INCIDENT RESPONSE SIMULATIONS BASED ON 500+ USE CASES

BY IZZMIER IZZUDDIN

USE CASES BY GROUP

Access Management

- Access Outside Business Hours
- Shared Account Usage

Cloud Security

- Abnormal Cloud API Calls
- Abnormal Cloud Storage Sharing Behavior

Email Security

- Abnormal Email Reply Patterns
- Email Spoofing Detection

Network Anomalies

- Detection of Non-Standard Port Traffic Spikes
- Suspicious Outbound FTP Activity

Malware Detection

- Suspicious File Hash Matching Known Malware
- Malware Callback Detection

Threat Detection

- Suspicious PowerShell Command Execution (Will be in the book)
- Rogue Access Point Detection (Will be in the book)

Privilege Escalation

- Suspicious Scheduled Task Creation (Will be in the book)
- Elevated Privilege Token Usage (Will be in the book)

Data Security

- Suspicious File Replication to External Drives (Will be in the book)
- Abnormal File Deletion Patterns (Will be in the book)

Insider Threat

- Abuse of Group Policy Objects (GPO) (Will be in the book)
- Suspicious Activity in Cloud Billing Accounts (Will be in the book)

Incident Response

- Firewall Policy Change Detection (Will be in the book)
- Detection of Unauthorised Remote Access Tools (RATs) (Will be in the book)

Vulnerability Exploits

- Exploitation of a Known Vulnerability in Software (Will be in the book)
- Detection of Deprecated Protocol Usage (Will be in the book)

Lateral Movement

- SMB Lateral Movement Detection (Will be in the book)
- Lateral Movement in Cloud Environments (Will be in the book)

Compliance and Governance

- Time-Based Access Violations (Will be in the book)
- Security Policy Change Detection (Will be in the book)

User Behavior

- Abnormal Growth in Cloud Storage Usage (Will be in the book)
- Suspicious Commands Executed via Command Line (Will be in the book)

ACCESS MANAGEMENT

USE CASE 1: ACCESS OUTSIDE BUSINESS HOURS

Scenario Overview:

- **Client Name:** Manchester United
- **Date/Time of Incident:** December 3, 2024, 11:30 PM GMT
- **Alert Type:** Access Outside Business Hours
- **Detection Source:** SIEM (Splunk)
- **Affected Environment:** Corporate Active Directory (AD), HR Database

Step 1: Initial Alert Details

Splunk Alert Name: Unusual Access Time Detected

- **Trigger Condition:** User access during non-business hours (8:00 PM to 6:00 AM GMT)
- **Severity:** High
- **Impacted Systems:** HRDatabase01, ADServer03
- **Impacted Accounts:**
    - **tooney** (HR Manager)
    - **tevez** (System Admin)

Step 2: Gather Logs and Analyse

Event Logs (Windows Security Logs - Event ID 4624):

Date/Time	Server	User Account	Logon Type	Client Address
2024-12-03 11:12 PM	HRDatabase01	rooney	Interactive	192.168.10.150
2024-12-03 11:18 PM	ADServer03	tevez	RemoteInteractive	192.168.10.151

Firewall Logs:

Date/Time	SourceIP	Destination	Protocol	Action
2024-12-03 11:10 PM	192.168.10.150	HRDatabase01	HTTPS	Allowed
2024-12-03 11:16 PM	192.168.10.151	ADServer03	RDP	Allowed

Step 3: Analyse Findings

1. **Suspicious Behavior Identified:**
    - Logins from privileged accounts (HR Manager and System Admin) during non-business hours.
    - Access to sensitive systems (HR Database and AD server).
    - Remote access from client IPs, raising concerns about unauthorised remote activity.
2. **Correlations:**
    - Log analysis reveals that both accounts accessed systems outside normal working hours without prior authorisation.
    - Client IPs (192.168.10.x) belong to internal subnets but need verification against expected device usage patterns.

Step 4: Mitigation Actions

1. **Immediate Response:**
    - Temporarily disable user accounts (rooney and tevez) to prevent further access.
    - Block suspicious client IPs (192.168.10.150 and 192.168.10.151) at the firewall.
2. **Notification:**
    - Notify the Incident Response Team (IRT) for further investigation.
    - Inform impacted users and request them to verify the activity.

Step 5: Follow-Up Investigation

1. **Threat Hunt:**
    - Review account activity over the past 7 days for anomalies (e.g., multiple failed login attempts or unusual access patterns).
    - Check for potential credential compromise by scanning internal threat intelligence feeds.
2. **Validate Business Context:**
    - Confirm whether the access during non-business hours was authorised (e.g., emergency maintenance tasks).
    - Verify the devices associated with the client IPs against an internal asset inventory.
3. **Policy Review:**
    - Enforce stricter access control policies for privileged accounts, including MFA and explicit time-based restrictions.

Questions & Answers for Analyst Training

Q1: What should you check first when investigating access outside business hours?

- Begin by validating the user account activity logs, checking if the logins are legitimate or unauthorised. Also, confirm the business need for access during non-working hours.

Q2: How can you detect if the user credentials are compromised?

- Analyse the user's login history for abnormal behavior, correlate the activity with external threat intelligence (e.g., breach databases), and look for matching Indicators of Compromise (IOCs).

Q3: What proactive measures can you implement to prevent this in the future?

- Apply time-based access restrictions for sensitive accounts.
- Mandate the use of MFA for privileged accounts.
- Implement alerting for login attempts outside normal working hours.

Additional Monitoring Rules for Detection

1. **Rule 1:** Detect logins from privileged accounts outside defined working hours.
2. **Rule 2:** Correlate login events with geolocation data and trigger alerts for unusual locations.
3. **Rule 3:** Monitor for repeated failed login attempts followed by successful logins during odd hours.

