Botsv3 Security Incident Analysis

Executive Summary

This report documents a security incident identified within Frothly's AWS environment using the BOTSv3 dataset. This investigation has revealed a sophisticated attack that exploited AWS cloud misconfigurations to upload files to the network.

API activity was detected that occurred without proper multi-factor authentication. One user 'BSTOLL' changed the access control list of s3 bucket 'frothlywebcode' which gave read and write permissions to that bucket to all users. Subsequently the file 'OPEN_BUCKET_PLEASE_FIX.txt' was uploaded to this bucket.

The scope of this investigation focuses specifically on AWS IAM misuse, S3 bucket misconfiguration and the exposure of sensitive systems.

Key Findings:
- Unauthenticated activity without multi-factor authentication.
- The S3 bucket 'frothlywebcode' was modified and publicly exposed.
- Possible unauthorised access and post-exploitation activity with the upload of "OPEN_BUCKET_PLEASE_FIX.txt".
- The workstation BSTOLL-L was identified as running a version of Windows that was not standard for the organisation.

While the BOTSv3 dataset contains evidence of broader network compromise, this report focuses specifically on failures within the AWS cloud environment that enabled system compromise.

SOC Roles

Security Operations Centre Context

Frothly's infrastructure spans on-premise Windows endpoints and AWS cloud services, requiring a SOC architecture that is capable of correlating events across environments. The SIEM deployment ingests CloudTrail logs for AWS API activity, S3 access logs for storage operations, and Windows host monitoring data for endpoint visibility. This capability was essential for reconstructing the incident in this report.

Tier 1 analysts act as the initial responders to any security alerts or potential threats to the network/organisation. Tier 1 analysts would be alerted to changes to the S3 bucket and would then be responsible for assessing the legitimacy of the threat, gathering evidence and analysing it. In this incident, the S3 configuration change and subsequent file upload would warrant immediate escalation rather than closure as a false positive.

Tier 2 analysts analyse security incidents in more depth than tier 1 analysts. The majority of work performed in this report mirrors the tier 2 role. This involves cross-correlating different log sources to rebuild a timeline of the attack and determining the extent of the attack and what data/systems have been affected.

Tier 3 analysts would develop new detection rules based on this incident and would continue to check for similar intrusions throughout the organisation. They would develop baselines of behaviour for normal IAM user activity, create specialised detection rules and implement automated detection and responses within the network.

Incident Handling

This details the lifecycle of the investigation into the incident and some recommended actions.

Detection and Analysis: Identified the mysterious file upload via CloudTrail anomaly.

Containment: Immediately revert the permissions on the S3 ACL bucket, suspend the B-STOLL account and isolate their endpoint.

Threat Eradication: Rotate all the credentials that could have been exposed, re-image the BSTOLL-L workstation with an up-to-date OS version.

Recovery: Deploy new AWS configuration rules to prevent buckets being made public in the future.schedule mandatory security awareness training.

The absence of MFA enforcement on AWS API calls represents a critical control gap that enabled this incident to progress beyond the severity it should have reached.

Threat Intelligence Correlation

The indicators identified in this investigation such as IAM username and S3 bucket name are internal artefacts rather than external threat indicators such as malicious IP addresses or file hashes. This reflects the nature of the incident: a cloud misconfiguration exploited to upload unauthorised content rather than a malware-based intrusion.

Traditional IOC-based threat intelligence correlation using platforms such as VirusTotal is limited for this type of incident. Expanding the investigation to include file content analysis and endpoint forensics on BSTOLL-L would be required to identify external threat indicators.

Several high traffic IPs were investigated on virustotal.com but none were flagged as suspicious.

Installation and Dataset Preparation

I installed an Ubuntu VM with an allocated 25GB on the VMware workstation. Splunk enterprise was downloaded onto my virtual machine through a terminal and the BOTSv3 dataset was downloaded from the GitHub repository and was extracted to a splunk folder.

I validated the installation of the dataset with the query "index=botsv3" and it indexed the correct number of events (2,030,269).

