LogRhythm Support for Department of Defense Instruction 8500.2

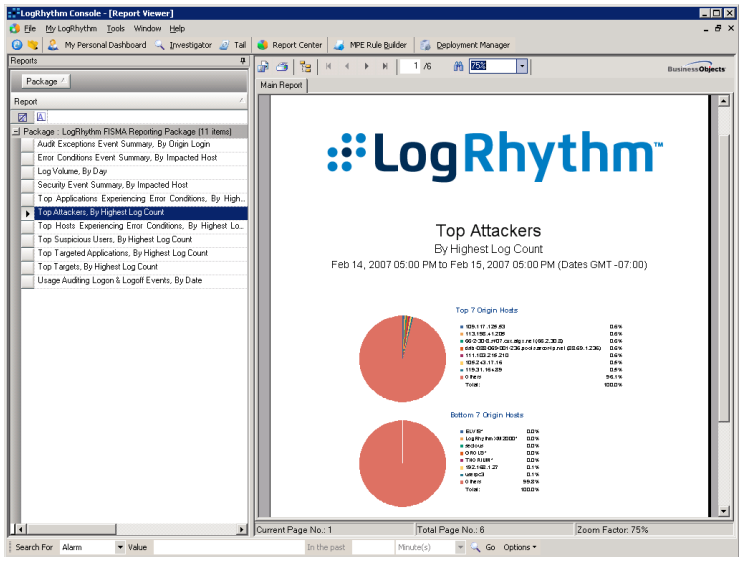
LogRhythm Support for Department of Defense Instruction 8500.2

"The Department of Defense has a crucial responsibility to protect and defend its information and supporting information technology." DoDI (Department of Defense Instruction) 8500.2 was established to provide U.S. Department of Defense information security standards for implementing information assurance controls. These published guidelines cover many areas surrounding "access control", "audit and accountability", "incident response", and "system and information integrity".

The collection, management, and analysis of log data are integral to meeting many DoDI 8500.2 guidelines. The use of LogRhythm directly meets some recommendations and decreases the cost to meet others. IT environments consist of heterogeneous devices, systems, and applications—all reporting log data. Millions of individual log entries can be generated daily, if not hourly. The task of organizing this information can be overwhelming. The additional recommendations of analyzing and reporting on log data render manual processes or homegrown remedies inadequate and cost prohibitive for many organizations.

LogRhythm delivers log collection, archiving, and recovery across the entire IT infrastructure and automates the first level of log analysis. Log data is categorized, identified, and normalized for easy analysis and reporting. LogRhythm's powerful alerting capabilities automatically identify the most critical issues and notify relevant personnel. With the click of a mouse or via an automated scheduler, LogRhythm's out-of-the box DoDI 8500.2 reporting packages ensure you meet your reporting needs.

DoDI 8500.2 and its recommendations guide organizations to implement and perform procedures to effectively capture, monitor, review and retain log data. The remainder of this paper lists the applicable DoD control guidelines, as specified in Instruction 8500.2, that LogRhythm helps address. For each recommendation, an explanation of how LogRhythm support the guideline is provided.Learn how LogRhythm's comprehensive log management and analysis solution can help your organization meet or exceed DoDI 8500.2 guidelines.



LogRhythm Report Center Screenshot

CO Continuity Controls

DoD Instruction 8500.2 Compliance Recommendation		How LogRhythm Supports the Guideline
COBR-1 Protection of Backup and Restoration Assets	Procedures are in place assure the appropriate physical and technical protection of the backup and restoration hardware, firmware, and software, such as router tables, compilers, and other security-related system software.	LogRhythm can track and report on when backups are performed within the past month, or any other time frame as dictated by organizational policy. **Example Reports:** • Backup Status
CODB-1 Data Backup Procedures	Data backup is performed at least weekly.	LogRhythm can track and report on when backups are performed within the past month, or any other time frame as dictated by organizational policy. **Example Reports:** • Backup Status
CODB-2 Data Backup Procedures	Data backup is performed daily, and recovery media are stored off-site at a location that affords protection of the data in accordance with its mission assurance category and confidentiality level.	LogRhythm can track and report on when backups are performed within the past month, or any other time frame as dictated by organizational policy. **Example Reports:** • Backup Status

