SOC ANALYST TRAINING

Anti-Call Masking Platform

Duration: ~45 minutes
Audience: Security Operations Center Analysts
Version: 2.0 | January 2026

PREREQUISITES

- Completed System Overview training
- SOC Analyst dashboard credentials
- Understanding of telecommunications basics
- Familiarity with fraud detection concepts

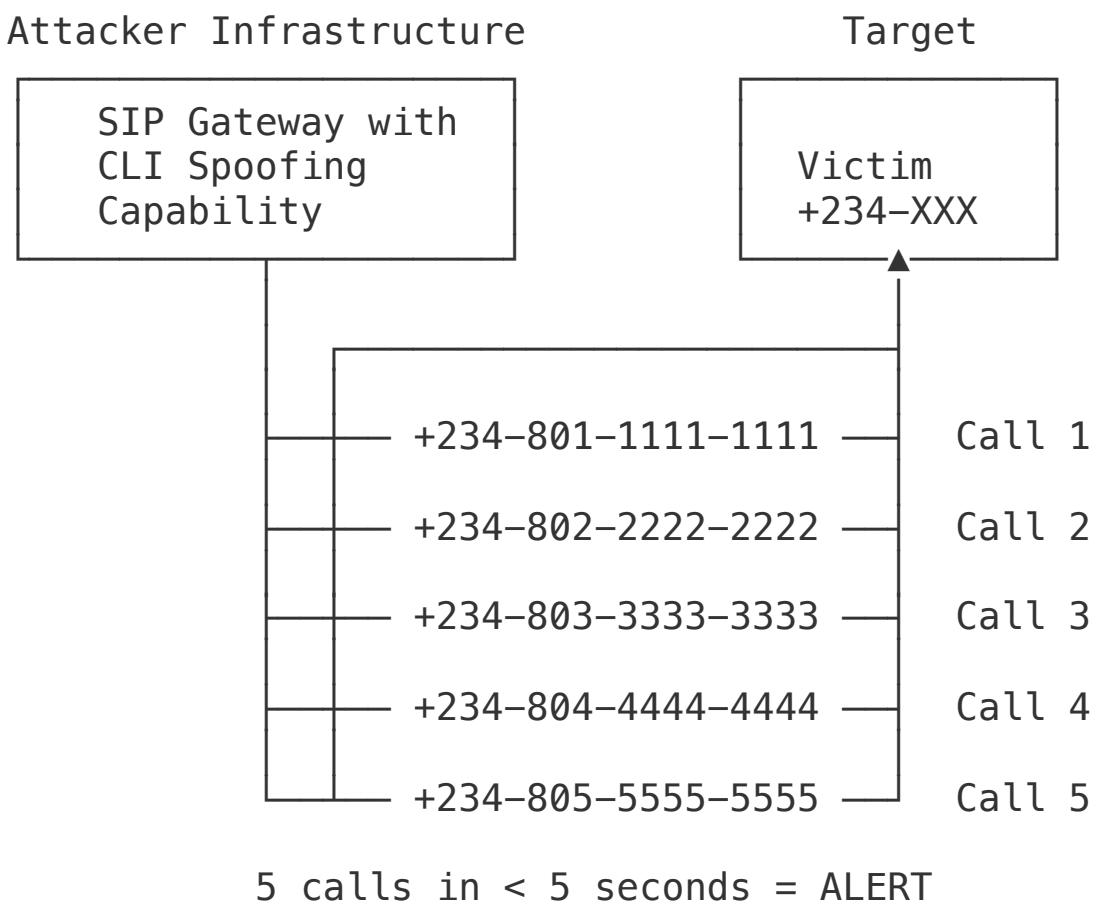
AGENDA

1. Understanding Call Masking Attacks
2. Dashboard Navigation
3. Alert Management
4. Investigation Techniques
5. Response Actions
6. Whitelist Management
7. Reporting & Documentation

UNDERSTANDING CALL MASKING ATTACKS

Know your enemy

ATTACK ANATOMY



WHY ATTACKERS USE MASKING

ATTACKER GOALS:

- Evade call blocking
- Appear legitimate
- Overwhelm targets
- Hide true identity

COMMON SCAMS:

- Bank impersonation
- Government fraud
- Prize/lottery scams
- Tech support fraud

DETECTION CRITERIA

> **Default Threshold:** 5+ distinct A-numbers calling the sam
> B-number within 5 seconds

Parameter	Value	Configurable
Minimum A-numbers	5	Yes (3-20)
Time Window	5 seconds	Yes (1-30s)
Cooldown Period	60 seconds	Yes

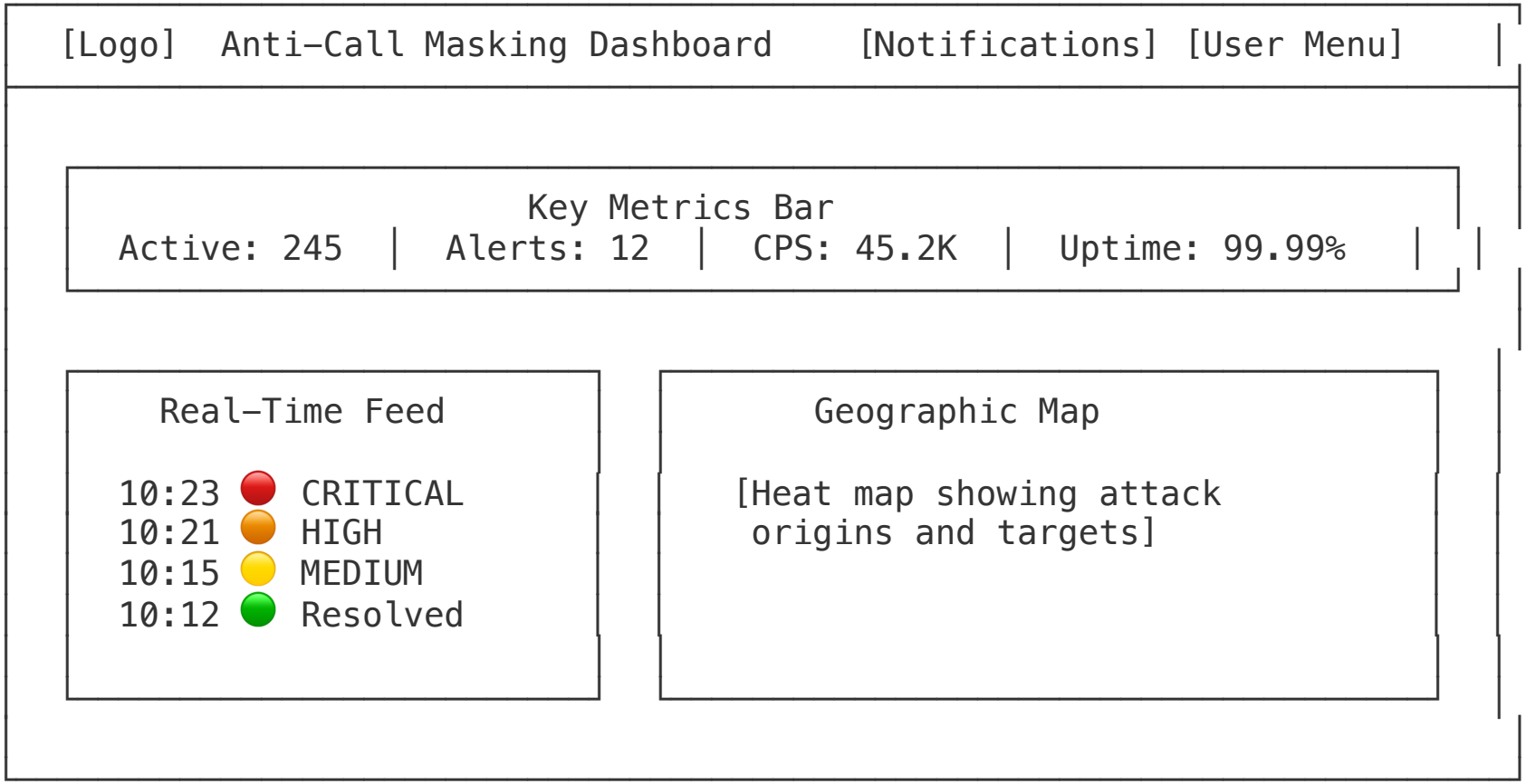
SEVERITY LEVELS

Severity	A-Numbers	Response SLA	Auto-Action
CRITICAL	7+	Immediate	Auto-disconnect
HIGH	5-6	15 minutes	Alert only
MEDIUM	3-4	30 minutes	Alert only
LOW	2	1 hour	Log only