This deployment mirrors a simplified SOC SIEM architecture where multiple log sources need to be accessed from a centralised location for analysis. In a production environment, an Ubuntu host OS is used due to its stability and lower resource overhead compared to other operating systems.
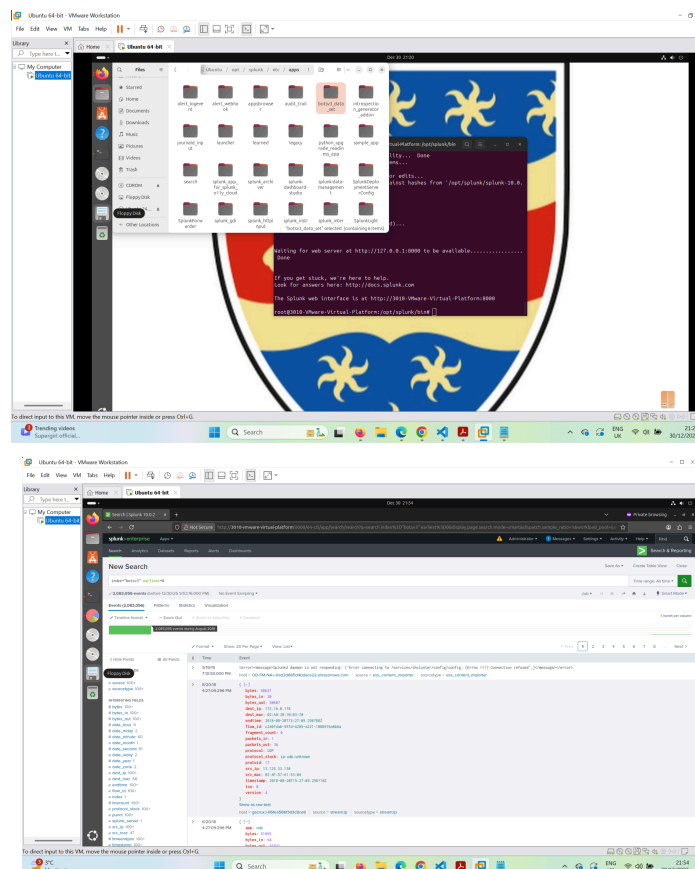
Investigation

Q1 - List out the IAM users that accessed an AWS service (successfully or unsuccessfully) in Frothly's AWS environment.

A - bstoll,btun,splunk_access,web_admin
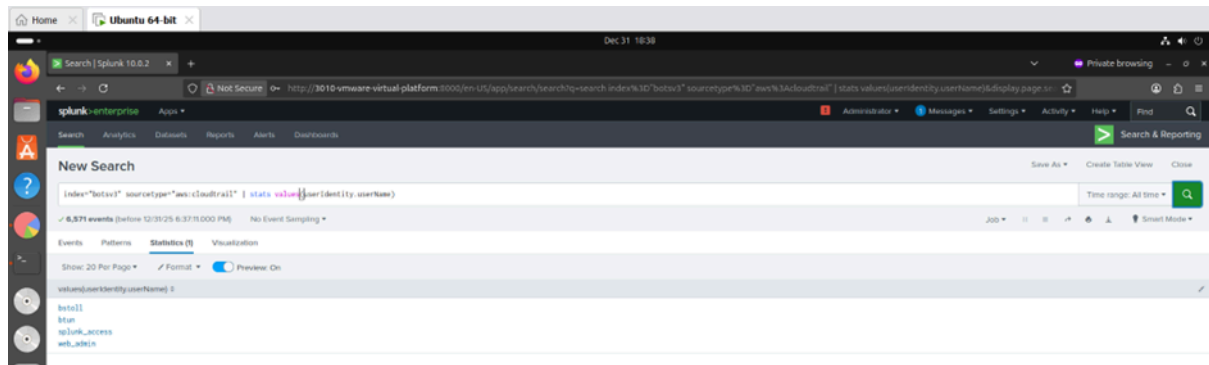
Establishing a baseline of active IAM users is a foundational step in any cloud security investigation. This inventory enables anomaly detection by identifying which accounts were active during the incident. The user BSTOLL was identified as a primary suspect later.

Q2 - What field would you use to alert that AWS API activity has occurred without MFA?