USE CASE 2: SHARED ACCOUNT USAGE

Scenario Overview

- **Client Name:** Manchester United
- **Date/Time of Incident:** December 3, 2024, 03:15 PM GMT
- **Alert Type:** Shared Account Usage
- **Detection Source:** SIEM (Splunk)
- **Affected Environment:** Corporate Active Directory (AD), Finance Database

Step 1: Initial Alert Details

Splunk Alert Name: Potential Shared Account Usage Detected

- **Trigger Condition:** Login activity from the same account originating from different IPs within 10 minutes.
- **Severity:** High
- **Impacted Systems:** FinanceDB01, ADServer02
- **Impacted Account: finance.team**

Step 2: Gather Logs and Analyse

Event Logs (Windows Security Logs - Event ID 4624):

Date/Time	Server	User Account	Logon Type	Client Address
2024-12-03 03:05 PM	FinanceDB01	finance.team	RemoteInteractive	192.168.60.100
2024-12-03 03:07 PM	FinanceDB01	finance.team	RemoteInteractive	192.168.60.101
2024-12-03 03:10 PM	ADServer02	finance.team	RemoteInteractive	192.168.60.102

Firewall Logs:

Date/Time	SourceIP	Destination	Protocol	Action
2024-12-03 03:04 PM	192.168.60.100	FinanceDB01	HTTPS	Allowed
2024-12-03 03:06 PM	192.168.60.101	FinanceDB01	HTTPS	Allowed
2024-12-03 03:09 PM	192.168.60.102	ADServer02	RDP	Allowed

Step 3: Analyse Findings

1. **Suspicious Behavior Identified:**
    - Same shared account (**finance.team**) logged in from different IP addresses within a short timeframe.
    - Unusual pattern for shared account activity that typically remains confined to one system.
2. **Correlations:**
    - Multiple logins occurred from distinct IPs, suggesting simultaneous use of shared credentials.
    - Unusual system access (Finance Database and AD Server) for the same account at overlapping times.

Step 4: Mitigation Actions

1. **Immediate Response:**
    - Disable the **finance.team** shared account to prevent further access.
    - Block the suspicious IPs (192.168.60.100, 192.168.60.101, 192.168.60.102) temporarily at the firewall.
2. **Notification:**
    - Notify the Finance Team and escalate to the Incident Response Team (IRT).
    - Inform relevant stakeholders, requesting input to validate authorised use of the shared account.

Step 5: Follow-Up Investigation

1. **Validate Shared Account Usage Policy:**
    - Check if shared account use aligns with organisational policy. If not, mandate the use of individual accounts for accountability.
2. **Check for Potential Credential Compromise:**
    - Cross-reference IPs with historical logs to check if they were associated with legitimate users.
    - Use breach databases and internal threat intelligence feeds to see if the shared account credentials were exposed.
3. **Audit Access to Sensitive Systems:**
    - Analyse what actions were performed using the **finance.team** account on the Finance Database and AD Server.
    - Check for data exfiltration attempts, unauthorised file access, or privilege escalations.

Questions & Answers for Analyst Training

Q1: Why is shared account usage a security risk?

- Shared accounts lack accountability since multiple users can access them, making it challenging to attribute actions to specific individuals. They are also prone to unauthorised access if credentials are leaked.

Q2: How can you enforce better control over shared accounts?

- Implement strict policies against shared account use, enforce multi-factor authentication (MFA), and assign individual user accounts with specific roles and permissions.

Q3: What additional SIEM rules would you configure to monitor shared account activity?

- Set alerts for simultaneous logins from different IPs or locations.
- Monitor for unusual access times and activity for shared accounts.

- Configure rules to detect access to multiple systems within a short time using the same credentials.

Additional Monitoring Rules for Detection

1. **Rule 1:** Alert on concurrent logins for the same account from different IPs.
2. **Rule 2:** Trigger alerts for shared account access outside business hours or from unusual locations.
3. **Rule 3:** Correlate shared account logins with sensitive systems (e.g., finance databases or AD servers) and alert on anomalies.

Cloud Security

USE CASE 3: ABNORMAL CLOUD API CALLS

Scenario Overview

- **Client Name:** Manchester United
- **Date/Time of Incident:** December 3, 2024, 04:30 PM GMT
- **Alert Type:** Abnormal Cloud API Calls
- **Detection Source:** SIEM (Splunk integrated with CloudTrail)
- **Affected Environment:** AWS Cloud Infrastructure

Step 1: Initial Alert Details

Splunk Alert Name: Unusual Cloud API Activity Detected

- **Trigger Condition:** Sudden surge in API calls from a single source IP exceeding a predefined threshold within a short timeframe.
- **Severity:** High
- **Impacted Systems:**
    - S3 Bucket: manu-sensitive-data
    - IAM: Unauthorised access attempts detected.
- **Impacted User:** automation.service

Step 2: Gather Logs and Analyse

CloudTrail Logs:

Date/Time	SourceIP	User	API Call	Status
2024-12-03 04:10 PM	203.0.113.50	automation.service	ListBuckets	Success
2024-12-03 04:11 PM	203.0.113.50	automation.service	GetBucketPolicy	Success
2024-12-03 04:12 PM	203.0.113.50	automation.service	PutBucketPolicy	Success
2024-12-03 04:15 PM	203.0.113.50	automation.service	CreateAccessKey	Success

2024-12-03 04:18 PM	203.0.113.50	automation.service	DeleteBucket	Denied

Firewall Logs:

Date/Time	SourceIP	Destination	Protocol	Action
2024-12-03 04:09 PM	203.0.113.50	AWS API Gateway	HTTPS	Allowed

Step 3: Analyse Findings

1. **Suspicious Behavior Identified:**
    - Abnormal surge of API calls from a single IP (203.0.113.50) associated with a service account (automation.service).
    - Potential misuse of privileges or a compromised service account trying to modify S3 bucket policies and create access keys.
2. **Correlations:**
    - The source IP is not a trusted corporate IP.
    - API calls attempted to alter security policies (PutBucketPolicy, CreateAccessKey), indicating possible malicious intent.