DASHBOARD NAVIGATION

Your primary workspace

MAIN DASHBOARD



NAVIGATION MENU

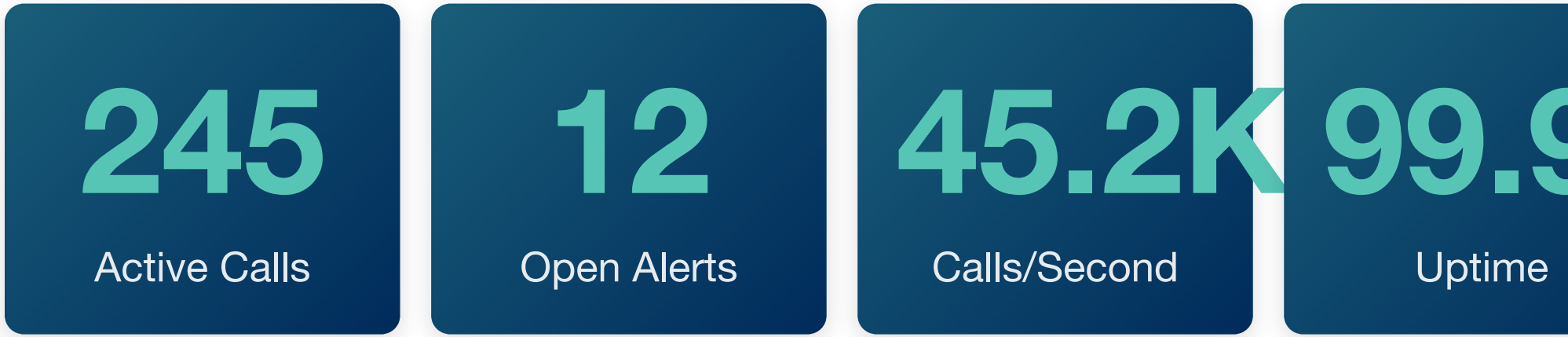
Section	Purpose	Shortcut
Dashboard	Main monitoring view	`G` + `D`
Alerts	Alert queue and history	`G` + `A`
Analytics	Charts and statistics	`G` + `N`
Reports	Generate reports	`G` + `R`
Whitelist	Manage exemptions	`G` + `W`

REAL-TIME FEED

- **Auto-updates** every second via WebSocket
- **Color-coded** by severity
- **Click any alert** to view details
- **Filter** by severity, status, or time
- **Sound alerts** for CRITICAL events

> **Tip:** Keep the feed visible at all times during your shift. Use `Space` to pause/resume updates.