A - userIdentity.sessionContext.attributes.mfaAuthenticated

index=botsv3 sourcetype="aws:cloudtrail" *mfa* | fieldsummary | filter field="*mfa*"
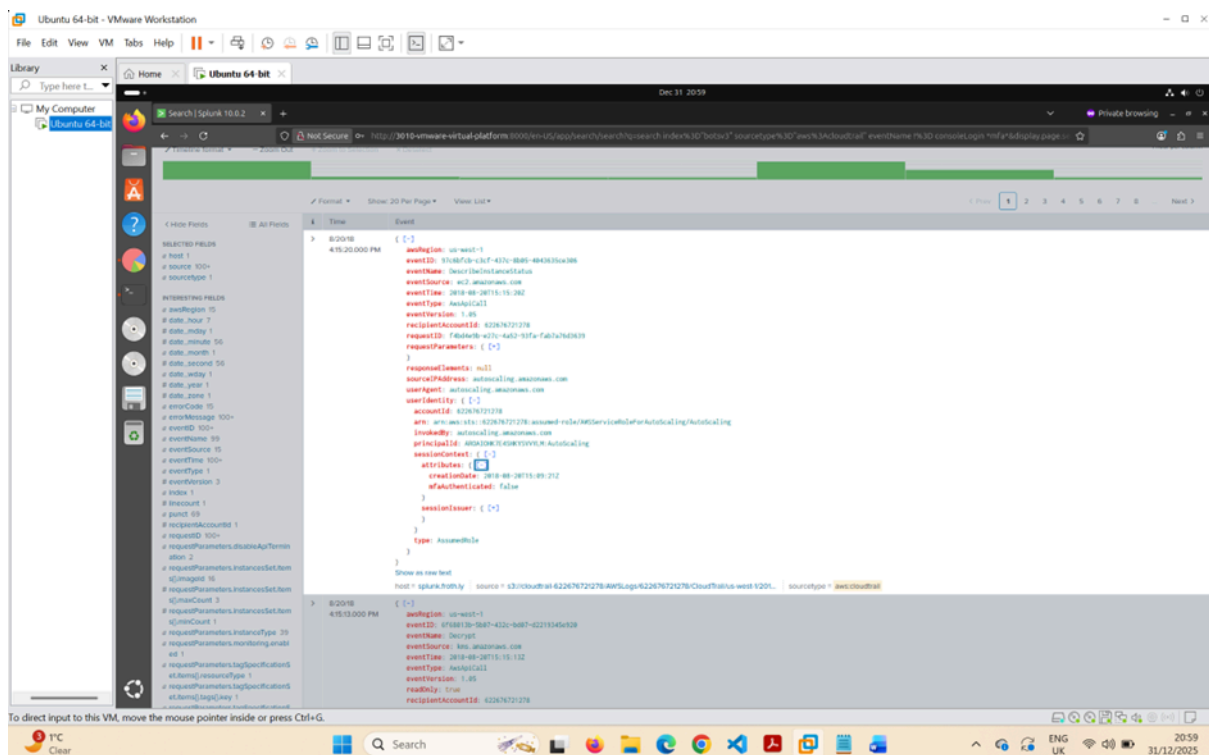
I then investigated activity that occurred within the aws environment that was not properly authenticated. Any activity that occurred without MFA represents a bypassing of an organization's primary method of network security. SOC teams should configure alerts on

this field to detect compromised sessions as all legitimate activity should have multi-factor authentication.

Q3 - What is the processor number used on the web servers?

A - E5–2676

I identified an Intel Xeon processor on the web servers, confirming legitimate AWS EC2 infrastructure. The confirmation of the processor type validates that the systems being investigated are legitimate EC2 instances instead of separate IT infrastructure from hostile groups.

Q4 - Bud accidentally makes an S3 bucket publicly accessible. What is the event ID of the API call that enabled public access?

A - ab45689d-69cd-41e7–8705–5350402cf7ac

This was a critical security event that enabled file upload later. This event granted complete unauthenticated internet access for the downloading and uploading of files to the network. SOC teams should implement real-time alerts for S3 ACL modifications. The event ID provides an identifier for future audit trails and can be correlated with user activity.

Q5 - What is Bud's username?

A - BSTOLL

The account with the username BSTOLL is the account responsible for making the bucket public. Determining the identity of this account is critical as they are either an insider or their account/credentials are compromised. The responsibility for determining this is held by the SOC and possibly directs their containment strategy.

Q6 - What is the name of the S3 bucket that was made publicly accessible?