DC Security Design and Configuration

DoD Instruction 8500.2 Compliance Recommendation		How LogRhythm Supports the Guideline
DCCT-1 Compliance Testing	A comprehensive set of procedures is implemented that tests all patches, upgrades, and new AIS applications prior to deployment.	LogRhythm can track and report on when patches are installed on devices, showing which systems have had patching within the past month, or any other time frame as dictated by organizational policy. **Example Reports:** • Patches Applied
DCII-1 IA Impact Assessment	Changes to the DoD information system are assessed for IA and accreditation impact prior to implementation.	LogRhythm analysis & reporting capabilities can be used for monitoring configuration changes. LogRhythm alerting can be utilized to detect and notify of changes to specific configurations. **Example Reports:** • Configuration Change Summary
DCPP-1 Ports, Protocols, and Services	DoD information systems comply with DoD ports, protocols, and services guidance. AIS applications, outsourced IT-based processes and platform IT identify the network ports, protocols, and services they plan to use as early in the life cycle as possible and notify hosting enclaves. Enclaves register all active ports, protocols, and services in accordance with DoD and DoD Component guidance.	LogRhythm provides monitoring and investigations showing the use of protocols in the network environment. Testing requires verification that all used services, protocols and ports have a business need. **Example Reports:** • Network Connection Summary
DCSL-1 System Library Management Controls	System libraries are managed and maintained to protect privileged programs and to prevent or minimize the introduction of unauthorized code.	LogRhythm's file integrity monitoring capability can be used to detect additions, modifications, deletions, and permission changes to the file system. Analysis & reporting capabilities can be used for monitoring configuration changes. Real-time alerting can be utilized to detect and notify of changes to specific configurations. **Example Reports:** • File Integrity Monitor Log Detail • File Integrity Monitor Log Summary

DoD Instruction 8500.2 Compliance Recommendation		How LogRhythm Supports the Guideline
DCSS-1 System State Changes	System initialization, shutdown, and aborts are configured to ensure that the system remains in a secure state.	LogRhythm provides central monitoring of system events by collecting log data from hosts, applications, network devices, etc. LogRhythm provides real-time event monitoring, alerting, and reporting on specific activity and conditions. **Example Reports:** • System Startup & Shutdown Summary
DCSS-2 System State Changes	System initialization, shutdown, and aborts are configured to ensure that the system remains in a secure state. Tests are provided and periodically run to ensure the integrity of the system state.	LogRhythm provides central monitoring of system events by collecting log data from hosts, applications, network devices, etc. LogRhythm provides real-time event monitoring, alerting, and reporting on specific activity and conditions. **Example Reports:** • System Startup & Shutdown Summary

EB Enclave Boundary Defense

DoD Instruction 8500.2 Compliance Recommendation		How LogRhythm Supports the Guideline
EBRP-1 Remote Access for Privileged Functions	Remote access for privileged functions is discouraged, is permitted only for compelling operational needs, and is strictly controlled. In addition to EBRU-1, sessions employ security measures such as a VPN with blocking mode enabled. A complete audit trail of each remote session is recorded, and the IAM/O reviews the log for every remote session.	LogRhythm collects remote access activity for VPN, SSH, telnet, etc. LogRhythm reports provide easy and independent review of remote access to information systems. **Example Reports:** • Suspicious Activity By User • Host Remote Access Summary

EC Enclave and Computing Environment

DoD Instruction 8500.2 Compliance Recommendation		How LogRhythm Supports the Guideline
ECAD-1 Affiliation Display	To help prevent inadvertent disclosure of controlled information, all contractors are identified by the inclusion of the abbreviation "ctr" and all foreign nationals are identified by the inclusion of their two character country code in: - DoD user e-mail addresses (e.g., john.smith.ctr@army.mil orjohn.smith.uk@army.mil); - DoD user e-mail display names (e.g., John Smith, Contractor <john.smith.ctr@army.mil> or John Smith, United Kingdom <john.smith.uk@army.mil>); and - automated signature blocks (e.g., John Smith, Contractor, J-6K, Joint Staff or John Doe, Australia, LNO, Combatant Command). Contractors who are also foreign nationals are identified as both (e.g.,john.smith.ctr.uk@army.mil). Country codes and guidance regarding their use are in FIPS 10-4.	LogRhythm collects all authentication activity. LogRhythm reports provide easy and standard review of unsuccessful login attempts to systems and applications. LogRhythm alerts can detect & report on multiple unsuccessful login attempts. **Example Reports:** • User Authentication Summary

