SIMULATED INCIDENT RESPONSE REPORT
SECURITY ALERT MONITORING & INCIDENT RESPONSE

FOR TRAINING / DEMO PURPOSES ONLY
NOT A REAL INVESTIGATION

Report ID: SIM-IR-4540
Generated: 2025-10-02
Environment: Simulated SOC Training Environment

Prepared by: SOC Simulation Engine

DISCLAIMER: This document is a simulated incident response report containing fabricated alerts and incidents for training or demonstration purposes only. It must not be presented as or used to represent an actual security incident.

Executive Summary

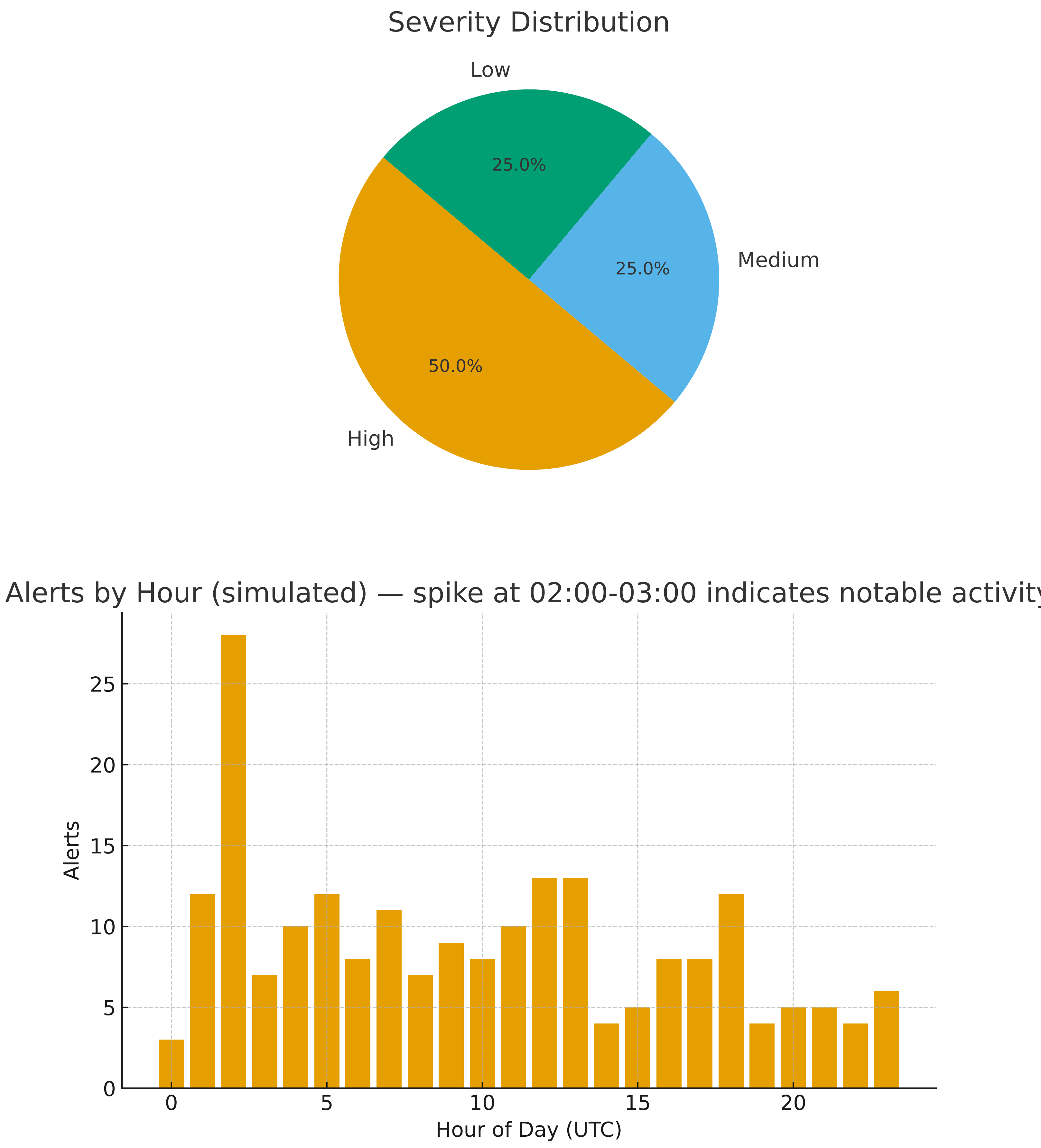
During simulated SOC monitoring, the SIEM generated a set of alerts which were triaged by analysts. True positive incidents were identified and classified. The following summarizes key metrics and prioritized incidents for follow-up.

Total Alerts Reviewed:	175
True Positive Incidents:	5
False Positives:	49
Analyst Triage Time (avg mins):	31
Hosts Isolated:	4
IOC Matches:	19
Logs Indexed (GB):	46.4

Detailed Incident Log (Simulated)

Incident ID	Title	Severity	Source	Affected Host	Detection Tim	Status	Action Taken
IR-2025-001	Brute-force A	High	Splunk Auth L	admin / web-	2025-10-01 0	Contained	Blocked IP 203.0.113.45; ena
IR-2025-002	Suspicious Ou	High	ELK NetFlow	10.0.2.15	2025-10-01 0	Investigating	Isolated host; forensics imag
IR-2025-003	Unusual Privi	Medium	Windows Eve	jdoe	2025-10-01 0	Monitoring	Reviewed RBAC; increased m
IR-2025-004	Endpoint Mal	Low	Elastic Endpo	3 endpoints	2025-09-30 2	Resolved	AV cleaned; signatures upda

Incident Severity Distribution & Alerts Timeline (Simulated)



Severity Distribution

Alerts by Hour (simulated) — spike at 02:00-03:00 indicates notable activity

Recommendations & Incident Response Playbook (Simulated)

Immediate (within 24 hours):

- Enforce MFA for all privileged accounts and apply account lockout for repeated failures.

- Continue investigation on isolated host 10.0.2.15; perform full forensic image and memory capture.

- Block malicious IPs at perimeter and add IDS signatures for observed patterns.

Short Term (1 week):

- Review RBAC and revert suspicious privilege grants if unauthorized.

- Tune SIEM rules to reduce false positives and add automated playbooks for common high-severity alerts.

Ongoing:

- Regular endpoint patching and scheduled phishing simulations.

- Implement DLP controls and monitor large outbound transfers.

Note: This is a simulated report. Use it for training, documentation, or SOC workflow testing only.

- Conduct tabletop exercises and update incident response procedures.