**InfoBlox Log Source Analysis**

**1. Executive Summary**

This analysis documents the implementation of InfoBlox log monitoring in our Egyptian banking SIEM environment. The document includes use cases, detection rules, and response procedures specific to InfoBlox security events to enhance our security monitoring capabilities in accordance with ISO 27001 and PCI DSS requirements, with attention to threat actors targeting Egyptian financial institutions.

**2. Compliance Alignment**

| **Control Family** | **Control ID** | **InfoBlox Monitoring Applicability** |
| --- | --- | --- |
| ISO 27001 | A.12.4 - Logging and monitoring | Ensures DNS/DHCP infrastructure logs are collected and analyzed |
| ISO 27001 | A.13.1 - Network security management | Monitors critical network service configuration changes |
| PCI DSS | Req. 10.2 - Implement automated audit trails | Captures all InfoBlox administrative actions |
| PCI DSS | Req. 10.6 - Review logs daily | Provides alerting for critical InfoBlox events |
| PCI DSS | Req. 11.4 - Intrusion-detection mechanisms | Detects abnormal InfoBlox activity that may indicate compromise |
| CBE | Egyptian Banking Security Framework | Monitors critical infrastructure for threats targeting financial systems |

**3. Egypt-Specific Threat Landscape**

**Threat Actors Targeting Egyptian Banking Infrastructure**

| **Threat Actor** | **TTPs** | **InfoBlox-Related Activity** |
| --- | --- | --- |
| APT-C-23 (Desert Falcons) | Spear-phishing, DNS hijacking, Watering hole attacks | DNS record manipulation to redirect banking customers to phishing sites |
| MuddyWater | DNS tunneling for C2, DNS cache poisoning | Excessive DNS queries with encoded data, unexpected DNS record changes |
| TA505 | Banking trojan delivery, DNS manipulation | DNS queries to newly registered domains, high-volume DNS requests |
| Local Financial Fraudsters | DNS hijacking of Egyptian bank domains | Unauthorized changes to banking domain records, registration of typosquatted domains |
| Ransomware Operators | Infrastructure reconnaissance via DNS | Scanning DNS for banking assets, DNS queries for internal resources |

**Regional Risk Factors**

1. Increased targeting of Middle Eastern and North African banking sectors
2. Politically motivated attacks against Egyptian financial infrastructure
3. Cross-border financial fraud targeting Egyptian banks
4. Regional instability creating opportunities for hacktivism

**4. Log Source Technical Details**

**InfoBlox Log Types and Formats**

| **Log Type** | **Description** | **Format Example** |
| --- | --- | --- |
| System | General system events | Mar 13 14:22:33 infoblox.local named[1234]: system event description |
| DNS | DNS query logs | Mar 13 14:22:33 infoblox.local named[1234]: client 10.0.0.1#12345: query: example.com IN A |
| DHCP | DHCP lease events | Mar 13 14:22:33 infoblox.local dhcpd[1234]: DHCPACK on 192.168.1.100 to 00:11:22:33:44:55 |
| Admin | Administrative actions | Mar 13 14:22:33 infoblox.local httpd[1234]: admin "admin" logged in from 10.0.0.2 |
| Security | Security-related events | Mar 13 14:22:33 infoblox.local named[1234]: client 10.0.0.3#12345: query denied |

**ArcSight Parser Configuration**

InfoBlox logs are parsed in ArcSight using the following configuration:

* Device Product: InfoBlox
* Device Vendor: InfoBlox Inc.
* Category Technique: Syslog

**5. Detection Use Cases**

**Use Case 1: Unauthorized Administrative Access**

**Description:** Detects potential unauthorized access to InfoBlox administration interfaces. Critical for protecting cardholder data environments (CDE) DNS infrastructure.