DoD Instruction 8500.2 Compliance Recommendation		How LogRhythm Supports the Guideline
ECAN-1 Access for Need-to-Know	Access to all DoD information (classified, sensitive, and public) is determined by both its classification and user need-to-know. Need-to-know is established by the Information Owner and enforced by discretionary or role-based access controls. Access controls are established and enforced for all shared or networked file systems and internal websites, whether classified, sensitive, or unclassified. All internal classified, sensitive, and unclassified websites are organized to provide at least three distinct levels of access: 1. Open access to general information that is made available to all DoD authorized users with network access. Access does not require an audit transaction. 2. Controlled access to information that is made available to all DoD authorized users upon the presentation of an individual authenticator. Access is recorded in an audit transaction.	LogRhythm collects information from production access control systems to help define role usage requirements, determine attempts to cross role boundaries, and changes to configurations that can affect separation of duties. **Example Reports:** • Object Access Summary
ECAT-1 Audit Trail, Monitoring, Analysis and Reporting	Audit trail records from all available sources are regularly reviewed for indications of inappropriate or unusual activity. Suspected violations of IA policies are analyzed and reported in accordance with DoD information system IA procedures.	LogRhythm provides centralized monitoring, analysis, and reporting of audit activity across the entire IT infrastructure. LogRhythm automates the process of identifying high-risk activity and prioritizes based on asset risk. High-risk activity can be monitored in real-time or alerted on. LogRhythm reports provide easy and standard review of inappropriate, unusual, and suspicious activity. **Example Reports:** • Usage Auditing Event Detail
ECAT-2 Audit Trail, Monitoring, Analysis and Reporting	An automated, continuous on-line monitoring and audit trail creation capability is deployed with the capability to immediately alert personnel of any unusual or inappropriate activity with potential IA implications, and with a user configurable capability to automatically disable the system if serious IA violations are detected.	LogRhythm provides centralized monitoring, analysis, and reporting of audit activity across the entire IT infrastructure. LogRhythm automates the process of identifying high-risk activity and prioritizes based on asset risk. High-risk activity can be monitored in real-time or alerted on. LogRhythm reports provide easy and standard review of inappropriate, unusual, and suspicious activity. **Example Reports:** • Alarm And Response Activity
ECCD-1 Changes to Data	Access control mechanisms exist to ensure that data is accessed and changed only by authorized personnel.	LogRhythm collects information from production access control systems to help define role usage requirements, determine attempts to cross role boundaries, and changes to configurations that can affect separation of duties. **Example Reports:** • Object Access Summary
ECCD-2 Changes to Data	Access control mechanisms exist to ensure that data is accessed and changed only by authorized personnel. Access and changes to the data are recorded in transaction logs that are reviewed periodically or immediately upon system security events. Users are notified of time and date of the last change in data content.	LogRhythm collects information from production access control systems to help define role usage requirements, determine attempts to cross role boundaries, and changes to configurations that can affect separation of duties: **Example Reports:** • Object Access Summary • File Integrity Monitor Log Detail
ECLC-1 Audit of Security Label Changes	The system automatically records the creation, deletion, or modification of confidentiality or integrity labels, if required by the information owner.	LogRhythm's file integrity monitoring capability can be used to detect additions, modifications, deletions, and permission changes to the file system. Analysis & reporting capabilities can be used for monitoring configuration changes. Real-time alerting can be utilized to detect and notify of changes to specific configurations. **Example Reports:** • File Integrity Monitor Log Detail • File Integrity Monitor Log Summary