Step 4: Mitigation Actions

1. **Immediate Response:**
    - Revoke the automation.service IAM user's access and rotate its credentials.
    - Block the source IP (203.0.113.50) in the AWS Web Application Firewall (WAF).
    - Audit S3 bucket policies and IAM roles for unauthorised changes.
2. **Notification:**
    - Notify the cloud operations and security teams.
    - Escalate the incident to the Incident Response Team (IRT).

Step 5: Follow-Up Investigation

1. **Validate Incident Impact:**
    - Confirm if any S3 data was accessed, modified, or exfiltrated.
    - Review CloudTrail logs for other suspicious activity from the same IP or user.
2. **Identify Root Cause:**
    - Investigate how the service account credentials might have been compromised.
    - Check if the credentials were exposed (e.g., hardcoded in scripts or leaked in public repositories).
3. **Enhance Cloud Security Measures:**
    - Enforce strict least privilege policies for all IAM users and roles.
    - Enable multi-factor authentication (MFA) for service accounts wherever possible.
    - Deploy anomaly detection rules for unusual API activity using AWS GuardDuty.

Questions & Answers for Analyst Training

Q1: What are common signs of compromised API credentials?

- Unusual API calls from untrusted IPs or regions.
- Sudden spikes in API usage.
- API calls attempting to modify security settings or access sensitive data.

Q2: How can you prevent API abuse in cloud environments?

- Use IAM policies with the principle of least privilege.
- Rotate and monitor API keys regularly.
- Implement tools like AWS GuardDuty and CloudTrail to monitor and alert on unusual behavior.

Q3: What additional logging and monitoring configurations would help detect such incidents?

- Enable AWS Config to track changes in resource configurations.

- Use CloudWatch to set alarms for API call thresholds.
- Monitor for unusual geographical locations in CloudTrail logs for API requests.

Additional Monitoring Rules for Detection

1. **Rule 1:** Set alerts for sudden spikes in API call rates by any user or IP.
2. **Rule 2:** Monitor API calls that attempt to modify security policies, IAM roles, or S3 bucket settings.
3. **Rule 3:** Detect access attempts to sensitive resources like S3 buckets or databases from untrusted IPs or regions.

USE CASE 4: ABNORMAL CLOUD STORAGE SHARING BEHAVIOR

Scenario Overview

- **Client Name:** Manchester United
- **Date/Time of Incident:** December 3, 2024, 11:15 AM GMT
- **Alert Type:** Abnormal Cloud Storage Sharing Behavior
- **Detection Source:** SIEM (Splunk integrated with Google Workspace/AWS S3)
- **Affected Environment:** Cloud Storage Platforms (Google Drive & AWS S3)

Step 1: Initial Alert Details

Splunk Alert Name: Unusual Cloud File Sharing Detected

- **Trigger Condition:** Sudden increase in external sharing of files from corporate cloud storage.
- **Severity:** High
- **Impacted Systems:**
    - Google Drive Folder: Sensitive Financial Data
    - S3 Bucket: manu-critical-docs
- **Impacted User:** finance.manager

Step 2: Gather Logs and Analyse

Google Drive Logs:

Date/Time	User	Action	File	Recipient	IP Address
2024-12-03 11:02 AM	finance.manager	Shared	Budget2024.xlsx	external@example.com	203.0.113.80

2024-12-03 11:05 AM	finance.manager	Shared	ExecutiveSummary.pdf	external@example.com	203.0.113.80
2024-12-03 11:10 AM	finance.manager	Shared	Q1_Profit_Margins.docx	external@example.com	203.0.113.80

AWS S3 Access Logs:

Date/Time	User	Action	Bucket	File	IP Address
2024-12-03 11:12 AM	finance.manager	PutObjectAcl	manu-critical-docs	projections2025.csv	203.0.113.80
2024-12-03 11:13 AM	finance.manager	PutObjectAcl	manu-critical-docs	salaries2023.csv	203.0.113.80

Step 3: Analyse Findings

1. **Suspicious Behavior Identified:**
    - Rapid external sharing of sensitive financial files from Google Drive.
    - Changes to S3 object ACLs granting public access to critical files.
    - All activities originate from a single external IP (203.0.113.80).
2. **Correlations:**
    - Activities involve high-value files containing sensitive data.
    - IP address 203.0.113.80 is not a recognised corporate IP.
    - Sudden surge in sharing behavior is highly unusual for the user finance.manager.

Step 4: Mitigation Actions

1. **Immediate Response:**

- Revoke the finance.manager account's permissions in Google Workspace and AWS S3.
- Change access controls for affected files and revoke external sharing links.
- Block external IP 203.0.113.80 at the firewall and cloud security gateways.

2. **Notification:**
   - Notify the cloud security and IT teams immediately.
   - Inform impacted stakeholders (finance team) and enforce a temporary data-sharing freeze for financial files.

Step 5: Follow-Up Investigation

1. **Identify Root Cause:**
   - Investigate if the user's credentials were compromised or if insider threat behavior occurred.
   - Review access logs for anomalous login patterns, such as logins from unusual locations or devices.
2. **Audit Cloud Security Configuration:**
   - Check if appropriate Data Loss Prevention (DLP) rules are in place for sensitive files.
   - Validate sharing settings and permissions on Google Drive folders and AWS S3 buckets.
3. **Long-Term Security Enhancements:**
   - Implement strict sharing controls, such as limiting external sharing to specific domains or IPs.
   - Use automated alerts for changes to S3 bucket policies or sharing settings.
   - Enable Multi-Factor Authentication (MFA) for all users handling sensitive data.

