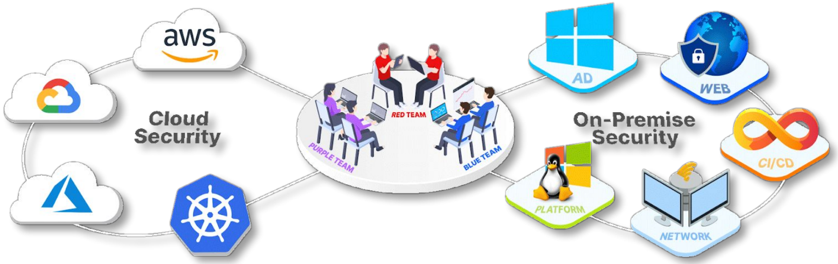
CWL
CyberWarFare Labs

BLUE OPS:
DETECTING & STOPPING S3 ATTACKS

ABOUT CYBERWARFARE LABS :

CW Labs is a Global Infosec company specializing in cybersecurity practical learning situated across UK, US & India. The company has 2 primary divisions :

1. Niche Cyber Range Labs
2. Continuous Learning : Infinity Platform



INFINITE LEARNING EXPERIENCE

About Speaker:

Ranjitha V

Security Intern@CWL

Interested in Defensive Security Operations.

Table Of Contents

- **What is a Bucket?**
- **What is Brute Bucket?**
- **Why it Matters?**
- **Detecting Suspicious Activity**
- **Stopping Brute Force Attempts**
- **The Challenge**

What is a Bucket?

- An S3 bucket is a storage container in Amazon Web Services (AWS) used to store and organize data such as files, logs, or backups.

- Each bucket has a unique name and acts like a root folder in the cloud.

What is Brute Bucket?

- Brute Bucket is a type of attack where hackers repeatedly guess S3 bucket names until they find one that exists and is misconfigured.
- The goal is to uncover sensitive data stored in exposed buckets.

Why It Matters?

- Sensitive data leakage risk
- Compliance violations
- Can be entry point for further attacks
- Reputational damage
- Financial impact

Detecting Suspicious Activity

- Analyze AWS CloudTrail / VPC Flow Logs
- Look for:
    - Repeated HeadBucket / ListObjects failures
    - High request volume from unusual IPs
    - Patterns in bucket name guesses

Stopping Brute-Force Attempts

- Enable S3 Block Public Access
- Use IAM policies & least privilege
- Configure CloudTrail alerts (Wazuh / SIEM)
- Automate blocking via AWS WAF / Security Rules
- Proactive Monitoring

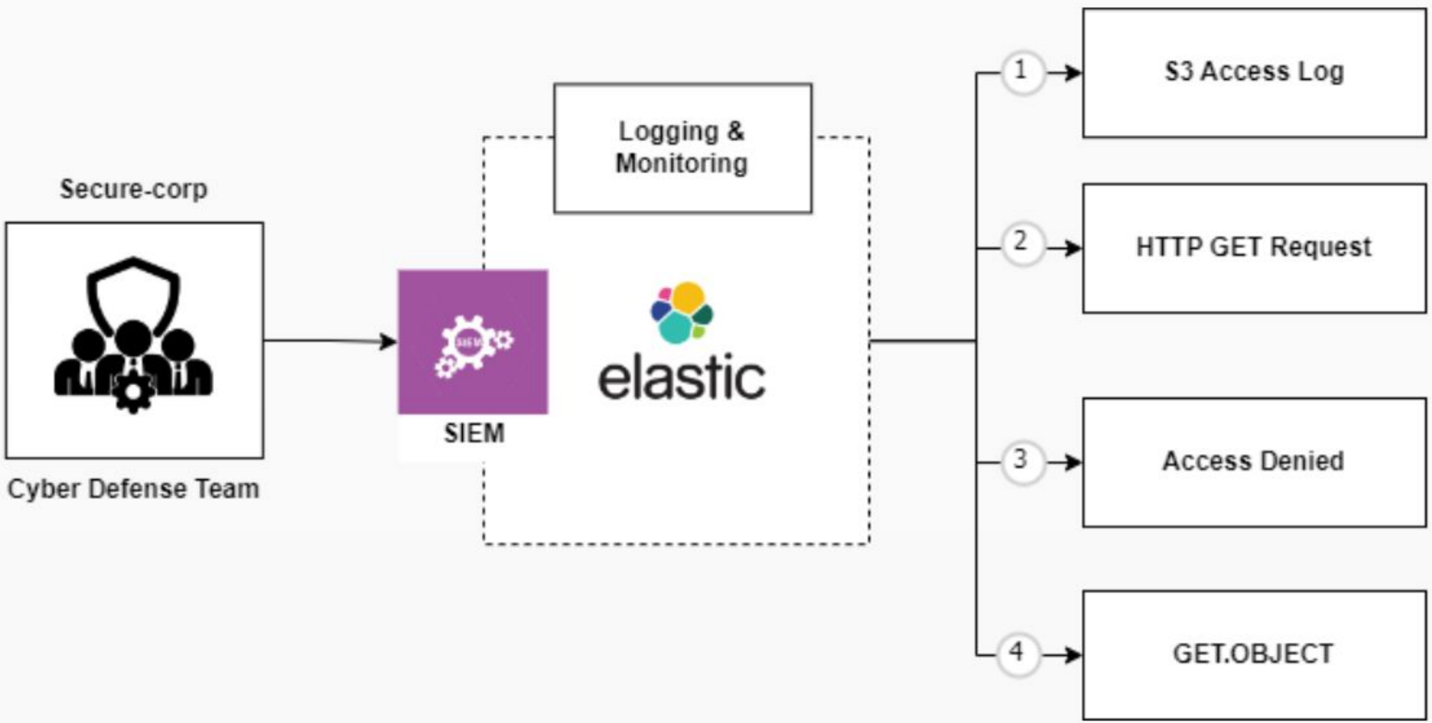
The Challenge

In this scenario, as part of Secure-corp’s security team, you are responsible for detecting and investigating suspicious brute-force attempts targeting the bucket “**securecorpimages**”

How We Solve It

By investigating CloudTrail logs and identifying repeated failed requests, we can uncover brute-force attempts. Using alerts and automated responses, we can stop attackers before they gain access.

Investigative Mind Map



CWL
CyberWarFare Labs

Thank You

For Professional Red Team / Blue Team / Purple Team / Cloud Cyber Range labs / Trainings

Please Contact :

support@cyberwarfare.live

To know more about our offerings, please visit: **https://cyberwarfare.live**