Coverity as Part of Your PCI DSS Compliance Toolkit

Build security and compliance into business-as-usual processes

Overview

The primary goal of any software security initiative (SSI) should be information assurance. Every organization should follow this principle when defining a secure software development life cycle (SSDLC) and selecting supporting solutions. Organizations that achieve a high level of information assurance are often in the best position to comply with standards such as the Payment Card Industry Data Security Standard (PCI DSS).

PCI DSS is an information security standard for any organization that handles payment cards, including any retailers, financial institutions, point-of-sale vendors, and hardware and software developers that create or operate the infrastructure for processing payments.

PCI DSS has 12 requirements for compliance organized into six groups:

1. Build and maintain a secure network and systems.
2. Protect cardholder data.
3. Maintain a vulnerability management program.
4. Implement strong access control measures.
5. Regularly monitor and test networks.
6. Maintain an information security policy.

Become PCI DSS compliant with Coverity

Coverity is a static analysis tool that helps reduce risk and lower overall project costs by identifying critical quality defects and potential security vulnerabilities early in the software development life cycle or SDLC (during development) and providing reliable, actionable remediation guidance. Because of this, Coverity is ideal for organizations required to comply with PCI DSS.

Depth and accuracy of analysis

PCI DSS requires that applications be free of certain defect types. Defects are an area of high risk because organizations that fail to achieve the necessary defect-detection rate will have secondary compliance issues.

Coverity is recognized as the leading SAST solution by Forrester, in part because of the strength of its analysis algorithms, which detect a broad range of security weaknesses, and because of its unmatched accuracy. These features translate into one of the highest defect-detection rates in the industry.

Tracking for sensitive and personal data

Coverity's sophisticated sensitive-data leak checker is particularly useful in PCI DSS–compliant environments. It was designed to help organizations ensure that they handle all cardholder data and personally identifiable information (including medical information) properly.

Coverity tracks 25 types of sensitive data, including national ID, cardholder data, account data, transaction information, medical information, biometric data, and geographical data. Mishandling of this type of information is a significant contributor to information leakage and the most common reason for failed audits.

Efficient issue management and remediation

Developers around the world use Coverity because it gives them fast, on-the-fly results and actionable remediation advice with the most precise and efficient fixes. And because it is deployed early in the SDLC, Coverity significantly reduces costs and risks downstream, saving organizations time and money.

Flexible, customizable reporting with rich data

The information stored by Coverity is rich in metadata, such as mappings to CWE, OWASP Top 10, and other standards, which makes building reports to meet your needs a simple, mechanical process. Coverity offers flexible reporting to demonstrate PCI DSS compliance:

- Coverity's report generation package creates commonly requested reports in several formats (such as PDF), including reports tailored for PCI quality security assessors (QSAs).
- All data that Coverity produces is available via a REST API in CSV, XML, and JSON formats. So you can create your own customized reports to show Coverity findings in any format and layout.

Continue reading to learn more about how Coverity can help you address specific PCI DSS requirements.