DoD Instruction 8500.2 Compliance Recommendation		How LogRhythm Supports the Guideline
ECLO-1 Logon	Successive logon attempts are controlled using one or more of the following: • Access is denied after multiple unsuccessful logon attempts. • The number of access attempts in a given period is limited. • A time-delay control system is employed. If the system allows for multiple logon sessions for each user ID, the system provides a capability to control the number of logon sessions.	LogRhythm collects all authentication activity. LogRhythm reports provide easy and standard review of unsuccessful login attempts to systems and applications. LogRhythm alerts can detect & report on multiple unsuccessful login attempts. **Example Reports:** • User Authentication Summary • Host Access Granted And Revoked
ECLO-2 Logon	Successive logon attempts are controlled using one or more of the following: • Access is denied after multiple unsuccessful logon attempts. • The number of access attempts in a given period is limited. • A time-delay control system is employed. If the system allows for multiple logon sessions for each user ID, the system provides a capability to control the number of logon sessions. Upon successful logon, the user is notified of the date and time of the user's last logon, the location of the user at last logon, and the number of unsuccessful logon attempts using this user ID since the last successful logon.	LogRhythm collects all authentication activity. LogRhythm reports provide easy and standard review of unsuccessful login attempts to systems and applications. LogRhythm alerts can detect & report on multiple unsuccessful login attempts. **Example Reports:** • User Authentication Summary • Host Access Granted And Revoked
ECLP-1 Least Privilege	Access procedures enforce the principles of separation of duties and "least privilege." Access to privileged accounts is limited to privileged users. Use of privileged accounts is limited to privileged functions; that is, privileged users use non-privileged accounts for all non-privileged functions. This control is in addition to an appropriate security clearance and need-to-know authorization.	LogRhythm monitors activities by both users and systems to assist in determining necessary access, frivolous access, and resource needs of production systems. Review of activities such as network connections, application access, and system logons can help identify appropriate and inappropriate use according to policy. **Example Reports:** • Suspicious Activity By User
ECMT-1 Conformance Monitoring and Testing	Conformance testing that includes periodic, unannounced, in-depth monitoring and provides for specific penetration testing to ensure compliance with all vulnerability mitigation procedures such as the DoD IAVA or other DoD IA practices is planned, scheduled, and conducted. Testing is intended to ensure that the system's IA capabilities continue to provide adequate assurance against constantly evolving threats and vulnerabilities.	Vulnerabilities can be detected by real-time examination tools or by using compatible vulnerability scanning systems. Attempts to attack the system can be alarmed on in real-time by LogRhythm. **Example Reports:** • Vulnerabilities Detected
ECMT-2 Conformance Monitoring and Testing	Conformance testing that includes periodic, unannounced in-depth monitoring and provides for specific penetration testing to ensure compliance with all vulnerability mitigation procedures such as the DoD IAVA or other DoD IA practices is planned, scheduled, conducted, and independently validated. Testing is intended to ensure that the system's IA capabilities continue to provide adequate assurance against constantly evolving threats and vulnerabilities.	Vulnerabilities can be detected by real-time examination tools or by using compatible vulnerability scanning systems. Attempts to attack the system can be alarmed on in real-time by LogRhythm. **Example Reports:** • Vulnerabilities Detected
ECPA-1 Production Code Change Controls	All privileged user accounts are established and administered in accordance with a role-based access scheme that organizes all system and network privileges into roles (e.g., key management, network, system administration, database administration, web-administration). The IAM tracks privileged role assignments.	LogRhythm collects all account management activities. LogRhythm reports provide easy and standard review of all account management activity: **Example Reports:** • Account Management Activity