Questions & Answers for Analyst Training

Q1: What are the risks of improper cloud storage sharing behavior?

- Unauthorised access to sensitive information.
- Potential regulatory violations due to data exposure.
- Increased likelihood of data exfiltration by malicious actors.

Q2: How can you detect abnormal sharing activity in cloud environments?

- Monitor for sudden surges in sharing actions.
- Detect changes in file permissions or ACLs.
- Use SIEM integrations to analyse logs from cloud platforms.

Q3: What preventive measures can be implemented to secure cloud storage?

- Enforce least privilege access policies.
- Restrict sharing permissions and disable public sharing by default.
- Use tools like Cloud Security Posture Management (CSPM) to enforce compliance policies.

Additional Monitoring Rules for Detection

1. **Rule 1:** Set alerts for file-sharing actions targeting external domains or public access links.
2. **Rule 2:** Monitor changes to S3 bucket ACLs and permissions.
3. **Rule 3:** Detect file access or sharing surges originating from untrusted IPs.

EMAIL SECURITY

USE CASE 5: ABNORMAL EMAIL REPLY PATTERNS

Scenario Overview

- **Client Name:** Manchester United
- **Date/Time of Incident:** December 3, 2024, 2:45 PM GMT
- **Alert Type:** Abnormal Email Reply Patterns
- **Detection Source:** Email Security Gateway integrated with SIEM (Splunk)
- **Affected Environment:** Corporate Email System (Microsoft 365)

Step 1: Initial Alert Details

Splunk Alert Name: Unusual Email Reply Patterns Detected

- **Trigger Condition:**
    - Replying to multiple external domains within a short time frame.
    - Replies to flagged domains associated with phishing campaigns.
- **Severity:** High
- **Impacted Accounts:**
    - marketing.manager@manutd.com
    - finance.officer@manutd.com

Step 2: Gather Logs and Analyse

Email Logs from Security Gateway:

Date/ Time	User	Action	Recipient	Subject	Flagged Domain	IP Address

2024-12-03 2:30 PM	marketing.manager@manutd.com	Replied	invoice@unknowncompany.xyz	Re: Urgent Payment Inquiry	Yes	198.51.100.25
2024-12-03 2:33 PM	finance.officer@manutd.com	Replied	billing@scamvendor.co	Re: Pending Invoice Approval	Yes	203.0.113.10
2024-12-03 2:35 PM	marketing.manager@manutd.com	Replied	events@fakeevent.com	Re: Invitation Confirmation	Yes	198.51.100.25

Attachment Analysis:

- **Attachment Name:** Invoice1234.pdf
    - **Result:** Identified as malicious (contains embedded macro for credential theft).

Email Metadata:

- **Reply Patterns:**
    - 5 external replies in under 10 minutes.
    - Domains flagged in threat intelligence feeds for phishing or malware.

Step 3: Analyse Findings

1. **Suspicious Behavior Identified:**
    - Employees replying to phishing emails originating from flagged domains.
    - Replies to emails containing malicious attachments and urgent financial topics.
    - Rapid email activity consistent with compromised accounts or automated replies.

2. **Correlations:**
    - Threat intelligence indicates flagged domains are associated with known phishing campaigns.
    - Analysis of attachments shows malicious intent to steal credentials or install malware.

Step 4: Mitigation Actions

1. **Immediate Response:**
    - Temporarily disable affected accounts (marketing.manager, finance.officer).
    - Quarantine all emails from flagged domains and block these domains at the email gateway.
    - Isolate devices associated with compromised accounts to prevent further damage.
2. **Notification:**
    - Notify the IT team and escalate to the Incident Response Team (IRT).
    - Inform affected employees and guide them on secure email handling practices.

Step 5: Follow-Up Investigation

1. **Verify Account Compromise:**
    - Check for unauthorised login attempts or unusual IP addresses in account login logs.
    - Review MFA logs to ensure no bypass occurred.
2. **Conduct Threat Hunt:**
    - Search SIEM for similar email patterns from other corporate accounts.
    - Analyse threat intelligence feeds for additional domains related to the flagged ones.
3. **Enhance Email Security Policies:**

- Strengthen email filtering rules to block flagged domains and detect suspicious subjects (e.g., "Urgent Payment").
- Enforce attachment scanning for all incoming emails.

Questions & Answers for Analyst Training

Q1: What makes abnormal email reply patterns suspicious?

- High frequency of replies to flagged domains in a short timeframe.
- Responses to emails with malicious attachments or phishing links.
- Patterns inconsistent with typical user behavior, such as replying to multiple unknown recipients.

Q2: How can you detect compromised email accounts?

- Monitor for logins from unusual locations or IPs.
- Detect rapid email activity, such as mass replies or forwarding.
- Look for changes to account settings, such as email forwarding rules to external addresses.

Q3: What are some preventive measures for email-based threats?

- Enforce Multi-Factor Authentication (MFA) for all email accounts.
- Use advanced email filtering tools integrated with threat intelligence.
- Train employees to recognise phishing attempts and report suspicious emails.

Additional Monitoring Rules for Detection

1. **Rule 1:** Set alerts for multiple replies to flagged domains within a short timeframe.
2. **Rule 2:** Monitor email activity for attachments with high-risk indicators (e.g., macros).
3. **Rule 3:** Trigger alerts for replies to unusual recipients or sudden changes in email volume.

