Security Metrics and Executive Reporting

Prepared by: Mr. Chandan Prasad
Position: SOC Analyst Intern
Company: CYART Tech

Part 1: Metrics Dashboard - Elastic Security

Key Performance Indicators (KPIs)

MTTD (Mean Time To Detect)

- Definition: Average time from when an attack starts to when we detect it
- Current Value: 45 minutes
- Target: 30 minutes
- Status: Above target (needs improvement)

MTTR (Mean Time To Respond)

- Definition: Average time from detection to when we contain the threat
- Current Value: 1 hour 30 minutes
- Target: 1 hour
- Status: Slightly above target

MTTI (Mean Time To Investigate)

- Definition: Average time to complete investigation after detection
- Current Value: 2 hours
- Target: 3 hours
- Status: Better than target ✓

False Positive Rate

- Definition: Percentage of alerts that are not real threats
- Current Value: 8%
- Target: 5%
- Status: Above target (too many false alarms)

Alert Volume

- Total alerts per day: 247
- High severity alerts: 18
- Medium severity alerts: 64

- Low severity alerts: 165

Dashboard Metrics Table

Metric	Current	Target	Status	Trend
MTTD	45 min	30 min	⚠ Above	→ Stable
MTTR	90 min	60 min	⚠ Above	↗ Improving
MTTI	120 min	180 min	✓ Good	↘ Improving
False Pos Rate	8%	5%	⚠ Above	↗ Worsening
Alert Volume	247/day	200/day	⚠ High	↗ Increasing
Detection Rate	85%	90%	⚠ Below	→ Stable
Dwell Time	2.5 hours	2 hours	⚠ Above	→ Stable
Incident Severity	Medium	Low	⚠ Above	→ Stable

Monthly Trend Analysis

November 2025 Metrics:

Week	MTTD	MTTR	False Pos	Incidents
Week 1	50 min	95 min	10%	8
Week 2	48 min	92 min	9%	12
Week 3	45 min	88 min	8%	15
Week 4	42 min	85 min	7%	18

Trend: Improving detection and response times, but false positive rate needs attention.

Part 2: Executive Summary Report

CYART Tech SOC Performance Summary

During November 2025, our Security Operations Center detected and responded to 47 security incidents with an average detection time of 45 minutes and response time of 90 minutes. While response capabilities improved throughout the month, we identified two critical areas requiring investment: detection latency and alert accuracy.

Our current false positive rate of 8% creates alert fatigue, consuming analyst resources on non-threats. We recommend implementing machine learning-based alert correlation to reduce false positives to 5%. Additionally, our detection time exceeds the 30-minute target, suggesting gaps in real-time monitoring capabilities.

Key achievements include maintaining 85% detection rate and zero successful breaches. Recommendations include deploying behavioral analytics, expanding network monitoring, and conducting quarterly red team exercises. These investments will reduce detection time to 30 minutes, lower false positives to 5%, and improve overall incident response efficiency by 35%.

Part 3: Dwell Time Analysis

What is Dwell Time?

Dwell time is the time between when an attacker first compromises a system and when we fully contain the threat. Shorter dwell time means less damage.

Mock Incident Analysis

Incident: Phishing email with malware attachment

Phase	Start Time	End Time	Duration	Notes
Attack Initiation	08:00	-	-	Phishing email sent to employees
Initial Compromise	08:15	-	15 min	User opens email and downloads attachment
Malware Execution	08:25	-	10 min after download	File executed, malware installed
First Alert	08:35	-	35 min	Suspicious process detected by Wazuh
Investigation	08:35	09:00	25 min	SOC analyst investigates alert
Containment	09:00	09:15	15 min	Isolate affected computer from network
Eradication	09:15	10:00	45 min	Remove malware, reset credentials
Full Recovery	10:00	11:00	60 min	Verify system clean, restore to service

Dwell Time Calculation

- Attack Start: 08:00
- Full Containment: 09:15
- Total Dwell Time: 1 hour 15 minutes

Impact Analysis

Stage	Potential Impact	Actual Impact	Prevention
Initial Compromise	Email account compromise	1 email account	Email filtering
Malware Execution	Full system compromise	Limited to user profile	Endpoint protection
Undetected Time	Data exfiltration	0 bytes	Real-time monitoring
Post-Containment	Lateral movement	Prevented by isolation	Network segmentation

Dwell Time Summary

Attack detection took 35 minutes from initial compromise. Containment was achieved in 75 minutes total dwell time. This exceeded our 60-minute target by 15 minutes, primarily due to investigation time. Quick alert detection prevented data exfiltration and lateral movement. With improved automation, we can reduce investigation time from 25 minutes to 10 minutes, achieving 60-minute dwell time target.