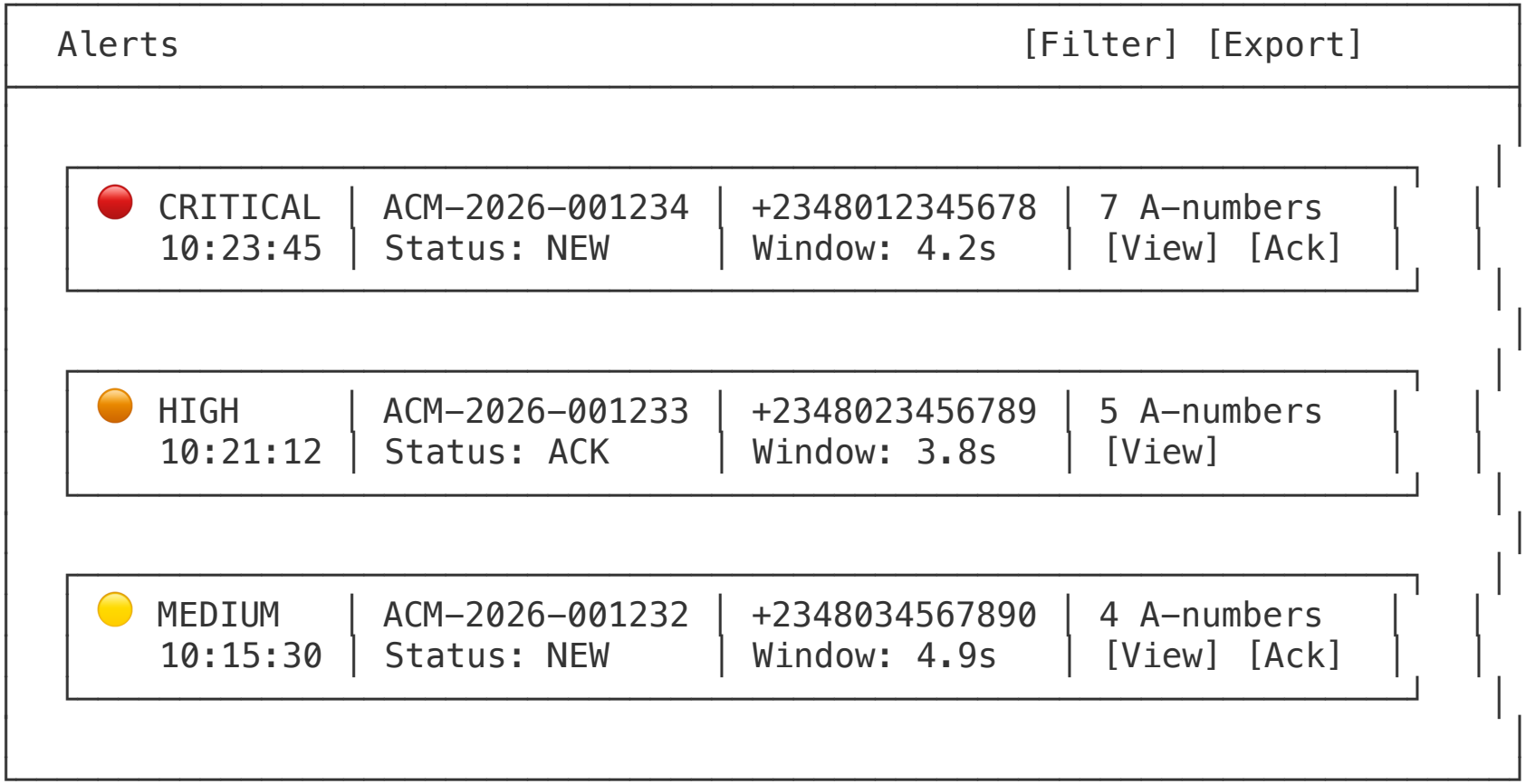
KEY METRICS EXPLAINED



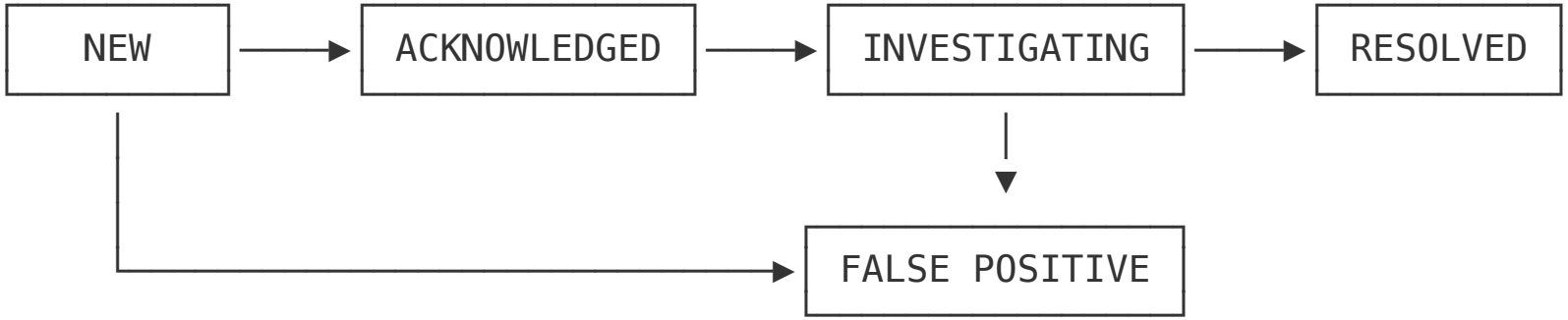
ALERT MANAGEMENT

Handling fraud alerts effectively

ALERT QUEUE VIEW

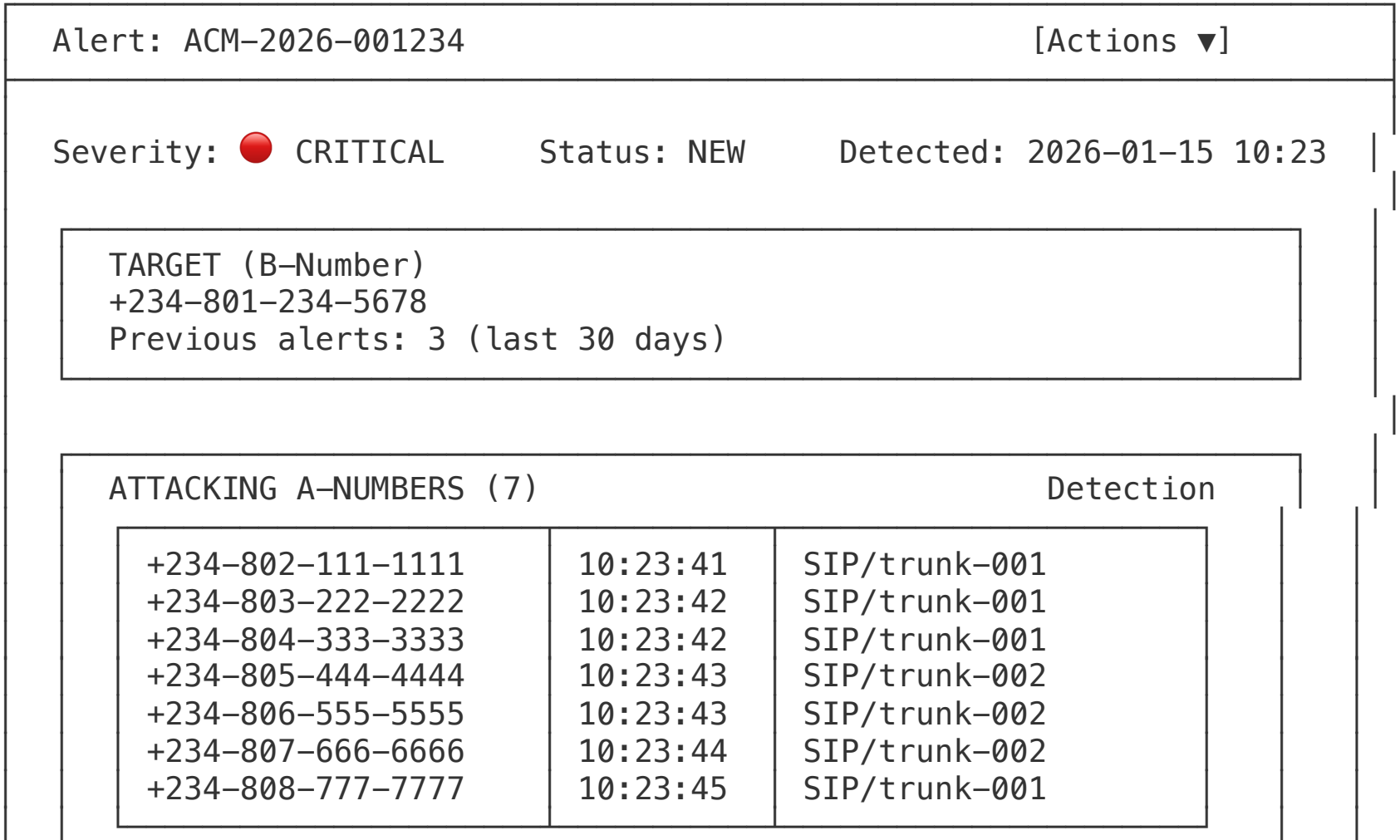


ALERT LIFECYCLE



Status	Meaning
NEW	Just detected, needs attention
ACKNOWLEDGED	Analyst has seen it
INVESTIGATING	Active investigation

ALERT DETAIL VIEW



AVAILABLE ACTIONS

Action	Shortcut	Description
Acknowledge	`A`	Take ownership of alert
Investigate	`I`	Start formal investigation
Disconnect	`D`	Terminate active calls
Block Pattern	`B`	Block A-number pattern
Add Note	`N`	Add investigation note
Escalate	`E`	Send to supervisor
Resolve	`R`	Mark as handled

BULK OPERATIONS

1. Select multiple alerts using checkboxes
2. Or use `Shift` + click for range
3. Click "Bulk Actions" dropdown
4. Choose operation:
    - Acknowledge All
    - Assign To...
    - Export Selected
    - Mark False Positive

INVESTIGATION TECHNIQUE

Finding the truth behind alerts

INVESTIGATION WORKFLOW

- **Step 1:** Acknowledge the alert
- **Step 2:** Review A-numbers for patterns
