SIEM Use Cases Development – Approach & Methodology Version 1.2

Enterprise Technology Specialists | SIEM, ATD, TIE | APAC

Use Case	Data Sources & Contexts	Events of Interest (EOI)	Incident Management / Metrics	Dependency
(1) Malware Control Centralize malware monitoring, incident responses, assessing and reporting operational impacts from end point to perimeter with regard to ensuring activation and standard use, monitoring and reviewing malware activity, and most importantly, responding to issues.	- Anti-Malware, Virus & Trojan - Spam Filtering - Web Security Controls - DNS - IPS/IDS Systems - Vulnerability Assessment - Integrity Checking Control - Network Flow - Firewalls - Email Security - Sandboxing Controls - Internal Threat Intelligence - External Threat Intelligence - Critical Hosts, Apps, DB	- Malware Detected, Remediated - Malware attack sources/ Destinations - Virus Detected, remediated - Spam Detected, Removed - Phishing Detected - Hosts with Infection or reinfections - Suspicious or Malicious Activities by sources/destinations - Anomalous or unusual Users/Hosts (src/dst) activities - Suspicious email or web traffic - Endpoint Protection start, stop, update failure - IOC - Bad IP, File Hash, URL - Correlated events	1. Initial & Advance EOI security analysis/Triage 2. Internal/External Intelligence Analysis & Correlation 3. Escalation and Notification (Alarms) 4. Reports (Detect, Protect, Response) 5. Response Actions (contain, remove) 6. Post Incident analysis & Activities	**Minimum:** - Adequate Core SIEM Infrastructure & Sizing (i.e. ETM, Receivers, ACE) - Endpoint Protection Controls **Additional Tools & Contexts:** - Assets characterisation, - Variables, Zones, Tags reflecting critical environment and parameters - Watch Lists, Alarms - Baseline - Data Enrichment - Geo Location Awareness - Application Data Monitoring - Network Flow Data Monitoring - Sandbox (static/Dynamic analysis) - Threat Intelligence sharing - Hunting & Response Automation tools

Use Case	Data Sources & Contexts	Events of Interest (EOI)	Incident Management / Metrics	Dependency
(2) Suspicious/Malicious User Activities (Access Control) Monitor and report on key status, violations, anomalous, suspicious and malicious access to critical resources.	- Directory Services - LDAP Services - AAA Services - RADIUS - Host OS logs - Firewalls, VPN - Proxy Systems - Physical security device logs - Integrity Checking Controls - Database Security Controls - Wireless Access Controller - Critical Hosts, Apps, DB -	- Access failures (source, destination, user, business unit) - Access failure (prioritized logical grouping) - Anomalous or unusual access by users/groups - Login success & failure; user, system, device class, time - Multiple logons from different geos - Suspicious access attempts or failure followed by success from same source - Privileged user access by access failure, by critical resource, by method, by different location/same time - Privileged user access follow by configuration changes - Administrative changes to directory service user and group objects; by admin, by user, by group, by resource criticality - Use of trusted and service accounts, by volume, by time of day, by domain - User activations, privilege change and terminations by device class - Remote access login success and failure (VPN, other); by user, by device class, by time with details - Unusual service account, terminated account use, login success and failures - Admin accounts with failed logons - IOC - Bad IP, File Hash, URL - Correlated events	1. Initial & Advance EOI security analysis/Triage 2. Internal/External Intelligence Analysis & Correlation 3. Escalation and Notification (Alarms) 4. Reports (Detect, Protect, Response) 5. Eradication Response Actions (contain, remove) 6. Post Incident analysis & Activities	**Minimum:** - Adequate Core SIEM Infrastructure: & Sizing (i.e. ETM, Receivers, ACE) - A Directory or AAA Service **Additional Tools & Context:** - Assets characterisation, - Variables, Zones, Tags reflecting critical environment and parameters - Watch Lists, Alarms - Baseline - Data enrichment - Geo Location Awareness - Application Data Monitoring - Database Security Monitoring - Threat Intelligence sharing - Hunting & Response Automation tools

