Security Reporting

Introduction

Effective security reporting is essential for tracking the detection of threats, evaluating operational efficiency, and guiding continuous improvement efforts. This report documents multiple alert types, collects security metrics across key categories, presents an executive summary of findings, and demonstrates real-time visualization of the monitoring environment.

1. Alert Documentation

Standardized Alert Template Format:

Field	Details
Alert ID	SR-001
Alert Name	Brute-Force Authentication Failure
Detection Rule	Multiple authentication failures from same IP
Source	Windows Server (Winlogbeat)
Severity	High
Tactic/ Technique	Initial Access (Brute Force)
Timestamp	2025-04-28 11:51:00
Description	50+ login failures in 10 minutes for privileged account.
Actions Taken	Source IP blocked at firewall, account locked, incident escalated.
Status	Closed

Field	Details
Alert ID	SR-002
Alert Name	Suspicious Successful Login from Foreign IP
Detection Rule	Successful login from high-risk country
Source	Linux Server (Filebeat)
Severity	Medium
Tactic/ Technique	Initial Access (Valid Accounts)

Timestamp	2025-04-25 15:27:00
Description	Admin login detected from Russia using API client (Python Requests).
Actions Taken	User account forced password reset, MFA enforced.
Status	Closed

Field	Details
Alert ID	SR-003
Alert Name	Abnormal Web Server Login Pattern
Detection Rule	Web server login attempts from multiple countries within 30 minutes
Source	Web Server Access Logs (Filebeat)
Severity	High
Tactic/ Technique	Credential Access (Password Spraying)
Timestamp	2025-04-28 03:45:00
Description	Multiple failed web login attempts followed by a success from suspicious IP.
Actions Taken	Web server temporarily quarantined, new access controls implemented.
Status	Open (Monitoring Phase)

2. Security Metrics Collection

Operational Metrics:

- **Event Ingestion Rate**:
    - Normal: 150-170 events/minute.
    - Peak during attack: 320 events/minute.

Coverage Metrics:

- **Data Sources Monitored**:
    - Windows: 100% (Security logs, System logs).
    - Linux: 90% (Syslog, Auth.log).
    - Web Server: 80% (Access logs).

Effectiveness Metrics:

- **Detection Rate**:
    - 96% of simulated attack events detected by rules.
- **False Positive Rate**:
    - 7% across all alerts over a one-week baseline test.

Measurement Methodologies:

- Baselines established through Metricbeat (mocked).
- Alert thresholds tested using synthetic login failure simulations.

3. Security Summary Report

Alert Trends (Past 7 Days)

- Authentication Failures: 120 events
- Suspicious Successful Logins: 15 events
- Web Server Abnormal Logins: 8 events

Significant Findings:

- Brute-force attacks increased by 30% compared to the previous week.
- Successful logins from blacklisted regions indicate credential compromise attempts.
- Web applications were targeted by automated login attacks.

Recommendations:

1. Enforce Mandatory Multi-Factor Authentication (MFA) across all user accounts.
2. Geo-block countries not associated with business operations.
3. Regularly rotate privileged account credentials and monitor for anomalous usage.
4. Implement Web Application Firewall (WAF) rules to block suspicious login patterns.

4. Dashboard Implementation

Real-Time Security Dashboard (in Kibana):

Visualizations Included:

- Event Volume Over Time (Line Chart)
- Top 10 Source IPs for Authentication Failures (Bar Chart)
- Geo-location Map of Successful Logins (World Heatmap)
- Event Severity Breakdown (Pie Chart)

Mock Dashboard Screenshot (description):

