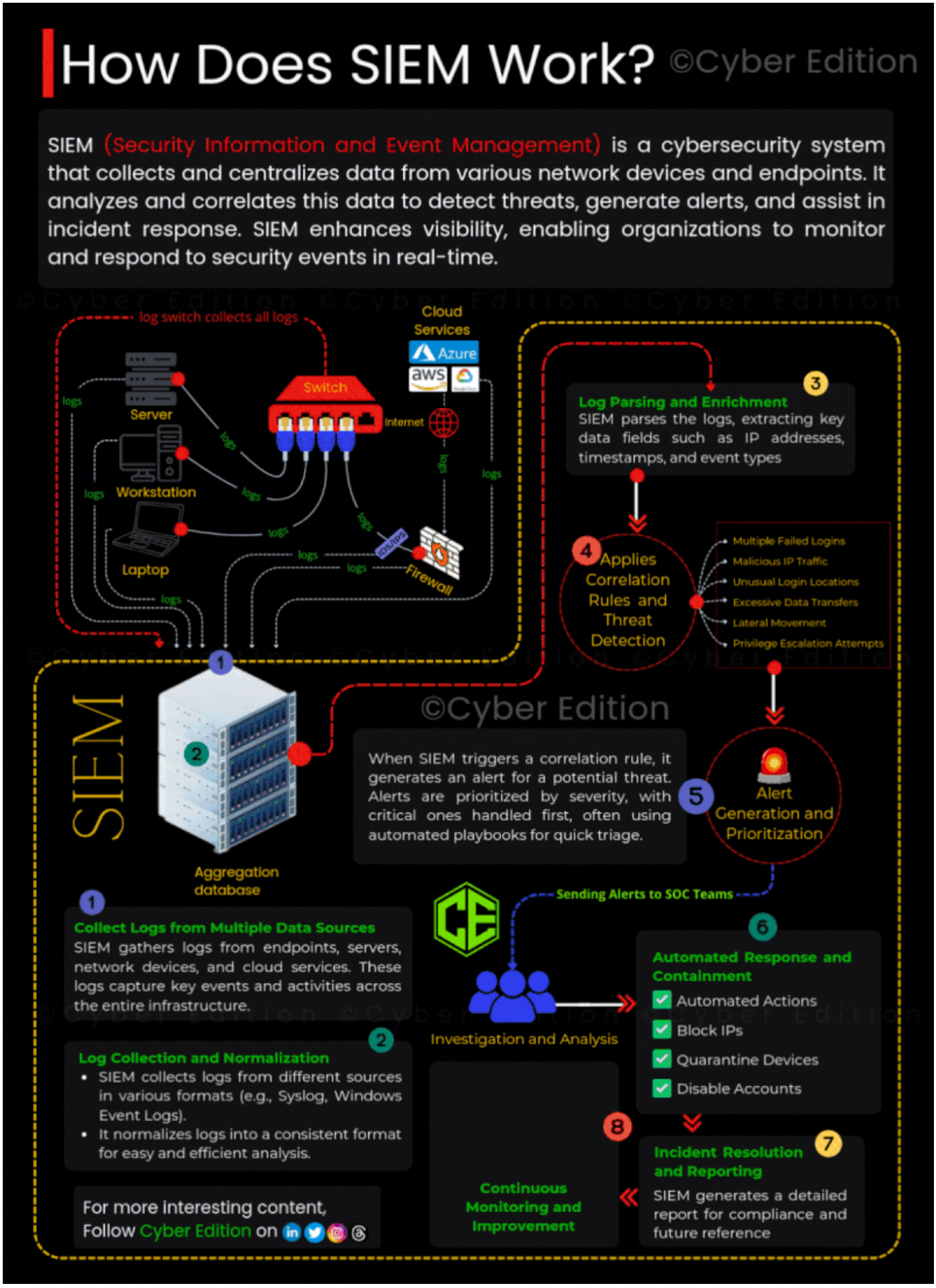
SIEM


How Does SIEM Work? ©Cyber Edition
SIEM (Security Information and Event Management) is a cybersecurity system that collects and centralizes data from various network devices and endpoints. It analyzes and correlates this data to detect threats, generate alerts, and assist in incident response. SIEM enhances visibility, enabling organizations to monitor and respond to security events in real-time.
log switch collects all logs
Cloud Services
Azure
aws
Switch
Internet
Server
Workstation
Laptop
Firewall
logs
logs/IPS
SIEM
Aggregation database
©Cyber Edition
1 Collect Logs from Multiple Data Sources
SIEM gathers logs from endpoints, servers, network devices, and cloud services. These logs capture key events and activities across the entire infrastructure.
2 Log Collection and Normalization
SIEM collects logs from different sources in various formats (e.g., Syslog, Windows Event Logs).
It normalizes logs into a consistent format for easy and efficient analysis.
3 Log Parsing and Enrichment
SIEM parses the logs, extracting key data fields such as IP addresses, timestamps, and event types
4 Applies Correlation Rules and Threat Detection
Multiple Failed Logins
Malicious IP Traffic
Unusual Login Locations
Excessive Data Transfers
Lateral Movement
Privilege Escalation Attempts
5 Alert Generation and Prioritization
When SIEM triggers a correlation rule, it generates an alert for a potential threat. Alerts are prioritized by severity, with critical ones handled first, often using automated playbooks for quick triage.
Sending Alerts to SOC Teams
Investigation and Analysis
6 Automated Response and Containment
Automated Actions
Block IPs
Quarantine Devices
Disable Accounts
7 Incident Resolution and Reporting
SIEM generates a detailed report for compliance and future reference
8 Continuous Monitoring and Improvement
For more interesting content, Follow Cyber Edition on