Part 4: Incident Statistics

Incident Types (November 2025)

Incident Type	Count	Percentage	Avg MTTD	Avg MTTR
Phishing	18	38%	30 min	60 min
Malware	12	26%	45 min	90 min
Brute Force	10	21%	50 min	45 min
Misconfiguration	5	11%	120 min	180 min
Other	2	4%	60 min	120 min

Severity Distribution

Severity	Count	Percentage	Avg MTTR
Critical	3	6%	45 min

Severity	Count	Percentage	Avg MTTR
High	15	32%	75 min
Medium	22	47%	105 min
Low	7	15%	240 min

Part 5: Performance Benchmarks vs Industry Standards

Metric	CYART Tech	Industry Standard	Gap
MTTD	45 min	30 min	-15 min (worse)
MTTR	90 min	60 min	-30 min (worse)
False Positive Rate	8%	5%	-3% (worse)
Detection Rate	85%	90%	-5% (worse)
Dwell Time	75 min	60 min	-15 min (worse)

Analysis: CYART Tech is performing below industry standards across all metrics. Investment in tooling and training is recommended.

Part 6: Recommendations for Improvement

Short-term (Next 30 days)

1. Tune Alert Thresholds - Reduce false positives from 8% to 6% by adjusting sensitivity
2. Add Real-time Rules - Deploy 5 new detection rules for common attacks
3. Improve Playbooks - Automate investigation steps to reduce MTTR by 20%
4. Staff Training - Conduct training on new tools and techniques

Medium-term (60-90 days)

1. Deploy Behavioral Analytics - Implement ML-based detection to reduce false positives to 5%
2. Expand Network Monitoring - Add DNS and network flow monitoring
3. Implement SOAR - Automate response playbooks for faster containment
4. Threat Intelligence Integration - Better feed quality and correlation

Long-term (6 months)

1. Red Team Exercises - Quarterly simulations to test detection capabilities

2. Threat Hunting Program - Proactive search for undetected threats
3. Advanced Analytics - Predictive analytics for threat forecasting
4. 24/7 Coverage - Expand SOC staffing for round-the-clock monitoring

Part 7: Budget Impact Analysis

Investment Requirements

Initiative	Cost	Expected ROI	MTTD Impact	MTTR Impact
Alert Tuning	$5K	300%	-5 min	-10 min
New Detection Rules	$10K	250%	-10 min	-5 min
Playbook Automation	$15K	200%	0 min	-30 min
Behavioral Analytics	$50K	180%	-10 min	-15 min
SOAR Platform	$75K	150%	0 min	-45 min
Total	$155K	196%	-25 min	-105 min

Expected Outcome: Reduce MTTD from 45 to 20 minutes, reduce MTTR from 90 to 45 minutes.

Part 8: Risk Assessment

Current Risk Level: MEDIUM

Key Risks:

1. Slow detection enables data theft (HIGH)
2. High false positive rate causes alert fatigue (MEDIUM)
3. Manual processes slow response (MEDIUM)
4. Detection gaps in network layer (HIGH)
5. Insufficient staffing for growth (MEDIUM)

Risk Mitigation: Implementing recommendations above will reduce risk level to LOW within 6 months.

Conclusion

CYART Tech SOC is performing below industry standards, with detection times and false positive rates requiring improvement. Investment in automation, analytics, and staffing is recommended. With implementation of proposed initiatives, we project a 55% improvement in MTTD and 50%

improvement in MTTR, bringing CYART Tech to industry-leading performance levels.

Appendix: Glossary

- MTTD: Mean Time To Detect - average detection time
- MTTR: Mean Time To Respond - average containment time
- MTTI: Mean Time To Investigate - average investigation time
- False Positive Rate: Percentage of non-threat alerts
- Dwell Time: Time from compromise to full containment
- Detection Rate: Percentage of actual attacks detected
- Alert Fatigue: Analyst burnout from too many false alerts

Report prepared by: Mr. Chandan Prasad, SOC Analyst Intern, CYART Tech