- **Step 3:** Check B-number history
- **Step 4:** Analyze source trunks/IPs
- **Step 5:** Determine if legitimate or fraud
- **Step 6:** Take action and document

PATTERN ANALYSIS

RED FLAGS (LIKELY FRAUD):

- Sequential A-numbers (e.g., +234-801-1111, +234-801-1112...)
- All calls from same SIP trunk
- B-number is a personal mobile
- Calls outside business hours
- International trunk with local CLIs

PATTERN ANALYSIS

GREEN FLAGS (LIKELY LEGITIMATE):

- B-number is known call center
- B-number is IVR/conference bridge
- Previous whitelist requests
- A-numbers are known business lines
- Pattern matches business operations

B-NUMBER HISTORY

B-Number History: +234-801-234-5678

Total Alerts (30 days): 3
False Positives: 0
Whitelist Status: Not whitelisted

Previous Alerts

Date	Severity	A-Numbers	Resolution
2026-01-10	HIGH	5	Resolved - Fraud
2026-01-05	MEDIUM	4	Resolved - Fraud
2025-12-28	HIGH	6	Resolved - Fraud

Analysis: This number is a repeat target. Likely vulnerable consumer.

SOURCE ANALYSIS

Source Type	Risk Level	Typical Action
Unknown International Gateway	High	Block + Escalate
Known Partner Trunk	Medium	Investigate + Notify
Internal Network	Low	Verify + Whitelist

DECISION MATRIX

Scenario	Action
Confirmed fraud, calls active	**Disconnect immediately**
Confirmed fraud, calls ended	Document + Block pattern
Likely legitimate business	Verify + Add to whitelist
Uncertain, need more info	Escalate to supervisor
Known false positive source	Mark FP + Update whitelist

RESPONSE ACTIONS

Taking action against fraud

DISCONNECTING CALLS

> **Warning:** Disconnecting calls affects live traffic. Use only when fraud is confirmed.

STEPS:

1. Confirm alert is genuine fraud
2. Click "Disconnect" or press `D`
3. Select calls to disconnect (or "All")
4. Confirm action
5. Add note explaining decision

BLOCKING PATTERNS

BLOCK TYPES:

Type	Example	Use When
Exact Number	+234-801-111-1111	Single bad actor
Prefix Block	+234-801-111-*	Sequential range attack
Trunk Block	SIP/trunk-suspect	Compromised gateway

> Prefix blocks can affect legitimate traffic. Use sparingly an
> review regularly.