A - frothlywebcode
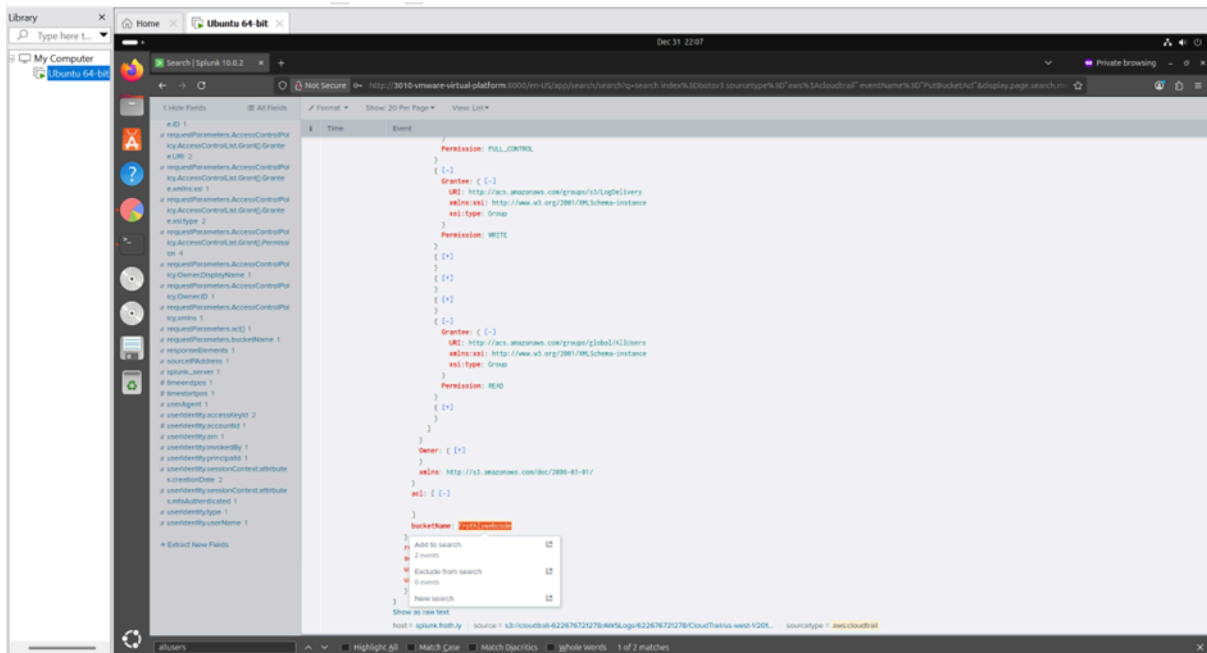
Bucket name suggests this could be the source code repository possibly containing a large number of high value targets for hostile . SOC analysts need to examine the data that resided in this bucket, the scope of the breach and their investigation.

Q7 - What is the name of the text file that was successfully uploaded into the S3 bucket while it was publicly accessible?

A - OPEN_BUCKET_PLEASE_FIX.txt
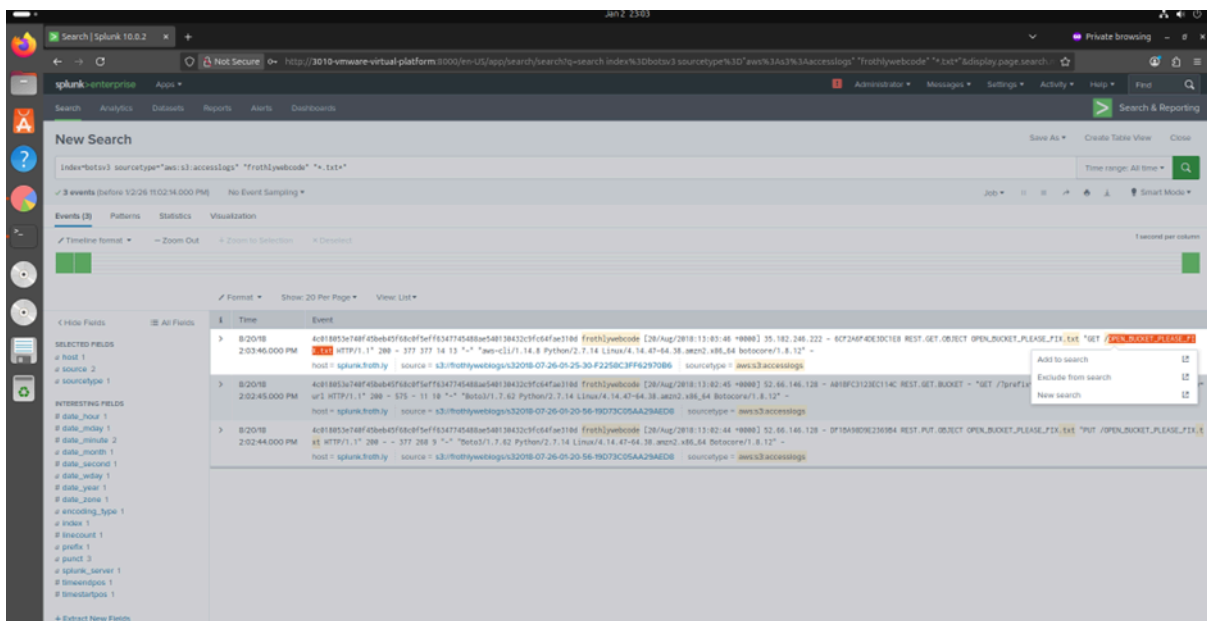
This confirms that unauthorised files were uploaded to the company network. The file is named OPEN_BUCKET_PLEASE_FIX.txt. The name may be a part of a social engineering attempt to cause any unsuspecting user into downloading it. This means it likely contained