USE CASE 6: EMAIL SPOOFING DETECTION

Scenario Overview

- **Client Name:** Manchester United
- **Date/Time of Incident:** December 3, 2024, 10:30 AM GMT
- **Alert Type:** Email Spoofing Attempt Detected
- **Detection Source:** Email Security Gateway integrated with SIEM (Splunk)
- **Affected Environment:** Corporate Email System (Microsoft 365)

Step 1: Initial Alert Details

Splunk Alert Name: Potential Email Spoofing Detected

- **Trigger Condition:**
    - Received emails where the sender's domain matches the organisation's domain but originates from external sources.
- **Severity:** High
- **Impacted Recipients:**
    - ceo.office@manutd.com
    - it.support@manutd.com

Step 2: Gather Logs and Analyse

Email Logs from Security Gateway:

Date/Time	Recipient	Sender	Source IP	Subject	SPF/DKIM/DMARC Status
2024-12-03 10:15 AM	ceo.office@manutd.com	ceo@manutd.com	185.100.85.45	Re: Confidential Payment	SPF Fail, DKIM Fail, DMARC Fail

2024-12-03 10:18 AM	it.support@manutd.com	helpdesk@manutd.com	185.100.85.45	Urgent: Password Reset	SPF Fail, DKIM Fail, DMARC Fail

Header Analysis:

- **Sender IP (185.100.85.45):** Not part of the authorised senders list in the SPF record for manutd.com.
- **DKIM Signature:** Missing, indicating the email did not pass DKIM verification.
- **DMARC Policy:** Reject, but the spoofed emails bypassed some filters.

Attachment and Link Analysis:

- **Attachment Name:** PaymentDetails.docx
    - **Result:** Contains macro for executing PowerShell scripts.
- **Embedded Link:** http://fake-manutd-login.com
    - **Result:** Phishing site mimicking Microsoft 365 login page.

Step 3: Analyse Findings

1. **Suspicious Behavior Identified:**
    - Spoofed emails impersonating high-profile internal senders (e.g., CEO, IT helpdesk).
    - Emails failed SPF, DKIM, and DMARC checks.
    - Contained phishing links and malicious attachments.
2. **Correlations:**
    - Sender IP is associated with a known malicious server from threat intelligence feeds.
    - Phishing site URL is flagged in multiple security databases.

Step 4: Mitigation Actions

1. **Immediate Response:**

- Quarantine the spoofed emails and block the sender IP (185.100.85.45) at the email gateway.
- Notify employees about the spoofing attempt and advise them not to interact with similar emails.

2. **Enhanced Email Security Measures:**
   - Review and tighten SPF, DKIM, and DMARC configurations to ensure strict enforcement.
   - Update email filtering rules to block unauthorised senders impersonating internal domains.
3. **Notification:**
   - Notify the Incident Response Team (IRT) to investigate the source of the spoofing attempt.
   - Inform senior leadership and impacted employees.

Step 5: Follow-Up Investigation

1. **Threat Hunt:**
   - Search for similar spoofing attempts in SIEM logs to identify potential patterns.
   - Review historical logs for any previous emails from the spoofing server IP.
2. **Validate Security Posture:**
   - Test SPF, DKIM, and DMARC records using tools like MXToolbox.
   - Conduct simulated phishing exercises to measure employee awareness.
3. **Threat Intelligence Integration:**
   - Add the flagged IP (185.100.85.45) and phishing domain to threat intelligence feeds for proactive blocking.

Questions & Answers for Analyst Training

Q1: What is the role of SPF, DKIM, and DMARC in email security?

- **SPF (Sender Policy Framework):** Verifies the sender's IP address is authorised to send on behalf of the domain.
- **DKIM (DomainKeys Identified Mail):** Ensures the email content has not been tampered with during transit.
- **DMARC (Domain-based Message Authentication, Reporting, and Conformance):** Combines SPF and DKIM to prevent spoofing and provides instructions for handling failed emails.

Q2: How can you detect spoofed emails without SPF, DKIM, and DMARC?

- Analyse email headers for inconsistencies, such as mismatched sender and source IP.
- Look for suspicious subject lines, attachments, or links.
- Correlate sender IPs and domains with threat intelligence feeds.

Q3: How do phishing sites mimic legitimate login pages?

- They use similar domain names (e.g., typo-squatting or homoglyph attacks).
- Clone the appearance and layout of legitimate login pages to trick users into entering credentials.

Additional Monitoring Rules for Detection

1. **Rule 1:** Set alerts for emails failing SPF, DKIM, and DMARC checks from internal domains.
2. **Rule 2:** Monitor email attachments and links flagged as malicious in threat intelligence feeds.
3. **Rule 3:** Trigger alerts for emails with high-profile sender names originating from unauthorised sources.

NETWORK ANOMALIES

USE CASE 7: DETECTION OF NON-STANDARD PORT TRAFFIC SPIKES

Scenario Overview

- **Client Name:** Manchester United
- **Date/Time of Incident:** December 3, 2024, 11:15 AM GMT
- **Alert Type:** Unusual Traffic Spike on Non-Standard Ports
- **Detection Source:** SIEM (Splunk) integrated with Network IDS/IPS
- **Affected Environment:** Corporate Network

Step 1: Initial Alert Details

Splunk Alert Name: Non-Standard Port Traffic Detected

- **Trigger Condition:** Traffic volume on uncommon ports (e.g., 8088, 44555) exceeding 500MB within 10 minutes.
- **Severity:** High
- **Impacted Systems:**
    - Server01
    - Workstation05
- **Impacted Ports:**
    - Port 8088 (Custom Application)
    - Port 44555 (Unknown Service)

Step 2: Gather Logs and Analyse

Firewall Logs:

Date/Time	Source IP	Destination IP	Port	Protocol	Data Transferred

2024-12-03 11:05 AM	192.168.1.15	45.67.89.100	8088	TCP	300MB
2024-12-03 11:07 AM	192.168.1.25	123.45.67.89	44555	UDP	250MB
2024-12-03 11:10 AM	192.168.1.15	45.67.89.100	8088	TCP	210MB

IDS/IPS Logs:

- **Rule Triggered:** Potential Data Exfiltration via Non-Standard Ports.
- **Suspicious Behavior Identified:** High-volume data transfer over non-standard ports to external IPs.