DoD Instruction 8500.2 Compliance Recommendation		How LogRhythm Supports the Guideline
ECPC-1 Production Code Change Controls	Application programmer privileges to change production code and data are limited and are periodically reviewed.	LogRhythm's file integrity monitoring capability can be used to detect additions, modifications, deletions, and permission changes to the file system. Analysis & reporting capabilities can be used for monitoring configuration changes. Real-time alerting can be utilized to detect and notify of changes to specific configurations. **Example Reports:** • File Integrity Monitor Log Detail • File Integrity Monitor Log Summary
ECPC-2 Production Code Change Controls	Application programmer privileges to change production code and data are limited and reviewed every 3 months.	LogRhythm's file integrity monitoring capability can be used to detect additions, modifications, deletions, and permission changes to the file system. Analysis & reporting capabilities can be used for monitoring configuration changes. Real-time alerting can be utilized to detect and notify of changes to specific configurations. **Example Reports:** • File Integrity Monitor Log Detail • File Integrity Monitor Log Summary
ECRG-1 Audit Reduction and Report Generation	Tools are available for the review of audit records and for report generation from audit records.	LogRhythm supplies a one stop repository from which to review log data from across the entire IT infrastructure. Reports can be generated and distributed automatically on a daily basis. LogRhythm provides an audit trail of who did what within LogRhythm and a report which can be provided to show proof of log data review. **Example Reports:** • Usage Auditing Event Detail
ECRR-1 Audit Record Retention	If the DoD information system contains sources and methods intelligence (SAMI), then audit records are retained for 5 years. Otherwise, audit records are retained for at least 1 year.	LogRhythm completely automates the process and requirement of collecting and retaining audit logs. LogRhythm retains logs in compressed archive files for cost effective, easy-to-manage, long-term storage. Log archives can be restored quickly and easily months or years later in support of after-the-fact investigations. **Example Reports:** • Archive Log Rate Analysis
ECTB-1 Audit Trail Backup	The audit records are backed up not less than weekly onto a different system or media than the system being audited.	LogRhythm completely automates the process and requirement of collecting and retaining audit logs. LogRhythm retains logs in compressed archive files for cost effective, easy-to-manage, long-term storage. Log archives can be restored quickly and easily months or years later in support of after-the-fact investigations. **Example Reports:** • Backup Status
ECTP-1 Audit Trail Protection	The contents of audit trails are protected against unauthorized access, modification or deletion.	LogRhythm's file integrity monitoring capability can be used to detect additions, modifications, deletions, and permission changes to the file system. Analysis & reporting capabilities can be used for monitoring configuration changes. Real-time alerting can be utilized to detect and notify of changes to specific configurations. **Example Reports:** • File Integrity Monitor Log Detail • File Integrity Monitor Log Summary • Archived Log Rate Analysis

DoD Instruction 8500.2 Compliance Recommendation		How LogRhythm Supports the Guideline
ECVP-1 Virus Protection	All servers, workstations and mobile computing devices implement virus protection that includes a capability for automatic updates.	LogRhythm detects and alerts on any error conditions originating from anti-virus applications, when the services are started and stopped, as well as identifies when new signatures are installed. Alarming can be configured to inform the custodian(s) of when any malware is detected inside the cardholder data environment. **Example Reports:** • Anti-Virus Signature Update Report
ECWN-1 Wireless Computing and Networking	Wireless computing and networking capabilities from workstations, laptops, personal digital assistants (PDAs), handheld computers, cellular phones, or other portable electronic devices are implemented in accordance with DoD wireless policy, as issued. (See also ECCT). Unused wireless computing capabilities internally embedded in interconnected DoD IT assets are normally disabled by changing factory defaults, settings or configurations prior to issue to end users. Wireless computing and networking capabilities are not independently configured by end users.	LogRhythm can observe and report on detected wireless networks, identifying wireless access points that communicate with the environment. **Example Reports:** • Wireless Access Points

IA Identification and Authentication

DoD Instruction 8500.2 Compliance Recommendation		How LogRhythm Supports the Guideline
IAIA-1 Individual Identification and Authentication	DoD information system access is gained through the presentation of an individual identifier (e.g., a unique token or user login ID) and password. For systems utilizing a logon ID as the individual identifier, passwords are, at a minimum, a case sensitive 8-character mix of upper case letters, lower case letters, numbers, and special characters, including at least one of each (e.g., emPagd2!). At least four characters must be changed when a new password is created. Deployed/tactical systems with limited data input capabilities implement the password to the extent possible. Registration to receive a user ID and password includes authorization by a supervisor, and is done in person before a designated registration authority. Additionally, to the extent system capabilities permit, system mechanisms are implemented to enforce automatic expiration of passwords and to prevent password reuse. All factory set, default or standard-user IDs and passwords are removed or changed. Authenticators are protected commensurate with the classification or sensitivity of the information accessed; they are not shared; and they are not embedded in access scripts or stored on function keys. Passwords are encrypted both for storage and for transmission.	LogRhythm collects all account management activities. LogRhythm reports provide easy and standard review of all account management activity. **Example Reports:** • User Authentication Summary

