VCS One Security

Technical Architecture Guide

Threat Detection Architecture

AI/ML Threat Detection Engine

Behavioral analysis models, anomaly detection algorithms, threat classification, and risk scoring engine.

Detection Capabilities:

- **Behavioral Analysis:** User and entity behavior analytics (UEBA) with baseline establishment and deviation detection
- **Anomaly Detection:** Statistical and ML-based anomaly detection with adaptive thresholds and unsupervised learning
- **Threat Classification:** Automated categorization of threats by severity, type, and potential impact
- **Risk Scoring:** Intelligent risk prioritization with business context and asset criticality weighting

Real-Time Log Analysis

SIEM integration, log aggregation, pattern matching, and correlation rules for comprehensive security monitoring.

Log Analysis Features:

- **SIEM Integration:** Native connectors for Splunk, QRadar, ArcSight, and cloud-native solutions
- **Log Aggregation:** Centralized collection from diverse sources with normalization
- **Pattern Matching:** Regex and machine learning-based pattern detection
- **Correlation:** Multi-event correlation rules for attack pattern recognition

Behavioral Analytics

Advanced user behavior analysis with baseline establishment and risk profiling.

Behavioral Features:

- **UBA:** User behavior analytics to detect insider threats and compromised accounts
- **Baseline:** Machine learning-based normal behavior establishment
- **Deviation:** Detection of unusual patterns and anomalous activities
- **Profiling:** Risk scoring based on behavioral patterns and history

Network Traffic Monitoring

Deep packet inspection, flow analysis, and intrusion detection for network security.

Network Monitoring:

DPI: Deep packet inspection for protocol analysis and content filtering

Flow Analysis: NetFlow and IPFIX analysis for traffic pattern detection

IDS: Intrusion detection with signature-based and anomaly-based detection

DDoS Protection: Distributed denial-of-service attack mitigation and rate limiting

Endpoint Protection

Agent-based monitoring, file integrity checking, and application control.

Endpoint Security:

Agent-Based: Lightweight agents for Windows, Linux, macOS monitoring

File Integrity: Real-time file system monitoring with integrity checks

Application Control: Whitelisting and blacklisting for application execution

Memory Protection: Runtime protection against memory-based attacks

Threat Intelligence Feeds

Global IOC databases, threat research integration, and automated IOC matching.

Intelligence Features:

IOC Databases: Integration with global threat intelligence feeds and STIX/TAXII

Threat Research: Research integration for emerging threats and vulnerabilities

Auto-Matching: Automated IOC matching with confidence scoring

Reputation: Domain, IP, and file reputation scoring

Compliance Automation

PDPA Compliance Framework

Personal data identification, consent management, data subject rights, and breach notification automation.

PDPA Features:

- **Data Identification:** Automated detection and classification of personal data
- **Consent Management:** Tracking and management of user consents with automated workflows
- **Subject Rights:** Automated handling of access, rectification, and deletion requests
- **Breach Notification:** Automated regulatory notifications within required timeframes

ISO 27001 Control Mapping

Information security controls, risk management, security awareness, and incident management.

ISO 27001 Controls:

- **Access Control:** Logical and physical access controls with role-based permissions
- **Cryptography:** Encryption policies and key management procedures
- **Operations Security:** Network security, malware protection, backup procedures
- **Incident Management:** Security incident response procedures and documentation

HIPAA Security Requirements

Protected health information (PHI) protection, access controls, audit logging, and business associate agreements.

HIPAA Controls:

- **PHI Protection:** Encryption and access controls for protected health information
- **Access Management:** User authentication, authorization, and session management
- **Audit Logging:** Comprehensive audit trails for all PHI access and modifications
- **BAAs:** Business associate agreements and risk assessments

Continuous Compliance Monitoring

Real-time control assessment, automated evidence collection, drift detection, and remediation tracking.

Monitoring Features:

Real-Time Assessment: Continuous evaluation of control effectiveness and compliance status

Evidence Collection: Automated artifact gathering for audit readiness

Drift Detection: Configuration drift detection and alerting

Remediation: Automated remediation workflows and tracking

Integration APIs

SIEM Integration

Splunk, QRadar connectors with log forwarding, event correlation, and dashboard creation.

SIEM Configuration:

- **Log Sources:** Configure log sources for Windows, Linux, network devices, applications
- **Forwarding:** Real-time log forwarding with compression and filtering
- **Correlation:** Build correlation rules for multi-stage attack detection
- **Dashboards:** Create operational and executive dashboards with key metrics

Identity Providers

Okta, Azure AD SSO with user provisioning, MFA integration, and conditional access.

