Common Criteria Evaluation and Validation Scheme
National Information Assurance Partnership (NIAP)

Title: Enterprise Management (EM)
Maintained by: National Information Assurance Partnership (NIAP)
Unique Identifier: 00x
Version: 2.0x
Status: Draft
Date of issue: 02/02/2024
Approved by:
Supersedes:

Background and Purpose

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

Enterprise management (EM) software is a category of software applications designed to support organizations in managing their core business processes, data, and resources. This software encompasses tools for areas like finance, accounting, supply chain, HR, customer relationships, project management, and even infrastructure monitoring. EM software automates and integrates complex business functions, providing insights and improving operational efficiency across an organization. It has a critical role in streamlining workflows and driving data-driven decision-making. Finally, EM software platforms act as central hubs for connecting and coordinating various software applications used within an organization. The role of EM software is breaking down data silos and enabling seamless communication and collaboration between different departments and systems.

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 present key aspects that support or guide the TC, and may elaborate on subtleties not apparent in the “bulleted” high level statements.

Use Case(s)

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

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 EM settings
        - Heartbeat Interval
        - Reporting Interval
    - Content updates
- Vulnerability Assessment
    - Import unknown 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
        - Load balanced
    - 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 EM 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

Threats

T.NETWORK_ATTACK

An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may engage in communications with applications and services running on or part of the OS with the intent of compromise. Engagement may consist of altering existing legitimate communications.

T.NETWORK_EAVESDROP

An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between applications and services that are running on or part of the OS.

T.LOCAL_ATTACK

An attacker may compromise applications running on the OS. The compromised application may provide maliciously formatted input to the OS through a variety of channels including unprivileged system calls and messaging via the file system.

T.LIMITED_PHYSICAL_ACCESS

An attacker may attempt to access data on the OS while having a limited amount of time with the physical device.

Assumptions

The following assumptions are made for the EM software 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.

Objectives

O.ACCOUNTABILITY

Conformant OSes ensure that information exists that allows administrators to discover unintentional issues with the configuration and operation of the operating system and discover its cause. Gathering event information and immediately transmitting it to another system can also enable incident response in the event of system compromise.

O.INTEGRITY

Conformant OSes ensure the integrity of their update packages. OSes are seldom if ever shipped without errors, and the ability to deploy patches and updates with integrity is critical to enterprise network security. Conformant OSes provide execution environment-based mitigations that increase the cost to attackers by adding complexity to the task of compromising systems.

O.MANAGEMENT

To facilitate management by users and the enterprise, conformant OSes provide consistent and supported interfaces for their security-relevant configuration and maintenance. This includes the deployment of applications and application updates through the use of platform-supported deployment mechanisms and formats, as well as providing mechanisms for configuration and application execution control.

O.PROTECTED_STORAGE

To address the issue of loss of confidentiality of credentials in the event of loss of physical control of the storage medium, conformant OSes provide data-at-rest protection for credentials. Conformant OSes also provide access controls which allow users to keep their files private from other users of the same system.

O.PROTECTED_COMMS

To address both passive (eavesdropping) and active (packet modification) network attack threats, conformant OSes provide mechanisms to create trusted channels for CSP and sensitive data. Both CSP and sensitive data should not be exposed outside of the platform.