**ArcSight Rule:**

Name: BANK\_InfoBlox\_Unauthorized\_Admin\_Access

Priority: High

Condition:

deviceVendor = "InfoBlox Inc." AND

categoryBehavior = "Authentication" AND

(message CONTAINS "login failed" OR

(message CONTAINS "logged in" AND sourceAddress NOT IN LIST AdminSourceIPs))

Aggregation: 3 events in 5 minutes

**Evidence to Collect:**

Mar 13 14:22:33 infoblox.local httpd[1234]: admin "admin" failed login from 10.0.0.100

Mar 13 14:22:38 infoblox.local httpd[1234]: admin "admin" failed login from 10.0.0.100

Mar 13 14:22:43 infoblox.local httpd[1234]: admin "admin" logged in from 10.0.0.100

Mar 13 14:22:55 infoblox.local httpd[1234]: admin "admin" modified zone "bankingdomain.eg"

**Tier 1 SOC Analyst Response:**

1. Verify if the source IP is associated with authorized administrators
2. Check if access occurred during bank's change management windows
3. Contact the admin to confirm if access was legitimate
4. Document findings in ticket
5. Check for correlation with Egyptian banking threat intelligence

**Escalation:** Escalate to Tier 2 SOC if:

* No change management ticket exists
* Access from external IP address
* More than 5 failed login attempts
* IP address associated with Egyptian threat actors

**Use Case 2: Critical DNS Configuration Changes**

**Description:** Monitors for potentially malicious changes to DNS configurations that could impact banking services or redirect customers to fraudulent sites.

**ArcSight Rule:**

Name: BANK\_InfoBlox\_Critical\_DNS\_Change

Priority: High

Condition:

deviceVendor = "InfoBlox Inc." AND

categoryBehavior = "Modify" AND

categoryObject = "Configuration" AND

message CONTAINS ANY ("zone", "dns", "record", "deleted", "modified", "created") AND

(message CONTAINS ANY ("banking", "payment", "secure", "login", "account", ".eg") OR

message CONTAINS ANY (list:EgyptianBankingDomains))

**Evidence to Collect:**

Mar 13 14:30:15 infoblox.local named[1234]: zone ourbank.eg/IN: creating new master file /var/named/master/db.ourbank.eg

Mar 13 14:30:22 infoblox.local named[1234]: zone ourbank.eg/IN: loaded serial 2025031302

Mar 13 14:30:25 infoblox.local httpd[1234]: admin "admin" modified record "login.ourbank.eg" A value changed from "192.168.10.50" to "192.168.10.51"

Mar 13 14:31:05 infoblox.local httpd[1234]: admin "admin" created record "secure-verify.ourbank.eg" A value "10.0.0.100"

**Tier 1 SOC Analyst Response:**

1. Cross-reference with change management tickets
2. Identify which admin made the change
3. Document exact changes made to Egyptian banking-related DNS records
4. Validate if change impacts online banking or payment systems
5. Check if new DNS entries match known phishing patterns

**Escalation:** Escalate to Tier 2 SOC if:

* Change affects Egyptian online banking domains
* Change made outside maintenance window
* Change has no corresponding change ticket
* New IPs are outside our expected network ranges

**Use Case 3: DNS Data Exfiltration Detection**

**Description:** Identifies potential data exfiltration via DNS tunneling, critical for protecting customer and financial data.

**ArcSight Rule:**

Name: BANK\_InfoBlox\_DNS\_Exfiltration

Priority: Medium

Condition:

deviceVendor = "InfoBlox Inc." AND

categoryBehavior = "Access" AND

categoryObject = "DNS" AND

(message CONTAINS "query:" AND

(LENGTH(message) > 200 OR

message MATCHES REGEX "query:.\*\.([a-zA-Z0-9]{30,})\."))

Aggregation: 10 events from same source in 5 minutes

**Evidence to Collect:**

Mar 13 15:10:22 infoblox.local named[1234]: client 10.0.0.21#54321: query: aG9zdD1iYW5rLmVnJnVzZXI9YWRtaW4mcGFzcz1wQHNzdzByZA==.exfil.example.com IN A

Mar 13 15:10:25 infoblox.local named[1234]: client 10.0.0.21#54322: query: dHJhbnNmZXI9MTAwMDAwJmFjY291bnQ9MTIzNDU2Nzg5MA==.exfil.example.com IN A

Mar 13 15:10:28 infoblox.local named[1234]: client 10.0.0.21#54323: query: Y2FyZG51bWJlcj00OTI3NjY2NDU1MzM0NDY2JmN2dj0xMjM=.exfil.example.com IN A

Mar 13 15:10:31 infoblox.local named[1234]: client 10.0.0.21#54324: query: Y3VzdG9tZXJkYXRhPXsiZmlyc3RuYW1lIjoiQWhtZWQiLCJsYXN0bmFtZSI6Ik1vaGFtZWQiLCJhY2NvdW50IjoiODc2NTQzMjEiLCJiYWxhbmNlIjoiMTIzNDU2Ljc4In0=.exfil.example.com IN A