NetFlow Logs:

Source IP	Destination IP	Port	Bytes Sent	Bytes Received
192.168.1.15	45.67.89.100	8088	300,000,000	0
192.168.1.25	123.45.67.89	44555	250,000,000	10,000

Traffic Inspection:

- **Port 8088 Data Analysis:** Custom application protocol transmitting large encrypted payloads.
- **Port 44555 Data Analysis:** UDP traffic with obfuscated payloads resembling beacon activity.

Step 3: Analyse Findings

1. **Suspicious Behavior Identified:**
    - Sudden and unusual spike in data volume on ports typically not used for business operations.
    - Traffic directed to external IPs not recognised as trusted destinations.
    - UDP traffic on Port 44555 indicates potential Command-and-Control (C2) communication.
2. **Correlations:**

- Traffic pattern aligns with potential data exfiltration or malware activity.
- Destination IPs flagged in threat intelligence feeds as associated with malicious activities.

Step 4: Mitigation Actions

1. **Immediate Response:**
    - Block traffic to external IPs 45.67.89.100 and 123.45.67.89 at the firewall.
    - Isolate the impacted devices (Server01 and Workstation05) from the network for investigation.
2. **Notification:**
    - Notify the IT and Incident Response Teams (IRT) of potential exfiltration or C2 activity.
    - Inform senior management of the situation and current mitigation efforts.
3. **Threat Containment:**
    - Disable non-essential services on ports 8088 and 44555 until root cause analysis is complete.
    - Implement rules in the IDS/IPS to block traffic on these ports temporarily.

Step 5: Follow-Up Investigation

1. **Threat Hunt:**
    - Review historical logs to identify any prior activity on the same ports.
    - Search for Indicators of Compromise (IOCs) such as associated IPs, unusual traffic patterns, or payload hashes.
2. **Endpoint Analysis:**
    - Scan impacted devices for malware using forensic tools (e.g., Volatility, Wireshark).
    - Examine running processes and network connections for anomalies.
3. **Validation of External IPs:**

- Validate external IPs against updated threat intelligence feeds to confirm malicious intent.

4. **Remediation:**
    - Patch any identified vulnerabilities in the custom application using Port 8088.
    - Review and update firewall and IDS/IPS configurations to prevent unauthorised use of non-standard ports.

Questions & Answers for Analyst Training

Q1: What are non-standard ports, and why are they used in attacks?

- **Non-standard ports** are ports not commonly used for well-known services (e.g., HTTP on 80, HTTPS on 443). Attackers use them to avoid detection by security tools configured to monitor standard ports.

Q2: How can you detect potential Command-and-Control (C2) activity?

- Monitor for unusual traffic patterns such as regular beaconing, large data transfers, or communication with known malicious IPs/domains.

Q3: What is the role of NetFlow data in investigating such incidents?

- **NetFlow data** provides details on source/destination IPs, ports, and traffic volumes, enabling analysts to identify anomalies and suspicious connections.

Additional Monitoring Rules for Detection

1. **Rule 1:** Set up alerts for unexpected traffic spikes on non-standard ports.
2. **Rule 2:** Monitor for outbound traffic to IPs flagged in threat intelligence feeds.
3. **Rule 3:** Correlate non-standard port traffic with unusual process activity on endpoints.

USE CASE 8: SUSPICIOUS OUTBOUND FTP ACTIVITY

Scenario Overview

- **Client Name:** Manchester United
- **Date/Time of Incident:** December 3, 2024, 2:30 PM GMT
- **Alert Type:** Suspicious Outbound FTP Activity
- **Detection Source:** SIEM (Splunk) and Firewall Logs
- **Affected Environment:** Corporate Network

Step 1: Initial Alert Details

Splunk Alert Name: Unusual Outbound FTP Traffic Detected

- **Trigger Condition:** Outbound FTP connection with data transfer exceeding 500MB in 10 minutes.
- **Severity:** High
- **Impacted Systems:**
    - FinanceServer01
- **Impacted Protocol:**
    - FTP (Port 21)

Step 2: Gather Logs and Analyse

Firewall Logs:

Date/Time	Source IP	Destination IP	Port	Protocol	Data Transferred
2024-12-03 2:15 PM	192.168.2.20	203.0.113.45	21	FTP	300MB
2024-12-03 2:17 PM	192.168.2.20	203.0.113.45	21	FTP	250MB

FTP Server Logs:

Date/Time	Username	Command	File Transferred	Size
2024-12-03 2:15 PM	finance_user	STOR	Payroll_Records_Q4_2024.zip	300MB
2024-12-03 2:17 PM	finance_user	STOR	Employee_Data_2024.zip	250MB

NetFlow Logs:

Source IP	Destination IP	Port	Bytes Sent	Bytes Received
192.168.2.20	203.0.113.45	21	550,000,000	1,000

Step 3: Analyse Findings

1. **Suspicious Behavior Identified:**
    - High-volume outbound FTP traffic from a finance server.
    - Transferred files contain sensitive information (e.g., payroll and employee data).
    - External destination IP (203.0.113.45) not recognised as a legitimate business partner.
2. **Correlations:**
    - Logs confirm the data transfer is from a legitimate user account (finance_user).
    - No prior outbound FTP connections from FinanceServer01 detected in historical logs.
3. **Potential Risks:**
    - Data exfiltration by an insider or compromised account.
    - External IP associated with malicious activity in threat intelligence feeds.