DoD Instruction 8500.2 Compliance Recommendation		How LogRhythm Supports the Guideline
IAIA-2 Individual Identification and Authentication	DoD information system access is gained through the presentation of an individual identifier (e.g., a unique token or user logon ID) and password. For systems utilizing a logon ID as the individual identifier, passwords are, at a minimum, a case sensitive, 8-character mix of upper case letters, lower case letters, numbers, and special characters, including at least one of each (e.g., emPagd2!). At least four characters must be changed when a new password is created. Deployed/tactical systems with limited data input capabilities implement these measures to the extent possible. Registration to receive a user ID and password includes authorization by a supervisor, and is done in person before a designated registration authority. Multiple forms of certification of individual identification such as a documentary evidence or a combination of documents and biometrics are presented to the registration authority. Additionally, to the extent capabilities permit, system mechanisms are implemented to enforce automatic expiration of passwords and to prevent password reuse, and processes are in place to validate that passwords are sufficiently strong to resist cracking and other attacks intended to discover a user's password. All factory set, default or standard-user IDs and passwords are removed or changed. Authenticators are protected commensurate with the classification or sensitivity of the information accessed; they are not shared; and they are not embedded in access scripts or stored on function keys. Passwords are encrypted both for storage and for transmission.	LogRhythm collects all account management activities. LogRhythm reports provide easy and standard review of all account management activity. **Example Reports:** • User Authentication Summary

PE Physical and Environmental

DoD Instruction 8500.2 Compliance Recommendation		How LogRhythm Supports the Guideline
PECF-1 Access to Computing Facilities	Only authorized personnel with a need-to-know are granted physical access to computing facilities that process sensitive information or unclassified information that has not been cleared for release.	LogRhythm can collect log messages from physical access devices (ie, Card Key) for analysis and reporting. **Example Reports:** • Door Access Summary
PECF-2 Access to Computing Facilities	Only authorized personnel with appropriate clearances are granted physical access to computing facilities that process classified information.	LogRhythm can collect log messages from physical access devices (ie, Card Key) for analysis and reporting. **Example Reports:** • Door Access Summary
PEPF-1 Physical Protection of Facilities	Every physical access point to facilities housing workstations that process or display sensitive information or unclassified information that has not been cleared for release is controlled during working hours and guarded or locked during non-work hours.	LogRhythm can collect log messages from physical access devices (ie, Card Key) for analysis and reporting. **Example Reports:** • Door Access Summary
PEPF-2 Physical Protection of Facilities	Every physical access point to facilities housing workstations that process or display classified information is guarded or alarmed 24 X 7. Intrusion alarms are monitored. Two (2) forms of identification are required to gain access to the facility (e.g., ID badge, key card, cipher PIN, biometrics). A visitor log is maintained.	LogRhythm can collect log messages from physical access devices (ie, Card Key) for analysis and reporting. **Example Reports:** • Door Access Summary

VI Vulnerability and Incident Management

DoD Instruction 8500.2 Compliance Recommendation		How LogRhythm Supports the Guideline
VIIR-1 Incident Response Planning	An incident response plan exists that identifies the responsible CND Service Provider in accordance with DoD Instruction O-8530.2, defines reportable incidents, outlines a standard operating procedure for incident response to include INFOCON, provides for user training, and establishes an incident response team. The plan is exercised at least annually.	LogRhythm provides a centralized management system capable of alarming, reporting and investigating security breaches to the network. LogRhythm supports an incident response plan by providing the real-time enterprise detection intelligence to address issues quickly to prevent damage and exposure. **Example Alarms:** • Alarm And Response Activity
VIIR-2 Incident Response Planning	An incident response plan exists that identifies the responsible CND Service Provider in accordance with DoD Instruction O-8530.2, defines reportable incidents, outlines a standard operating procedure for incident response to include INFOCON, provides for user training, and establishes an incident response team. The plan is exercised at least every 6 months.	LogRhythm provides a centralized management system capable of alarming, reporting and investigating security breaches to the network. LogRhythm supports an incident response plan by providing the real-time enterprise detection intelligence to address issues quickly to prevent damage and exposure. **Example Alarms:** • Alarm And Response Activity
VIVM-1 Vulnerability Management	A comprehensive vulnerability management process that includes the systematic identification and mitigation of software and hardware vulnerabilities is in place. Wherever system capabilities permit, mitigation is independently validated through inspection and automated vulnerability assessment or state management tools. Vulnerability assessment tools have been acquired, personnel have been appropriately trained, procedures have been developed, and regular internal and external assessments are conducted. For improved interoperability, preference is given to tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and use the Open Vulnerability Assessment Language (OVAL) to test for the presence of vulnerabilities.	Vulnerabilities can be detected by real-time examination tools or by using compatible vulnerability scanning systems. Attempts to attack the system can be alarmed on in real-time by LogRhythm. **Example Reports:** • Vulnerabilities Detected