Identity Setup:

- **SSO Configuration:** SAML/OAuth setup for seamless authentication
- **Provisioning:** SCIM-based automated user lifecycle management
- **MFA:** Multi-factor authentication with backup methods
- **Conditional Access:** Risk-based access policies and device compliance

Ticketing Systems

Jira, ServiceNow integration with automated ticket creation, status synchronization, and SLA tracking.

Cloud Security APIs

AWS Security Hub, Azure Security Center, GCP Security Command Center, and CloudTrail integration.

Cloud Integration:

- **AWS:** Security Hub findings, CloudTrail events, GuardDuty alerts, and config compliance checks
- **Azure:** Security Center recommendations, Sentinel integration, Activity logs, and Azure AD logs
- **GCP:** Security Command Center findings, Cloud Audit logs, Cloud Asset Inventory, and VPC Flow logs

Incident Response Architecture

Automated Playbooks

Structured procedures, decision trees, containment automation, and recovery workflows.

Playbook Features:

- **Structured Procedures:** Step-by-step response workflows with decision branches
- **Decision Trees:** Automated decision-making based on threat characteristics
- **Containment:** Automated network isolation, account suspension, and system quarantine
- **Recovery:** Automated restoration workflows with validation steps

Multi-Team Coordination

Incident orchestration, role assignment, communication workflows, and escalation procedures.

Coordination Features:

- **Orchestration:** Multi-team incident management with role-based assignments
- **Communication:** Automated notification workflows via email, Slack, Teams, SMS
- **Escalation:** Automated escalation to management based on severity and timeline

Investigation Workflow

Timeline reconstruction, evidence collection, forensic analysis, and root cause determination.

Post-Incident Analysis

Automated incident report generation, lessons learned capture, and improvement recommendations.

Security Architecture

Encryption Standards

AES-256 for data at rest, TLS 1.3 for data in transit, key management (HSM), and certificate management.

Encryption Implementation:

- **Data at Rest:** AES-256 encryption for databases, file systems, and backups
- **Data in Transit:** TLS 1.3 for all network communications with certificate pinning
- **Key Management:** Hardware security modules (HSM) for secure key storage and rotation
- **Certificates:** Automated certificate lifecycle management with monitoring

Zero-Trust Network Architecture

Micro-segmentation, identity-based access, continuous verification, and least privilege enforcement.

Zero-Trust Implementation:

- **Network Segmentation:** Micro-segmentation with software-defined perimeters
- **Identity-Based Access:** Every access request verified regardless of location
- **Continuous Verification:** Ongoing authentication and authorization checks
- **Least Privilege:** Granular permissions with just-in-time access escalation

Advanced Security Controls

Identity and Access Management

Role-based access control, privileged access management, just-in-time access, and session management.

IAM Features:

- **RBAC:** Role-based access control with permission inheritance
- **PAM:** Privileged access management for administrative accounts
- **JIT Access:** Just-in-time access with approval workflows
- **Session Management:** Active session monitoring with automatic termination

Vulnerability Scanning

Automated scanning, asset discovery, risk prioritization, and patch management.

Vulnerability Management:

- **Scanning:** Automated vulnerability scans with credentialed access
- **Discovery:** Continuous asset discovery and inventory management
- **Prioritization:** Risk-based vulnerability prioritization with CVSS scoring
- **Patching:** Automated patch deployment with testing workflows

Penetration Testing

Authorized testing, vulnerability validation, exploit demonstration, and remediation verification.

Testing Features:

- **Authorized Testing:** Scheduled and on-demand penetration tests with scope definition
- **Vulnerability Validation:** Manual testing to validate automated scan results
- **Exploit Demonstration:** Proof-of-concept exploits to assess business impact
- **Remediation:** Verification of security fixes and re-testing procedures

Additional Security Controls

Audit Trail Generation

Comprehensive logging and audit trails for compliance and forensic investigations.

Audit Features:

- **Immutability:** Tamper-proof audit logs with cryptographic integrity
- **Retention:** Configurable retention policies with archival capabilities
- **Search:** High-performance log search and analytics
- **Reporting:** Automated compliance report generation

Security Controls Summary

Comprehensive security controls across all layers of the architecture.

Control Summary:

- **Network:** Firewalls, segmentation, DDoS protection, and intrusion prevention
- **Application:** Web application firewalls, API security, and input validation
- **Data:** Encryption, masking, backup encryption, and secure deletion
- **Identity:** MFA, SSO, password policies, and account lockout

Enterprise-Grade Security

Contact VCS for Security Assessment

Value Creating Solutions Sdn Bhd