Step 4: Mitigation Actions

1. **Immediate Response:**
    - Block external IP 203.0.113.45 at the firewall to stop further data transfer.
    - Disable the finance_user account temporarily to prevent unauthorised actions.
    - Isolate FinanceServer01 from the network for forensic analysis.
2. **Notification:**
    - Notify the Incident Response Team (IRT) and escalate the incident as potential data exfiltration.
    - Inform senior management and the legal team about possible data theft.
3. **Containment:**
    - Review and revoke unnecessary FTP access permissions for all users.
    - Implement enhanced monitoring for outbound FTP traffic.

Step 5: Follow-Up Investigation

1. **Forensic Analysis:**
    - Examine FinanceServer01 for malware, unauthorised access, or misconfigured FTP services.
    - Analyse file access logs to determine how the sensitive data was obtained.
2. **Credential Audit:**
    - Investigate if finance_user credentials were compromised or abused.
    - Check for signs of phishing or credential leaks using breach monitoring tools like Have I Been Pwned.
3. **External IP Validation:**
    - Validate 203.0.113.45 against updated threat intelligence feeds.
    - Conduct geolocation analysis to trace the IP's origin and associated activities.
4. **Remediation:**

- Patch vulnerabilities in FTP configurations to prevent unauthorised usage.
- Replace sensitive data (e.g., payroll and employee records) and implement encryption at rest and in transit.

Questions & Answers for Analyst Training

Q1: Why is FTP traffic a red flag for sensitive data?

- FTP transfers data in plaintext (unless secured via FTPS/SFTP), making it vulnerable to interception. Additionally, high-volume FTP traffic is uncommon in modern business environments, raising suspicions of potential data exfiltration.

Q2: How can you prevent unauthorised outbound FTP activity?

- Disable unused FTP services, enforce firewall rules to restrict FTP traffic, and use secure protocols like SFTP. Monitor for high-volume or unusual FTP activity.

Q3: What are the key indicators of data exfiltration in FTP logs?

- Large file transfers, connections to untrusted external IPs, and unusual activity from legitimate user accounts are strong indicators of data exfiltration.

Additional Monitoring Rules for Detection

1. **Rule 1:** Alert on high-volume outbound FTP traffic exceeding normal thresholds.
2. **Rule 2:** Trigger alerts for FTP connections to external IPs not whitelisted.
3. **Rule 3:** Correlate FTP usage with user behavior anomalies (e.g., logins from unusual locations).

MALWARE DETECTION

USE CASE 9: SUSPICIOUS FILE HASH MATCHING KNOWN MALWARE

Scenario Overview

- **Client Name:** Manchester United
- **Date/Time of Incident:** December 3, 2024, 4:15 PM GMT
- **Alert Type:** Suspicious File Hash Matching Known Malware
- **Detection Source:** SIEM (Splunk) integrated with Threat Intelligence Platform (VirusTotal)
- **Affected Environment:** Endpoint Systems

Step 1: Initial Alert Details

Splunk Alert Name: File Hash Matched Known Malware Signature

- **Trigger Condition:** File hash matches a known malware signature from the threat intelligence feed.
- **Severity:** Critical
- **Impacted Systems:**
    - Workstation-01
    - FinanceServer02

File Details:

- **Hash (SHA-256):** f7c3bc1d808e04732adf679965ccc34ca7ae3441
- **File Name:** invoice_document.exe
- **Malware Name (per VirusTotal):** Emotet Loader

Step 2: Gather Logs and Analyse

Antivirus Logs:

Date/Time	System	Action	File Path
2024-12-03 4:10 PM	Workstation-01	Quarantined	C:\Users\John\Downloads\invoice_document.exe
2024-12-03 4:12 PM	FinanceServer02	Blocked	D:\Shared\HRFiles\invoice_document.exe

Network Logs:

Source IP	Destination IP	Port	Protocol	Bytes Transferred
192.168.10.25	45.76.123.210	80	HTTP	3,000 KB
192.168.20.15	203.0.113.75	443	HTTPS	5,500 KB

Threat Intelligence Report (VirusTotal):

- **File Hash Match:** Yes
- **Associated Threat Actor:** TA542 (Emotet Group)
- **Known Indicators of Compromise (IOCs):**
    - Command & Control (C2) Domains: malicious-site.com, badactor.org
    - Associated IPs: 45.76.123.210, 203.0.113.75

Step 3: Analyse Findings

1. **Suspicious Behavior Identified:**
    - A file (invoice_document.exe) flagged by VirusTotal as malware detected on multiple systems.
    - The file hash is associated with the Emotet malware family, often used for credential theft and ransomware delivery.
    - Network logs show outbound connections from impacted systems to known malicious IPs.
2. **Correlations:**

- Both systems downloaded or attempted to execute the suspicious file.
- Outbound connections from these systems align with the known IOCs for the Emotet malware.

3. **Potential Risks:**
    - Credential theft and lateral movement within the network.
    - Risk of further malware payloads being downloaded.

Step 4: Mitigation Actions

1. **Immediate Response:**
    - Isolate Workstation-01 and FinanceServer02 from the network to prevent further spread.
    - Block outbound connections to known C2 IPs (45.76.123.210, 203.0.113.75) at the firewall.
    - Quarantine the malicious file on affected systems and ensure it is not executed.
2. **Notification:**
    - Notify the Incident Response Team (IRT) about the confirmed malware presence.
    - Inform system users (John from Workstation-01 and relevant stakeholders for FinanceServer02).
3. **Containment:**
    - Deploy endpoint detection and response (EDR) tools across the network to scan for additional malware traces.
    - Update antivirus and threat intelligence databases to ensure protection against similar threats.

Step 5: Follow-Up Investigation

1. **Forensic Analysis:**

- Examine impacted systems for evidence of lateral movement or additional payloads.
- Analyse memory dumps and file activity for signs of malicious processes.