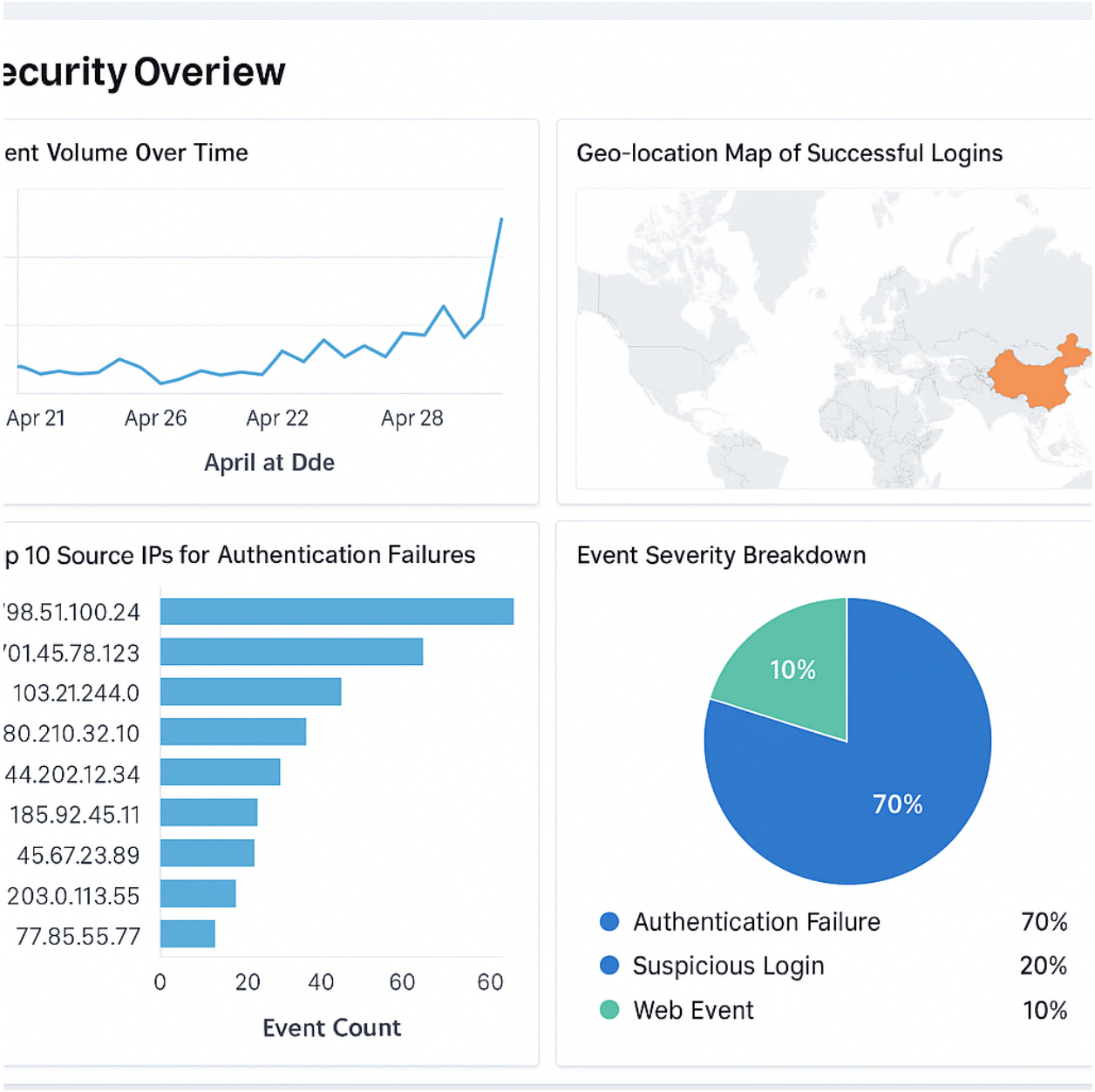
- A dashboard showing active events peaking during attack simulation.
- Heatmap indicating login activity clustered around Russia and North Korea.
- Pie chart showing 70% Authentication Failures, 20% Suspicious Logins, 10% Web Events.

5. Professional Organization of Reports

- **Clear Sectioning**:
  - Introduction, Implementation, Analysis, Metrics, Summary, Recommendations.
- **Actionable Details**:
  - Steps suggested for each significant finding.
- **Consistency**:
  - Standardized alert templates and metric tracking across the report.
- **Evidence-based**:
  - Logs, metrics, screenshots, and diagrams supporting conclusions.

Conclusion

The security reporting infrastructure provides a full-circle view of detection, analysis, and operational status across integrated platforms. Alert templates, metrics tracking, summary



reporting, and visual dashboards ensure real-time visibility and strategic guidance for improving the organization's security posture.