Use Case	Data Sources & Contexts	Events of Interest (EOI)	Incident Management / Metrics	Dependency
(3) Boundary Defence Monitoring Monitoring of access activity from various boundary defences such as firewalls, routers, VPNs and other network resources as well as cross-correlating network flows with other operational data to identify suspicious/malicious behaviour and threats.	- VPN - Firewall, NAT - IPS/IDS - Proxy - Routers - NAC - Wireless AP - Network flow - RADIUS, AAA - RAS - Configuration Assessment - Domain Controller - Critical Hosts, Apps, DB - All network devices	- Access failures by source and destination - Inbound connections to internal sources by system, user and time - Outbound connections to external sources by system, user, and time - Outbound DMZ connections to external sources by system, user and time - Perimeter attacks by category - Dropped traffic from DMZ, FW - Blocked internal sources by port, by destinations - Blocked outbound connections by port, by destination - Unusual DNS access and requests - Changes to active and standby configurations by perimeter device class - Connections from sites of concerns - Unusual peak utilization sources and destination - Network Traffic by protocol, by connection, by source, by destination - Configuration changes FW, VPN, WAP, Domain - Failure FW, VPN, WAP, Domain - Multiple login failures by FW, VPN, Domain - Wireless network access by location, by user, by failed attempts - IOC - Bad IP, File Hash, URL - Correlated events	1. Initial & Advance EOI security analysis/Triage 2. Internal/External Intelligence Analysis & Correlation 3. Escalation and Notification (Alarms) 4. Reports (Detect, Protect, Response) 5. Eradication Response Actions (block, contain, remove) 6. Post Incident analysis & Activities	**Minimum:** - Adequate Core SIEM Infrastructure: & Sizing (i.e. ETM, Receivers, ACE) - A key gateway security control in data source column **Additional Tools & Context:** - Assets characterisation, - Variables, Zones, Tags reflecting critical environment and parameters - Watch Lists, Alarms - Baseline - Data enrichment - Geo Location Awareness - Application Data Monitoring - Database Security Monitoring - Threat Intelligence sharing - Hunting & Response Automation tools - Sandboxing

Use Case	Data Sources & Contexts	Events of Interest (EOI)	Incident Management / Metrics	Dependency
(4) PCI Compliance & Audit Continuous monitoring of user and system access to PCI resources, suspicious & malicious software activities across PCI zones, infrastructure controls supporting PCI compliance mandates, configuration changes, infrastructure segregation, identity management, resource access, incidents management and investigations.	Common PCI Data sources are : - PCI Firewalls - PCI IPS/IDS - PCI Core Routers, Switches & Wireless LAN (Netflow data) - PCI Hosts OS, Apps, DB logs - PCI Database Activity Monitoring - PCI Application Activity Monitoring - Host based Integrity Checking Controls - Active Directory (LDAP) Controls - Configuration Management & Assessment controls - HIPS/NISP Controls - Encryption Control - Vulnerability Assessment Controls - Identity Management - Physical Access Controls - Other specific PCI security & compliance control applicable for monitoring (i.e. PAN protection, DLP, etc…)	- Unauthorised PCI inbound/outbound network traffic - Unencrypted CHD transmission across restricted networks - Resources access with subsequent configuration changes outside of approved change windows - Unauthorized changes on critical PCI assets (TBD) - NTP setting changes events - Deleting logs events - Audit Log setting changed on PCI asset (disabled) event - Default or weak user name and passwords - Unauthorised services used across the PCI zones & assets - Expected security controls are running (status: start/stop) - Endpoint security services is running - AV Signature & rules are updated - Endpoint Protection Status (Stop, Start) events - Unauthorised storage of CHD - Unauthorized access to CHD - User Activity (Unique ID) event on PCI asset - Access to & use of PCI zone assets - PCI Privileged User and System level accounts event - Unauthorized physical access to PCI Asset - Other WOW/DD PCI correlated events (TBD) -	- Daily alerts, monthly reports and quarterly reviews of materials - PCI classified asset threats, Risk and vulnerability - PCI violations and respective Alarms/Case/events references - Refined dashboards, views and reports to support PCI audits & management visibility - Time range of available monitoring & logging records to support retention requirements - Log data types, retention time, rotation & archival date & time - PCI Alarms and Incidents - Log Integrity check (ELM)	**Minimum:** - Adequate Core SIEM Infrastructure: & Sizing (i.e. ETM, Receivers, ACE, ELM) - Application Data Monitoring (ADM), Netflow - Database Security Monitoring (DEM, DAM, etc…) **Additional Notes:** - It is best to establish a matrix of compliance requisites and SIEM “proof points.” - Distribution of PCI Applications , Servers and infrastructure - PCI Incident Severity Definition & Incident Response processes - PCI Zone Definitions (Asset Grouping, Criticality, tagging, variables) - Internal and External Storage Devices - Logical Storage pools aligned with WOW PCI compliance audit requirements - ELM Log Archiving (DB, Indexing, Raw log Organization)

SIEM Use Cases Development – Approach & Methodology Version 1.2

Enterprise Technology Specialists | SIEM, ATD, TIE | APAC