malware. This requires the immediate rotation of all user credentials within the organisation to prevent any information gained from this attack from being used in future attacks.

Q8 - What is the FQDN of the endpoint that is running a different Windows operating system edition than the others?

A - bstoll-l.froth.ly
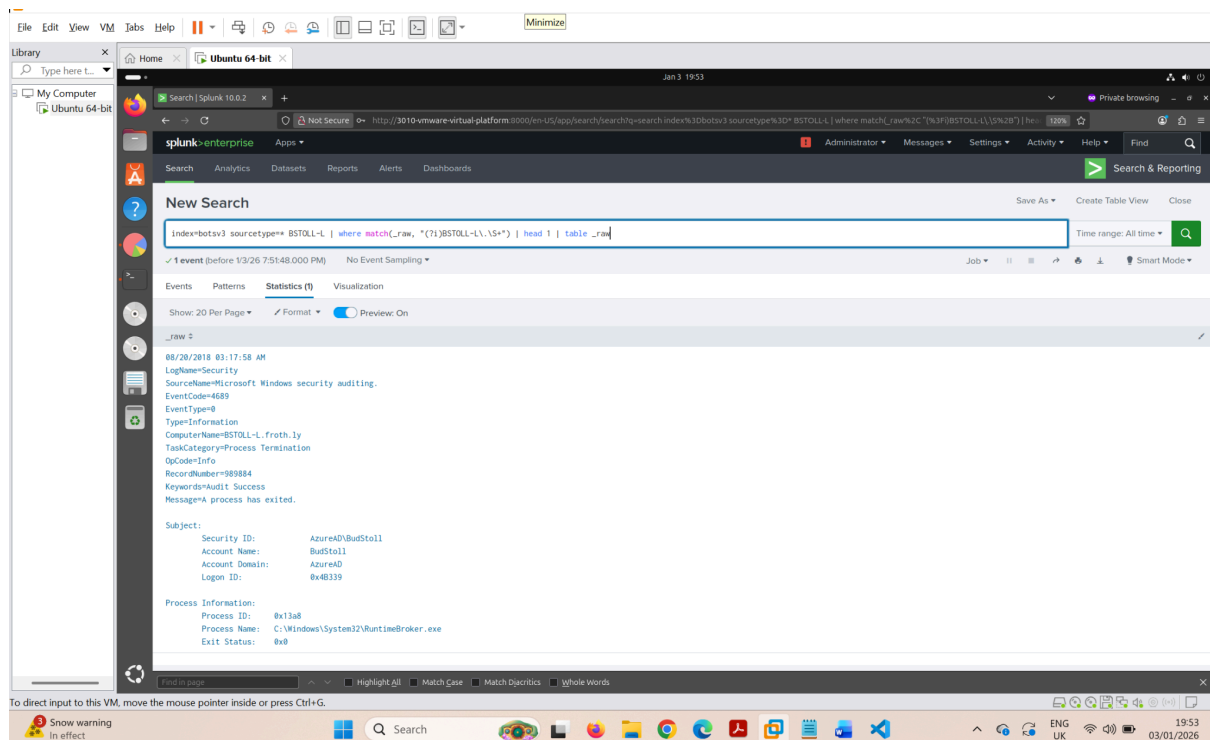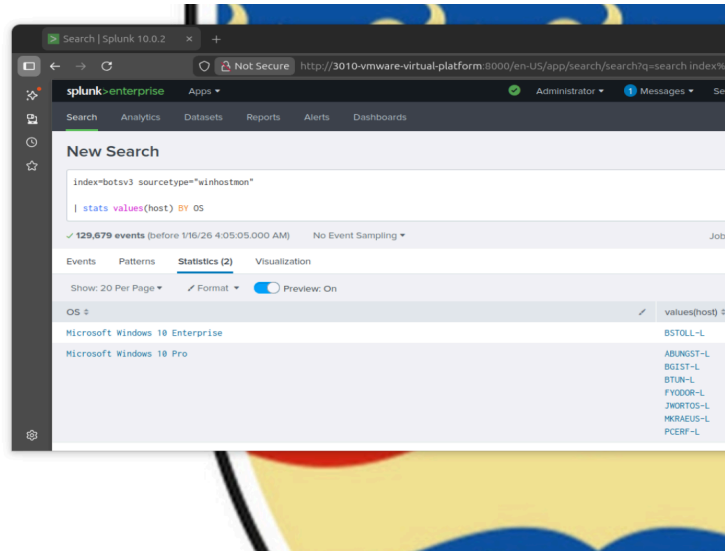
This demonstrates that the endpoint BSTOLL-L was running Windows 10 Enterprise which is an outlier compared to the other endpoints on the network which all run Windows 10 Pro. SOC teams need to investigate this anomaly to determine if this endpoint was the initial compromise vector.

