Compliance Component

DEFINITION	
Name	Application-Based Intrusion Detection Systems (IDS)
Description	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.
Rationale	The ability to interface with applications directly allows Application-Based IDS to detect suspicious behavior such as users exceeding their security authorization.
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	
List the Domain Name	Security
List the Discipline Name	Technical Controls
List the Technology Area Name	Intrusion Detection Systems
List Product Component Name	

COMPLIANCE COMPONENT TYPE	
Document the Compliance Component Type	Guideline
Component Sub-type	

COMPLIANCE DETAIL	
State the Guideline, Standard or Legislation	**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.
Document Source Reference #	NIST SP 800-18 (www.csrc.nist.gov/publications/nistpubs) CERT Guide to System and Network Security Practices (www.cert.org/security-improvement/)
Standard Organization	
Name	*Website*
Contact Information	

Government Body			
Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC) CVE Vulnerability Search on ICAT Metabase	*Website*	http://csrc.nist.gov/ http://icat.nist.gov/
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* ☒ *Current* ☐ *Twilight* ☐ *Sunset*		
Rationale for Component Classification			
Document the 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* ☒ *Approved* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date	04/03/2003	*Date Accepted / Rejected*	05/14/2003
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			