**Tier 1 SOC Analyst Response:**

1. Identify source host's location (CDE/non-CDE network)
2. Analyze the domain structure for encoded data patterns
3. Check if source host handles sensitive banking data
4. Run quick analysis report on volume of DNS queries from this host
5. Attempt base64 decoding of suspicious query components

**Escalation:** Escalate to Tier 2 SOC if:

* Source is within PCI cardholder data environment
* Pattern matches known DNS exfiltration techniques
* Host contains customer financial data
* Decoded data contains sensitive Egyptian customer information

**6. SOC Shift Handover Documentation**

For 24/7 monitoring across shifts, document the following for InfoBlox alerts:

**Active Investigations:**

* Current status of any open InfoBlox-related incidents
* Actions taken during current shift
* Pending actions for next shift

**Tuning Activities:**

* False positives identified during shift
* Temporary exceptions created
* Rule modifications pending implementation

**Daily Summary Report:**

* Total InfoBlox alerts triggered
* Distribution by severity
* Notable patterns observed
* Recommendations for rule adjustments

**7. Incident Response Tier Escalation Matrix**

| **Alert** | **Tier 1** | **Tier 2** | **Tier 3** |
| --- | --- | --- | --- |
| Unauthorized Admin Access | Initial triage, validation against whitelist, log evidence collection | Deeper investigation, admin interview, extended evidence collection | Full incident response, forensic analysis, Central Bank of Egypt notification assessment |
| Critical DNS Changes | Change validation, impact assessment, log timeline creation | Analysis of change intent, security implications, evidence preservation | Coordination with network team, recovery planning, external notifications |
| DNS Data Exfiltration | Pattern identification, volume analysis, basic data decoding | Host investigation, data loss assessment, pattern analysis | Advanced forensics, regulatory reporting assessment, legal team engagement |

**8. Evidence Collection Guidelines**

**Required Log Evidence**

For each InfoBlox alert, collect the following evidence:

1. **Pre-incident logs (24 hours prior):**
2. ArcSight query:
3. deviceVendor = "InfoBlox Inc." AND sourceAddress = "<suspect\_IP>"
4. startTime = now()-24h endTime = <incident\_time>
5. **Complete administrative session logs:**
6. ArcSight query:
7. deviceVendor = "InfoBlox Inc." AND (categoryBehavior = "Authentication" OR categoryBehavior = "Modify")
8. AND sourceAddress = "<admin\_IP>" startTime = <session\_start> endTime = <session\_end>
9. **Related DNS activity:**
10. ArcSight query:
11. deviceVendor = "InfoBlox Inc." AND categoryObject = "DNS"
12. AND message CONTAINS "<modified\_domain>"
13. startTime = now()-48h endTime = now()

**Evidence Format Requirements**

1. Raw logs must be preserved in their original format
2. Include timestamp, source IP, username, and action details
3. Document any correlation with other security systems
4. Preserve all related change management tickets
5. Create a timeline of events in standard format
6. Document all investigative actions taken

**9. Implementation Plan for Ongoing Monitoring**

**Phase 1: Initial Deployment (Complete)**

* [x] Configure log forwarding from InfoBlox to ArcSight
* [x] Verify log parsing and field mapping
* [x] Develop initial use cases aligned with ISO 27001 and PCI DSS

**Phase 2: Tuning (In Progress)**

* [ ] Establish baselines for normal InfoBlox activity in Egyptian banking environment
* [ ] Adjust thresholds based on baseline data
* [ ] Document false positive scenarios specific to banking DNS traffic
* [ ] Create Egyptian banking domain watchlist

**Phase 3: Advanced Detection (Planned)**

* [ ] Implement correlation with banking application logs
* [ ] Develop specialized rules for Egyptian online banking DNS protection
* [ ] Create automated reports for ISO 27001 and PCI DSS compliance audits
* [ ] Configure alerts for Egypt-specific threat intelligence feeds

**10. References and Resources**

* InfoBlox Admin Guide v8.4.2
* ISO 27001 A.12.4 Implementation Guide
* PCI DSS Requirements 10.2, 10.6
* Central Bank of Egypt Cybersecurity Framework
* MITRE ATT&CK Middle East Threat Landscape Report