Conclusions and Recommendations

This investigation of the BOTSv3 dataset revealed a cyber attack that exploited multiple security control failures, resulting in an S3 bucket being made publicly accessible and used to host unauthorised content. The endpoint configuration drift identified on BSTOLL-L represents an additional security concern requiring further investigation.

Recommendations

1. Deploy IAM policy that denies all API calls that are not made with multi-factor authentication.
2. Migrate all workstations to the latest Windows Enterprise version for advanced security features.
3. Rotate all credentials in the network
4. Ensure that all copies of "OPEN_BUCKET_PLEASE_FIX.txt" are removed from the network.
5. Re-image the BSTOLL-L endpoint.
6. Deploy CloudTrail alerting for PutBucketAcl events

Business Impact

Frothly is a small company with approximately 50 employees based in the UK and subject to UK regulations. This incident exposed the organisation to several risks: the publicly accessible bucket could have been used to host and distribute malicious content, creating potential legal liability; the compromise of the BSTOLL account indicates credential theft or insider misuse requiring investigation; and the underlying control failures (missing MFA enforcement, no bucket policy restrictions) leave the organisation vulnerable to future attacks.

Regulatory Impact

As a UK company, Frothly must comply with UK GDPR. While this incident did not directly expose customer data, the compromise of the BSTOLL account and potential access to internal systems may constitute a personal data breach if investigation reveals customer data was accessible. The organisation should assess:

Obligation	Requirement	Consequence of Failure

ICO notification	Within 72 hours of becoming aware	Fines up to £8.7 million or 2% of annual turnover
Customer notification	Without undue delay if high risk to individuals	Reputational damage, potential civil claims
Documentation	Record breach details regardless of notification	Regulatory non-compliance

Estimated Costs

Cost Category	Estimate	Reasoning
Credential rotation	£1,500 - £3,000	50 employees × 1-2 hours productivity loss during password resets; IT support time for locked accounts
Endpoint remediation	£500 - £1,000	Re-imaging BSTOLL-L workstation; IT labour and potential hardware costs
AWS security hardening	£2,000 - £5,000	Implementing Config rules, IAM policy updates; likely requires external AWS expertise
Security awareness training	£1,000 - £2,500	50 employees; either external provider or staff time to develop internal programme

Reflections

This incident demonstrates a series of cascading failures where missing preventive controls enabled the exposure of company infrastructure to external users. A defense-in-depth approach that utilised MFA, config rules and proper endpoint detection and response would have prevented this attack.

The investigation highlighted the value of centralised log correlation which connected CloudTrail API activity, S3 access logs and windows host monitoring which was essential for reconstructing the incident. SOC teams should ensure visibility across all infrastructure layers.