Common Criteria Evaluation and Validation Scheme

National Information Assurance Partnership (NIAP)

Title: Enterprise Security Management (ESM) - Enterprise Management (EM)

Maintained by: National Information Assurance Partnership (NIAP)

Unique Identifier: 00x

Version: 0.2x

Status: draft

Date of issue:

Approved by:

Supersedes:

Background and Purpose

This document describes a core set of security requirements for Enterprise Security Management systems. These requirements cover basic security characteristics and behaviors for an ESM management server.

The intent is that the remaining sections provide succinct statements that highlight the relevant aspects to be addressed by the Technical Community (TC) constructing the PP. Here, the authors provide a narrative that introduces the reader to the problem being solved, and presents key aspects that support or guide the TC, and may elaborate on subtleties not apparent in the “bulleted” high level statements.

Use Cases

[USE CASE] **Monitoring and Management**

[USE CASE 1] Custom Events

The ability to handle custom event management and monitoring across server and workstation endpoints.

[USE CASE 2] Standard Services and Alerts

The ability to monitor multiple system services across endpoints, such as alerting for low disk space, high memory usage alerts, account creations, accounts being added or removed from groups, services stopping.

[USE CASE 3] Patching and Policies

The ability to deploy patches, security, and business policies to server and workstation endpoints, in addition to deploying instructions to network configurable infrastructure devices.

[USE CASE 4] Discovery

The capability to effectively browse, query, and export aggregated host-based endpoint data through a management dashboard query interface, in addition to automatically add newly discovered endpoints to a monitored database.

[USE CASE] **Expandability**

[USE CASE 1] Vendor Expansion

The ability to integrate and expand with additional vendor packages for custom monitoring and configuration of varying physical and virtual hardware.

[USE CASE 2] Resource Expansion

The capability to generate performance and predictive analysis to estimate when a monitored resource will be exhausted and allow for administrators to plan accordingly.

[USE CASE] **Security**

The ability to function in any configuration of endpoints with or without agents in the following ways.

Agent

[USE CASE 1] Detection of Potential Unauthorized Activity

The ability for agents to detect potentially unauthorized activity, software, or users by collection of host-based endpoint data and reporting back to the management server for further analysis.

[USE CASE 2] Remediation of Malicious Activity

The ability for the management server to instruct agents to perform remediation activities on the endpoints to cleanup detected malicious activity and report back through secured channels.

Agentless

[USE CASE 1] Detection of Potential Unauthorized Activity

The detection of potentially unauthorized activity, software, or users is enabled by remote collection of host-based endpoint data by the management server.

[USE CASE 2] Remediation of Malicious Activity

The ability to perform remediation activities on the endpoint remotely from the management server to cleanup detected malicious activity.

Resources to be protected

- Sensitive data stored by the ESM system.
- Credentials for authentication to or from the ESM system.
- Cryptographic key material to perform secure communications with host agents.
- Sensitive data in transit to or from the ESM system.

Attacker access

- An attacker is assumed to attempt attacks from the following vantage points:
  - The network across which the application engages in communication, both actively and passively. Including potentially IOT devices and BYOD.
  - The platform on which the application is installed, though as an unprivileged subject.
  - The endpoint (host agent) by planting crafted malicious artifacts on the Endpoint platform to be consumed by the ESM System.
- An attacker has an arbitrary amount of time to analyze the behavior of the application, its interaction with its host device or platform, and/or the data it transmits over the network.

Essential Security Requirements

- Patch Management
  - Scanning and updating patches is important enterprise security and requires management at all phases: QA, development, staging, production, etc. and maintaining strict policies to avoid any unexpected events.
- Policy Management
  - Exception creation and policy configuration.
  - View protected processes.
  - Agent and ESM settings
    - Heartbeat Interval
    - Reporting Interval
  - Content updates
- Vulnerability Assessment
  - Import current and future hashes and set policy for them based on rules.
    - Ability to administratively override previous policies.
  - Scanning hosts for missing patches, configurations, security policies
    - Scanning file executions and running files.
- Architecture

    - Resiliency
        - Failover
        - Loadbalanced
    - Endpoint and Tenant Management
        - Role-based access control
        - Agent revocation
    - Permission Segregation
        - Role based Tier model, protecting privileged accounts and resources from non-privileged.
    - Compliance
        - Auditing capabilities
    - Confidentiality
        - Encrypted communication between ESM host and clients
- Risk Management
    - Behavior Detection/Threat Modeling
    - Network Virtualization
    - Ties into architecture with custom defense strategies based on the capabilities of the architecture
    - Zero Trust
- Reporting Capabilities
    - Log forwarding (SIEM, Syslog, Email, etc.)
    - Security events search criteria

Assumptions

The following assumptions are made for the ESM product and its operational environment:

- Depending on configuration and capability, the product may or may not be:
    - Bound to directory server to support multi-user login
- The ESM system is connected to a network. For purposes of sending/receiving endpoint agent data. Other entities on the network are not inherently trustable.
- Administrators are not malicious in nature.
- Users are not malicious in nature, though they may inadvertently or intentionally engage in risky behavior.

Outside the TOE's Scope

- Cloud ESM devices – this is not to include a VM running in the cloud running ESM, but ESM cloud specific tool like AWS Security Hub or Azure Sentinel