Weekly Security Operations Report

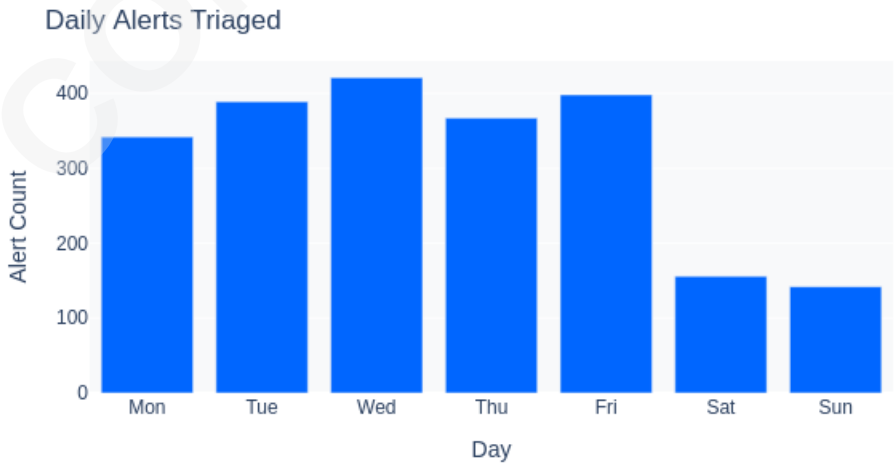
Week of December 07, 2025

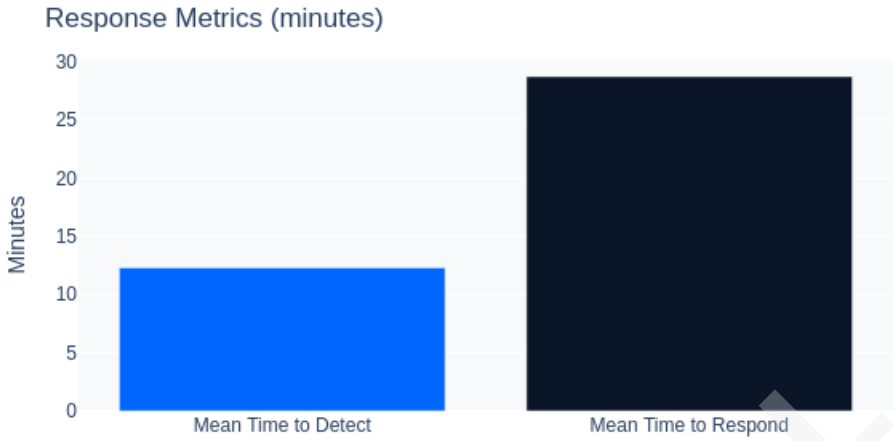
Executive Summary

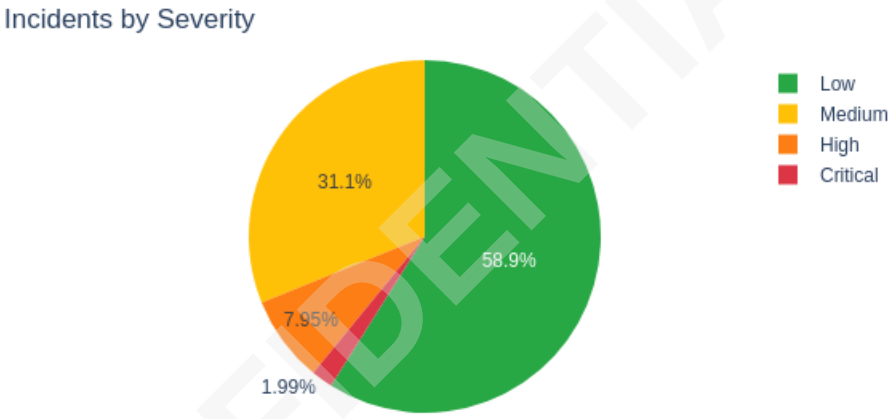
This week, the BlueCyber Security Operations Center processed 2,215 security alerts across all monitored environments. Our team detected and responded to 151 security incidents, with 3 classified as critical severity. Mean time to detect (MTTD) improved by 8% to 12.3 minutes, while mean time to respond (MTTR) decreased to 28.7 minutes. No successful breaches occurred, and all critical incidents were contained within SLA requirements.

Weekly Metrics Dashboard

Metric	This Week	Last Week	Change
Total Alerts	2,215	2,089	+6.0%
Incidents Detected	151	147	+2.7%
Critical Incidents	3	5	-40.0%
MTTD (minutes)	12.3	13.4	-8.2%
MTTR (minutes)	28.7	31.2	-8.0%
False Positive Rate	23.4%	25.1%	-1.7%







Top Incidents Summary

ID	Severity	Type	Status	MTTR
INC-2847	Critical	Malware Detection	Resolved	18 min
INC-2851	Critical	Unauthorized Access	Resolved	34 min
INC-2856	Critical	Data Exfiltration Attempt	Resolved	42 min
INC-2849	High	Phishing Campaign	Resolved	27 min
INC-2853	High	Brute Force Attack	Resolved	15 min

Threat Intelligence Highlights

- **Emerging Threat:** New ransomware variant "DarkVault 2.0" detected targeting healthcare sector
- **CVE Alert:** Critical vulnerability CVE-2024-XXXXX in widely-used VPN software - patches deployed

• **Campaign Activity:** Increased phishing attempts spoofing Microsoft 365 login pages
• **Geopolitical:** Elevated APT activity from state-sponsored groups targeting defense contractors

Action Items & Recommendations

1. **Immediate:** Review and update email filtering rules to address new phishing campaign patterns
2. **This Week:** Conduct tabletop exercise for ransomware response procedures
3. **Ongoing:** Continue monitoring for DarkVault 2.0 indicators of compromise
4. **Strategic:** Evaluate additional EDR coverage for remote workforce endpoints