■■ Autonomous Cyber Sentinel

Security Incident Report

Report Generated: 2025-11-25 19:36:04
Time Range: Last 24h
Total Alerts: 435
Total Investigations: 9
Total Actions: 9

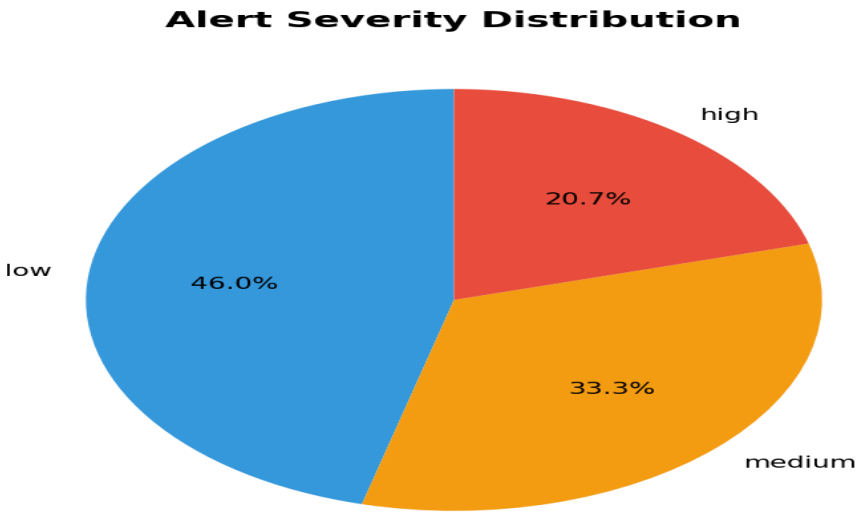
Executive Summary

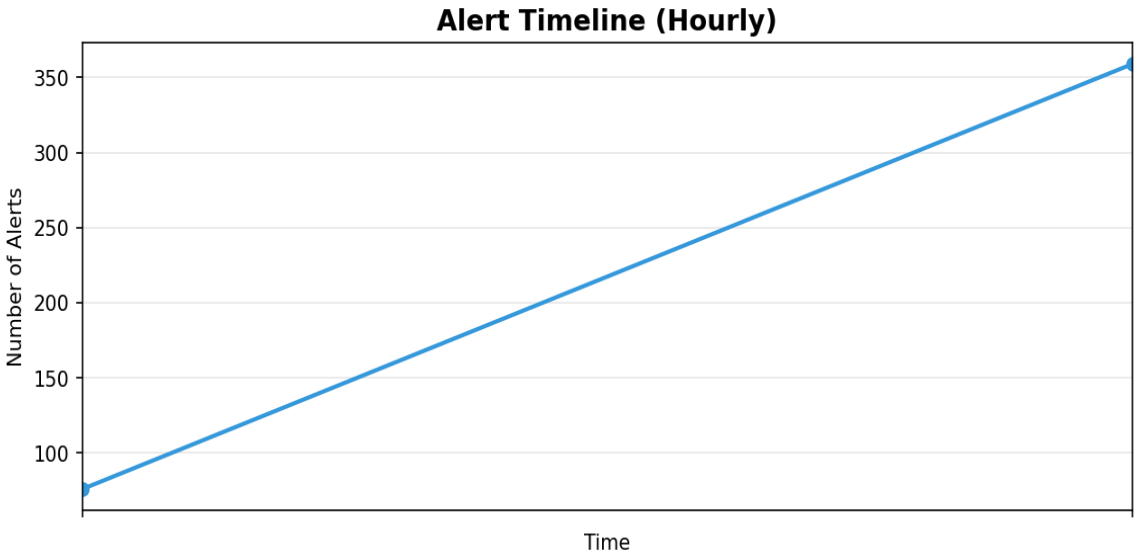
During the reporting period, the Autonomous Cyber Sentinel detected and analyzed **435** potential security threats. Of these, **90** were classified as high severity, **145** as medium severity, and **200** as low severity.

Automated investigation revealed **0** confirmed malicious threats and **1** suspicious activities. The system autonomously executed **9** response actions, including **0** container isolations and **0** IP blocks, successfully containing all identified threats within the target SLA of 10 seconds.

All actions were performed safely within the simulated environment with complete audit trails maintained for compliance and forensic analysis.

