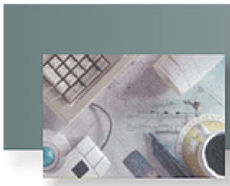

Technology Area

DEFINITION	
Name	Virus Detection and Elimination
Description	Virus Detection and Elimination addresses those policies, methods and tools associated with detecting, combating, reporting and eradicating malicious program code (e.g., worms, Trojan horse, malware). A virus usually has a destructive or disruptive effect on the executable program or system component that it affects.
Rationale	Provide a scalable multi-tiered defense to fend off virus threats and prevent loss of time and money.
Benefits	Protect assets (i.e., data and resources) from corruption, disruption, destruction, and unavailability. Can assist in the system quarantine, repair and clean-up virus damage.
ASSOCIATED ARCHITECTURE LEVELS	
List the Domain Name	Security
List the Discipline Name	Technical Controls
Associated Compliance Components	
List the Compliance Component Names	• Virus Detection and Elimination Policies and Best Practices • Virus Detection and Elimination Criteria for Anti-Virus Management Tools • Virus Detection and Elimination Criteria for Gateways • Virus Detection and Elimination Criteria for E-mail/Groupware • Virus Detection and Elimination Criteria for Servers • Virus Detection and Elimination Criteria for Workstations • Virus Detection and Elimination Criteria for Wireless
Associated Product Components	
List the Product Component Names	• McAfee o VirusScan (workstation) o NetShield (server) o Groupshield (e-mail) o WebShield Appliances(gateway) o EPolicy Orchestrator (management tool) o VirusScan Wireless Devices (wireless) • Symantec o AntiVirus Corporate Edition (workstation) o AntiVirus Corporate Edition (server) o AntiVirus Corporate Edition (e-mail) o AntiVirus Corporate Edition (gateway) o AntiVirus Corporate Edition (management tool) • Sybari Software Inc. o Antigen for Microsoft Exchange (e-mail) o Antigen for Lotus Notes/Domino (e-mail) o Antigen for Microsoft Exchange (gateway)

	• Computer Associates o InoculateIT (workstation) o InoculateIT (server) o InoculateIT (management tool)

TECHNOLOGY AREA DETAIL

Supporting Documentation	• NIST 800-5 and 500-1166 • Gartner Research Group – Enterprise Anti-Virus product evaluation. Release Note 22 May 2002
Document Source Reference #	

Standard Organization / Government Body

Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	*Website*	http://csrc.nist.gov/
Contact Information	inquiries@nist.gov		
Name	ICSA Labs	*Website*	www.icsalabs.com
Contact Information	ICSA Labs is a division of TruSecure Corporation and can be reached at 1-888-396-8348 (info@trusecure.com)		

KEYWORDS

List Keywords	virus, zoo, trojan horse, backdoor, worm, stealth, blended threat, boot sector infector, companion, denial of service, dropper, file infector, logic bomb, malware, multi-partite, overwriting, parasitic, polymorphic, tunneling, variant, terminate and stay resident (tsr), management; boot sector infector

CURRENT STATUS

Provide the Current Status	☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected*

AUDIT TRAIL

Creation Date	02-06-03	*Date Accepted / Rejected*	02-27-2003
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			