ESCALATION CRITERIA

ESCALATE TO SUPERVISOR WHEN:

- Attack involves 10+ A-numbers
- Multiple B-numbers targeted simultaneously
- Source is a known partner trunk
- Uncertain about appropriate action
- VIP/high-profile target involved
- Potential NCC reporting required

DOCUMENTATION REQUIREMENTS

EVERY RESOLVED ALERT MUST HAVE:

- **Classification:** Fraud / False Positive / Unknown
- **Actions Taken:** What you did
- **Justification:** Why you did it
- **Follow-up:** Any pending items

> Good documentation protects you and helps others learn from your investigations.

WHITELIST MANAGEMENT

Managing legitimate exceptions

WHEN TO WHITELIST

GOOD CANDIDATES:

- Call centers
- Conference bridges
- IVR systems
- Emergency services
- Verified business lines

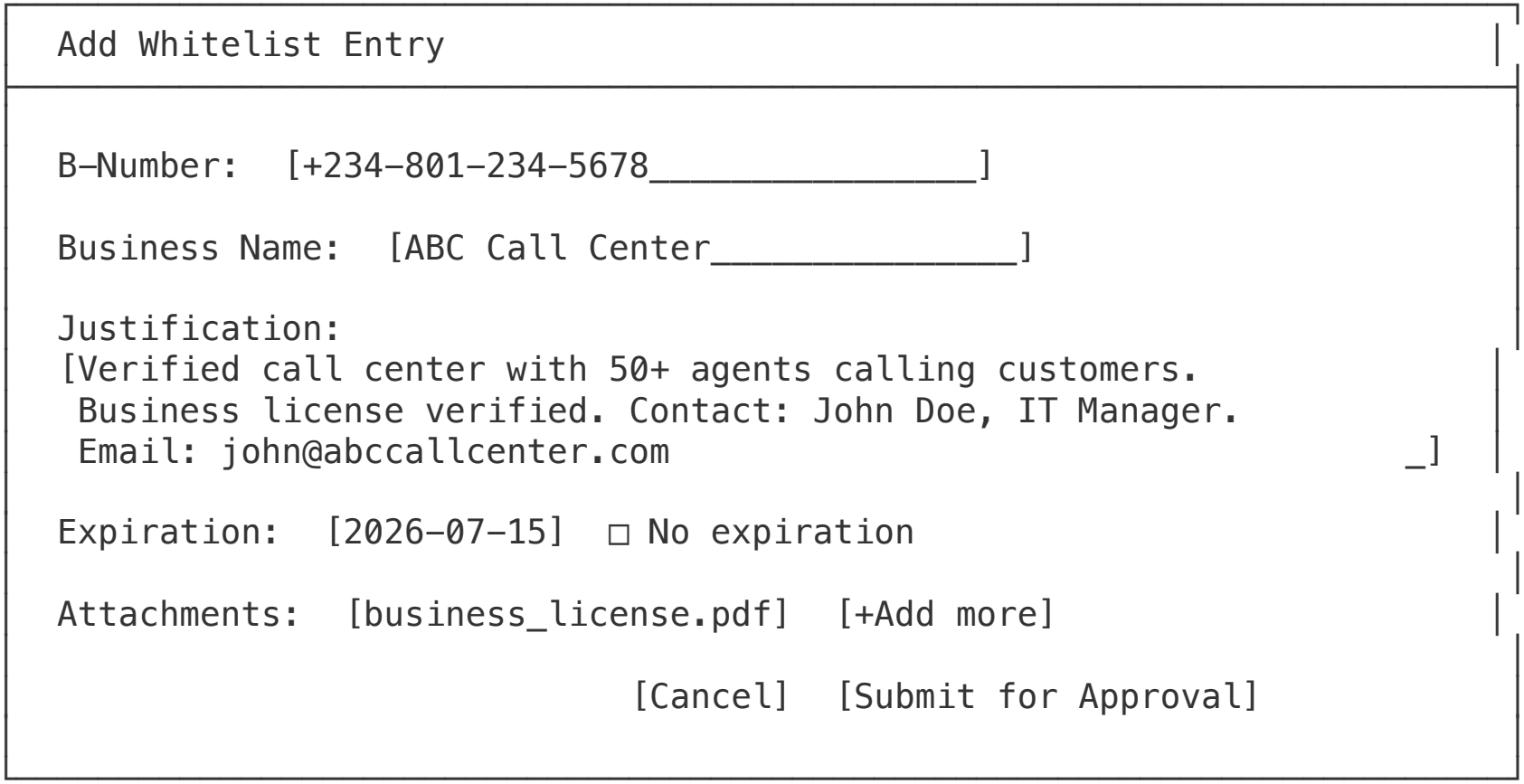
DO NOT WHITELIST:

- Personal mobile numbers
- Unverified requests
- Numbers with fraud history
- Temporary workarounds

ADDING TO WHITELIST

1. Navigate to **Configuration > Whitelist**
2. Click "Add Entry"
3. Enter B-number (with country code)
4. Provide business justification
5. Set expiration date (recommended)
6. Attach supporting documentation
7. Submit for approval

WHITELIST ENTRY FORM



WHITELIST REVIEW

Review Frequency	Action
Weekly	Review entries expiring soon
Monthly	Audit high-activity entries
Quarterly	Full whitelist review

> Outdated whitelist entries are a security risk. Remove entri
> for closed businesses.

REPORTING & DOCUMENTATION

Tracking and compliance

SHIFT HANDOVER

END-OF-SHIFT REPORT:

- Total alerts handled
- Open alerts (with status)
- Escalations pending
- Notable incidents
- System issues encountered
- Whitelist changes

> Use the "Generate Shift Report" button before handover

INCIDENT REPORTS

MAJOR INCIDENTS REQUIRE FORMAL REPORT:

- 10+ A-numbers in single attack
- Multiple B-numbers targeted
- VIP/sensitive target
- Media attention potential
- NCC notification required

Template available at: `Reports > Templates > Major Incident`

NCC COMPLIANCE

> Daily NCC reports are generated automatically at 06:00 W

YOUR RESPONSIBILITIES:

- Ensure alerts are properly classified
- Document actions taken
- Flag major incidents for inclusion
- Review weekly compliance summary

EXPORTING DATA

AVAILABLE EXPORTS:

Export Type	Format	Use Case
Alert List	CSV, PDF	Management reports
Investigation	PDF	Law enforcement
Statistics	CSV, Excel	Analysis
Audit Trail	PDF	Compliance

BEST PRACTICES

Tips from experienced analysts

EFFICIENCY TIPS

- **Use keyboard shortcuts** - Much faster than clicking
- **Set up filters** - Focus on your assigned severity levels
- **Use multiple monitors** - Dashboard + Alert detail
- **Create saved searches** - Common investigation queri
- **Take regular breaks** - Alert fatigue is real

COMMON MISTAKES TO AVOID

- **Don't** disconnect without verification
- **Don't** whitelist without documentation
- **Don't** ignore LOW severity alerts
- **Don't** skip documentation
- **Don't** handle outside your authority

RESPONSE TIME GUIDELINES

Severity	Acknowledge	Action	Resolve
CRITICAL	1 min	5 min	15 min
HIGH	5 min	15 min	30 min
MEDIUM	15 min	30 min	2 hours
LOW	30 min	2 hours	Shift end

WHEN IN DOUBT...

Ask your supervisor!

It's always better to ask than to make a mistak
that affects live traffic.

KEY TAKEAWAYS

- **Understand the threat** - Know how masking attacks work
- **Use the tools** - Dashboard, shortcuts, filters
- **Investigate thoroughly** - Check patterns, history, sources
- **Act appropriately** - Match response to threat
- **Document everything** - Protect yourself and help others

RESOURCES

DOCUMENTATION:

- SOC_ANALYST_MANUAL.md
- USER_MANUAL.md
- runbook.md

SUPPORT:

- Supervisor on shift
- Slack: #soc-support
- Escalation: PagerDuty

QUESTIONS?

SOC Analyst Training Complete

Next Steps:

1. Practice in sandbox environment
2. Shadow experienced analyst
3. Certification quiz