous cloud security posture assessment**. By integrating **Prowler** with core **AWS services**, it significantly enhances **visibility into vulnerabilities** and **compliance deviations**, reduces manual effort, and accelerates the identification of risks. This framework serves as a foundational component for maintaining a high standard of security maturity and compliance within dynamic cloud environments. Future enhancements could include integrating **automated remediation workflows**, expanding to cover more compliance standards, or incorporating advanced threat intelligence feeds.


T-POT STACK
Internet
Azure Public IP
Network Security Group
Ubuntu Virtual Machine
Honeytrap Service
Cowrie Service
HOneYtr4p Service
Tanner Service
Sentrypeer Service
Suricata NIDS Service
Elasticsearch
Kibana Portal
eraser