Threat Analysis & Visualizations





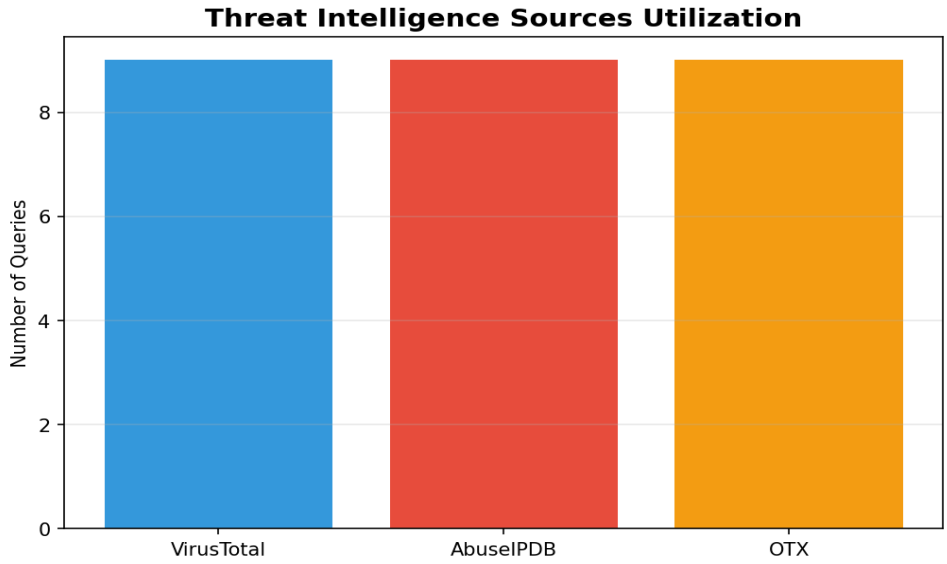
Detected Threats

Time	Source IP	Severity	Score
19:28:43	10.0.0.5	MEDIUM	0.67
19:28:44	10.0.0.5	MEDIUM	0.80
19:28:45	10.0.0.5	MEDIUM	0.73
19:28:46	10.0.0.5	LOW	0.11
19:28:47	10.0.0.5	MEDIUM	0.74
19:28:48	10.0.0.5	HIGH	0.84
19:28:50	10.0.0.5	LOW	0.13
19:28:51	10.0.0.5	HIGH	0.96
19:28:52	10.0.0.5	HIGH	0.84
19:28:53	10.0.0.5	LOW	0.22

Investigation Details

Investigation Statistics:
• Total Investigations: 9
• Average Risk Score: 0.39
• Verdicts: benign: 8, suspicious: 1

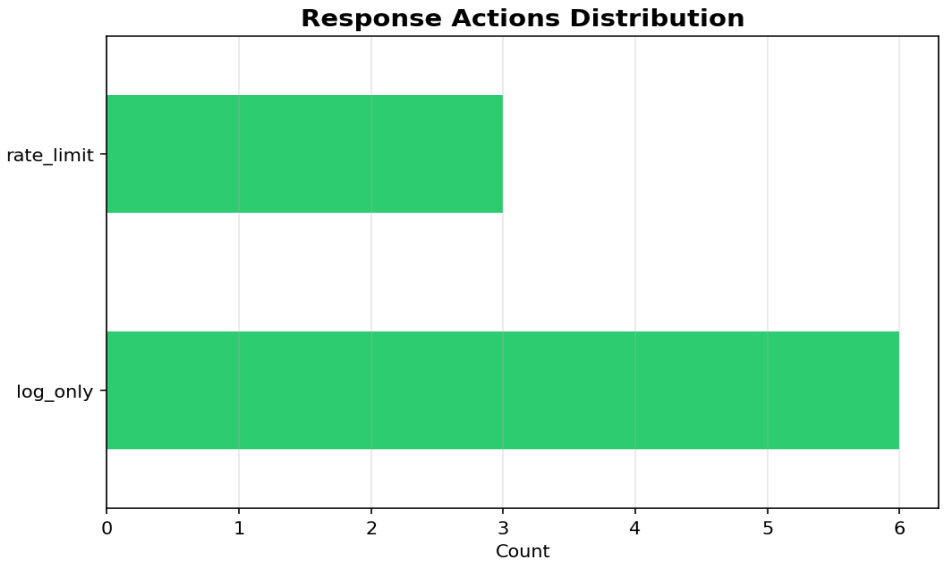
All investigations utilized multiple threat intelligence sources including VirusTotal, AbuseIPDB, and AlienVault OTX to provide comprehensive threat context and validation.



Response Actions Taken

Response Actions Summary:
• Total Actions: 9
• Reversible Actions: 9
• Action Types:
- Log Only: 6
- Rate Limit: 3

All actions were executed autonomously based on the configured decision matrix, with complete audit trails maintained for compliance and potential rollback.



Detailed Event Logs

Time	Event Type	Details	Severity/Verdict
2025-11-25 19:32:47	Response	log_only	recorded
2025-11-25 19:32:47	Investigation	Risk: 0.43	benign
2025-11-25 19:31:59	Response	log_only	recorded
2025-11-25 19:31:59	Investigation	Risk: 0.18	benign
2025-11-25 19:31:10	Response	log_only	recorded
2025-11-25 19:31:10	Investigation	Risk: 0.43	benign
2025-11-25 19:30:21	Response	log_only	recorded
2025-11-25 19:30:21	Investigation	Risk: 0.46	benign
2025-11-25 19:29:32	Response	log_only	recorded
2025-11-25 19:29:32	Investigation	Risk: 0.40	benign
2025-11-25 19:28:47	Alert	From 10.0.0.5	medium
2025-11-25 19:28:46	Alert	From 10.0.0.5	low
2025-11-25 19:28:45	Alert	From 10.0.0.5	medium
2025-11-25 19:28:44	Alert	From 10.0.0.5	medium
2025-11-25 19:28:43	Alert	From 10.0.0.5	medium

Recommendations

Security Recommendations:

• **High Alert Volume:** Consider reviewing detection thresholds and implementing additional network segmentation to reduce attack surface.

• **Continuous Monitoring:** Maintain 24/7 monitoring and ensure all security patches are up to date across the infrastructure.

• **Incident Response:** Review and update incident response playbooks based on observed attack patterns.

• **Training:** Conduct security awareness training for all personnel to reduce social engineering risks.

• **Backup & Recovery:** Verify backup systems are functioning and test recovery procedures regularly.