2. **Root Cause Identification:**
    - Determine how the malicious file was introduced, such as email phishing or compromised website downloads.
    - Investigate user behavior and system logs for any signs of intentional or unintentional actions leading to infection.
3. **Remediation Steps:**
    - Patch vulnerabilities on the impacted systems and servers.
    - Train employees on recognising malicious attachments and downloads.

Questions & Answers for Analyst Training

Q1: What is the significance of file hash matching in malware detection?

- File hashes uniquely identify files. Matching a hash with a known malware signature helps quickly detect and confirm malicious activity without requiring full file analysis.

Q2: How can you confirm if a suspicious file is part of a larger attack?

- Correlate the file with network logs, system behavior, and threat intelligence reports. Look for additional IOCs like C2 communications, lateral movement, or additional malicious files.

Q3: Why isolate systems during an active malware detection?

- Isolation prevents the malware from spreading to other systems and stops ongoing communication with C2 servers, limiting the attack's impact.

Additional Monitoring Rules for Detection

1. **Rule 1:** Alert on file hash matches with high-confidence malware signatures.
2. **Rule 2:** Monitor for unusual file downloads or executions from external sources.

3. **Rule 3:** Detect outbound connections to known malicious IPs and domains in real time.

USE CASE 10: MALWARE CALLBACK DETECTION

Scenario Overview

- **Client Name:** Manchester United
- **Date/Time of Incident:** December 3, 2024, 7:45 PM GMT
- **Alert Type:** Malware Callback Detection
- **Detection Source:** SIEM (Splunk) and IDS (Snort)
- **Affected Environment:** Corporate Network

Step 1: Initial Alert Details

SIEM Alert Name: Outbound Connection to Known Malicious C2 Server

- **Trigger Condition:** Outbound network traffic to a known malicious IP from internal endpoints.
- **Severity:** Critical
- **Impacted Systems:**
    - Workstation-05
    - HRServer03

Indicators of Compromise (IOCs):

- **Malicious IPs:**
    - 192.168.70.20
    - 203.0.113.55
- **Domains:**
    - malicious-callback.net
    - stealth-c2.org
- **Protocol:** HTTP, HTTPS, DNS

Step 2: Gather Logs and Analyse

IDS Logs (Snort):

Timestamp	Source IP	Destination IP	Alert	Protocol
2024-12-03 7:40 PM	10.0.1.15	192.168.70.20	Outbound Connection to Known C2 Server	HTTP
2024-12-03 7:42 PM	10.0.1.18	203.0.113.55	Malicious Domain Resolution	DNS

SIEM Logs (Splunk):

Event Time	System	Action	Details
2024-12-03 7:40 PM	Workstation-05	Outbound HTTP Request	Domain: malicious-callback.net
2024-12-03 7:42 PM	HRServer03	Outbound DNS Query	Domain: stealth-c2.org

Threat Intelligence Feed:

- **Malicious IPs:** Associated with Cobalt Strike C2 frameworks.
- **Domains:** Used in ransomware distribution and phishing campaigns.

Step 3: Analyse Findings

1. **Suspicious Behavior Identified:**
    - Outbound connections to known malicious C2 servers.
    - Systems attempting to communicate with domains associated with advanced malware frameworks.
2. **Correlations:**
    - Logs show direct correlation between DNS queries and HTTP requests to malicious domains.
    - Threat intelligence identifies the domains and IPs as part of active malware campaigns.

3. **Potential Risks:**
    - Risk of data exfiltration or additional payload delivery from C2 servers.
    - Malware could establish persistence, enabling lateral movement.

Step 4: Mitigation Actions

1. **Immediate Response:**
    - Block outbound connections to the malicious IPs (192.168.70.20, 203.0.113.55) and domains (malicious-callback.net, stealth-c2.org) at the firewall.
    - Isolate Workstation-05 and HRServer03 to prevent further activity.
2. **Notification:**
    - Notify the Incident Response Team (IRT) and escalate the incident to Tier-2 analysts.
    - Inform system owners and users about the potential compromise.
3. **Containment:**
    - Conduct a deep scan of affected systems using EDR tools to detect and remove malicious executables.
    - Apply patches and updates to vulnerable software that could have been exploited.

Step 5: Follow-Up Investigation

1. **Forensic Analysis:**
    - Analyse memory and disk images from Workstation-05 and HRServer03 for malware artifacts.
    - Identify the source of infection, such as phishing emails or drive-by downloads.
2. **Root Cause Identification:**

- Check for phishing emails or malicious downloads that may have introduced the malware.
- Investigate for lateral movement attempts by analysing network traffic patterns.

3. **Remediation Steps:**
   - Harden endpoint defenses and ensure all endpoints have updated threat signatures.
   - Conduct user awareness training on phishing and suspicious activity.

Questions & Answers for Analyst Training

Q1: What is a Command and Control (C2) server, and why is it significant?

- A C2 server is used by attackers to control compromised systems remotely. It is significant because it allows attackers to execute commands, exfiltrate data, and deliver additional payloads.

Q2: How can malware callbacks be detected proactively?

- By monitoring outbound traffic for connections to known malicious IPs or domains using threat intelligence feeds, IDS, and anomaly detection systems.

Q3: What additional security measures can help prevent malware callbacks?

- Implement DNS filtering to block malicious domains.
- Use network segmentation to limit communication between endpoints.
- Enable strict outbound firewall rules and regularly update threat intelligence feeds.

Additional Monitoring Rules for Detection

1. **Rule 1:** Alert on DNS queries to known malicious domains or newly registered domains.
2. **Rule 2:** Detect outbound connections to external IPs flagged by threat intelligence feeds.
3. **Rule 3:** Monitor for unusual traffic patterns, such as large data transfers to unknown external destinations.