## DEFINITION

<table>
<thead>
<tr>
<th>Name</th>
<th>Application-Based Intrusion Detection Systems (IDS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Application-Based IDS is a special subset of Host-Based IDS (HIDS) that analyzes the events transpiring within a software application. The most common information source for Application-Based IDS is the application’s transaction log file.</td>
</tr>
<tr>
<td>Rationale</td>
<td>The ability to interface with applications directly allows Application-Based IDS to detect suspicious behavior such as users exceeding their security authorization.</td>
</tr>
</tbody>
</table>
| Benefits                    | - Application-Based IDS monitors the interaction between user and application, which traces activity to individual users.  
                            - Application-Based IDS works with applications that access encrypted data since it interfaces with the application at transaction endpoints where information is presented to users in unencrypted form. |

## ASSOCIATED ARCHITECTURE LEVELS

<table>
<thead>
<tr>
<th>List the Domain Name</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>List the Discipline Name</td>
<td>Technical Controls</td>
</tr>
<tr>
<td>List the Technology Area Name</td>
<td>Intrusion Detection Systems</td>
</tr>
</tbody>
</table>

## COMPLIANCE COMPONENT TYPE

<table>
<thead>
<tr>
<th>Document the Compliance Component Type</th>
<th>Guideline</th>
</tr>
</thead>
<tbody>
<tr>
<td>Component Sub-type</td>
<td></td>
</tr>
</tbody>
</table>

## COMPLIANCE DETAIL

### General Application-Based IDS Requirements

- Administrators shall be trained on the Application-Based IDS before implementation. Despite vendor claims of ease of use, training and/or experience are absolutely necessary to manage any IDS.
- It is preferred to have the Application-Based IDS controlled directly from a central location(s). However, the Application-Based IDS may be agent-based where response decisions are made at the agent.
- Application-Based IDS administrators shall be able to create or change policies easily.

### Application-Based IDS Deployment Requirements

- Application-Based IDS shall be deployed in conjunction with Network-Based IDS (NIDS) and/or HIDS to fully protect the system.
- It is recommended that organizations install the NIDS first, followed by the HIDS, and then the Application-Based IDS installation on
critical servers.

- Application-Based IDS shall be enabled on hosts that have critical applications.
- Application transaction logs shall be enabled.
- It is preferred to install Application-Based IDS Management software on a separate system from the application being monitored.
- It is preferred to have the Application-Based IDS use an agent-Manager (server) architecture, where policy is created and modified on the manager and automatically distributed to all agents.
- It is preferred that application agents poll the manager at periodic intervals for policy changes or new software updates.

**Application-Based IDS Analysis Requirements**

- Application-Based IDS shall utilize, at a minimum, information from an application’s transaction log files.
- Application-Based IDS shall have easy-to-use tools to analyze the logs.
- Application-Based IDS shall use Misuse Detection methods (matching a predefined pattern of events describing an attack) and may also include Anomaly Detection (abnormal, unusual behavior) components.
- Application-Based IDS may be configured to intercept the following types of requests and use them in combinations and sequences to constitute an application’s normal behavior:
  - File System (file read or write)
  - Network (packet events at the driver (NDIS) or transport (TDI) level)
  - Configuration (read or write to the registry on Windows)
  - Execution Space (write to memory not owned by the requesting application. For example, attempts to inject a shared library DLL into another process)
- Operators shall follow a schedule for checking the results of the Application-Based IDS to ensure attackers have not modified the system.

**Application-Based IDS Response Requirements**

- Application-Based IDS shall respond in real-time.
- It is preferred that Application-Based IDS provide active responses to intrusions by:
  - Collecting additional information by turning up the number of events logged, or
  - Terminating the user’s access.
- Operators shall be extremely careful when creating rules to ensure intruders cannot abuse the feature to deny access to legitimate users.
- Application-Based IDS may provide passive responses requiring
subsequent human action to intrusions by:

- Generating alarms and notifications with popup windows, cellular phones, pagers and email, or
- Reporting alarms and alerts using SNMP traps and plug-ins to central network management consoles.

- All Application-Based IDS communications shall be secure and use encrypted tunnels or other cryptographic measures.
- Application-Based IDS shall create output with the following information for each intrusion detected:
  - Time/date
  - Sensor IP address
  - Specific attack name
  - Source and destination IP addresses
  - Network protocol used
  - Description of the attack type
  - Attack severity level
  - Type of loss expected
  - Type of vulnerability exploited
  - Access validation
  - Exceptional condition
  - Environmental (unexpected interaction with the operating system or between two applications)
  - Host Configuration
  - Race (delay between the time a system checks to see if an operation is allowed and the time it performs the operation)
  - Design
  - Software types and versions vulnerable
  - Patch information to counter the attack
  - References to advisories about the attack or vulnerability
  - It is preferred that Application-Based IDS reports combine redundant attack entries and make attacks of highest importance stand out.

<table>
<thead>
<tr>
<th>Document Source Reference #</th>
<th>NIST SP 800-18 (<a href="http://www.csrc.nist.gov/publications/nistpubs">www.csrc.nist.gov/publications/nistpubs</a>)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Standard Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Website</td>
</tr>
</tbody>
</table>

Contact Information
<table>
<thead>
<tr>
<th>Government Body</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)</td>
</tr>
<tr>
<td></td>
<td>CVE Vulnerability Search on ICAT Metabase</td>
</tr>
<tr>
<td>Website</td>
<td><a href="http://csrc.nist.gov/">http://csrc.nist.gov/</a></td>
</tr>
<tr>
<td></td>
<td><a href="http://icat.nist.gov/">http://icat.nist.gov/</a></td>
</tr>
</tbody>
</table>

| Contact Information | inquiries@nist.gov |

**KEYWORDS**

List all Keywords
Honey Pot, intrusion, cracker, buffer overflows, passwords, sniffing, exploit, denial-of-service, Java, ActiveX, SMURF, DNS, probes, logging, auditing, monitoring, anomaly, patterns, exploits, misuse

**COMPONENT CLASSIFICATION**

Provide the Classification
- [ ] Emerging
- [x] Current
- [ ] Twilight
- [ ] Sunset

Rationale for Component Classification

**Conditional Use Restrictions**

Document the Conditional Use Restrictions

**Migration Strategy**

Document the Migration Strategy

**Impact Position Statement**

Document the Position Statement on Impact

**CURRENT STATUS**

Provide the Current Status
- [ ] In Development
- [ ] Under Review
- [x] Approved
- [ ] Rejected

**AUDIT TRAIL**

Creation Date: 04/03/2003
Date Accepted / Rejected: 05/14/2003

Reason for Rejection

Last Date Reviewed

Reason for Update