Expanded standards compliance and vulnerability detection

PCI DSS requirement	Addressing compliance
6.1: Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities.	Coverity can help you create a continuous vulnerability and remediation process across development projects. Risk rankings take into consideration industry best practices and potential impact. For example, the criteria for ranking a vulnerability may include its CVSS base score or its classification by Synopsys. When new security vulnerabilities are discovered, Coverity categorizes them as high, medium, or low risk, so developers can quickly access defects based on impact/risk.
6.3: Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: • In accordance with PCI DSS (for example, secure authentication and logging) • Based on industry standards and/or best practices. • Incorporating information security throughout the software-development life cycle	Based on industry standards and best practices, Coverity was designed to "build security into" the software development life cycle, whether the software is for an internal or external application. Coverity also generates strong documentation to assist with compliance activities in accordance with PCI DSS.
6.4.3: Production data (live PANs) are not used for testing or development	Use Coverity's SENSITIVE_DATA_LEAK checker with data source type CardHolderData to analyze for any PANs present in development, testing, or production source code. Remove any PANs that are uncovered.
6.4.4: Removal of test data and accounts from system components before the system becomes active/ goes into production.	Meet this requirement by analyzing code for test data and accounts and using Coverity Components to filter out that information so you can remove it before the system goes into production.
6.4.5.3: Functionality testing to verify that the change does not adversely impact the security of the system.	Meet this requirement by using Coverity to search the code's change set for security vulnerabilities. Coverity provides more accurate analysis as it understands the abstract syntax tree (AST) of the code. Coverity can also analyze any nonmodified code that calls a function whose code changed, also referred to as the "ripple effect."
6.5: Address common coding vulnerabilities in software-development processes as follows: • Train developers at least annually in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities. • Develop applications based on secure coding guidelines.	For developers, one of the best ways to learn how to address coding vulnerabilities is to learn why a vulnerability was flagged as exploitable and to see the flow of tainted data from source to sink. Coverity gives developers this information, as well as detailed remediation advice for fixing defects based on secure coding guidelines. For developers who are also eLearning customers, Coverity provides links to courses relevant to the CWEs it finds in the code, so developers can stay up-to-date on secure coding practices in their own programming languages.
6.5.1: Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.	Coverity has many injection checkers*: ANGULAR_BYPASS_SECURITY, ANGULAR_ELEMENT_REFERENCE, ANGULAR_EXPRESSION_INJECTION, ANGULAR_SCE_DISABLED, BUFFER_SIZE, COOKIE_SERIALIZER_CONFIG, CSS_INJECTION, DISTRUSTED_DATA_DESERIALIZATION, DOM_XSS, DYNAMIC_OBJECT_ATTRIBUTES, EL_INJECTION, FB.HRS_REQUEST_PARAMETER_TO_COOKIE, FB.HRS_REQUEST_PARAMETER_TO_HTTP_HEADER, FB.SQL_NONCONSTANT_STRING_PASSED_TO_EXECUTE, FB.SQL_PREPARED_STATEMENT_GENERATED_FROM_NONCONSTANT_STRING, FB.XSS_REQUEST_PARAMETER_TO_JSP_WRITER, FB.XSS_REQUEST_PARAMETER_TO_SEND_ERROR, FB.XSS_REQUEST_PARAMETER_TO_SERVLET_WRITER, FORMAT_STRING_INJECTION, HEADER_INJECTION, INSECURE_CSP, JAVA_CODE_INJECTION, JCR_INJECTION, JINJA2_AUTOESCAPE_DISABLED, JSP_DYNAMIC_INCLUDE, JSP_SQL_INJECTION, LDAP_INJECTION, LDAP_NOT_CONSTANT, LOCALSTORAGE_MANIPULATION, NOSQL_QUERY_INJECTION, OGNL_INJECTION, OS_CMD_INJECTION, PATH_MANIPULATION, PMD.ApexSOQLInjection, PMD.ApexXSSFromEscapeFalse, PMD.ApexXSSFromURLParam, PMD.VfHtmlStyleTagXss, PMD.VfUnescapeEl, PW.NON_CONST_PRINTF_FORMAT_STRING, READLINK, REGEX_INJECTION, RUBY_VULNERABLE_LIBRARY, SCRIPT_CODE_INJECTION, SESSIONSTORAGE_MANIPULATION, SIGMA.conflicting_names_servlet, (cont. on next page)

PCI DSS requirement	Addressing compliance
6.5.1: Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws. (cont.)	SIGMA.content_security_policy_disabled_express_helmet, SIGMA.dangerously_exposed_interface_android, SIGMA.duplicate_validation_forms_struts, SIGMA.http_header_validation_disabled_netty, SIGMA.insecure_xss_filter_express_helmet, SIGMA.javascript_code_in_description_openapi, SIGMA.ldap_entry_poisoning_core_java, SIGMA.markdown_allow_dangerous_html_react, SIGMA.no_sniff_disabled_express_helmet, SIGMA.remote_execution_enabled_consul, SIGMA.script_checks_enabled_consul, SIGMA.unsafe_deserialization_activemq_settrustallpackages, SIGMA.unsafe_deserialization_activemq_settrustedpackages, SIGMA.unsafe_deserialization_apache_xmlrpc, SIGMA.unsafe_deserialization_core_java_xmldecoder, SIGMA.unsafe_deserialization_jackson_objectmapper, SIGMA.unsafe_deserialization_spring_boot_activemq_trustall_properties, SIGMA.unsafe_deserialization_spring_boot_activemq_trustall_xml, SIGMA.unsafe_deserialization_spring_boot_activemq_trustall_yaml, SIGMA.unsafe_deserialization_spring_boot_activemq_trusted_properties, SIGMA.unsafe_deserialization_spring_boot_activemq_trusted_xml, SIGMA.unsafe_deserialization_spring_boot_activemq_trusted_yaml, SIGMA.unsafe_innerhtml_manipulation_react, SIGMA.unsafe_innerhtml_manipulation_vue_jsx, SIGMA.unsafe_innerhtml_manipulation_vue_vhtml_directive, SIGMA.weak_xss_protection_servlet, SIGMA.xss_filter_disabled_express_helmet, SIZECHECK, SQLI, SQL_NOT_CONSTANT, STRING_NULL, SYMFONY_EL_INJECTION, TAINTED_ENVIRONMENT_WITH_EXECUTION, TEMPLATE_INJECTION, UNESCAPED_HTML, UNKNOWN_LANGUAGE_INJECTION, UNSAFE_DESERIALIZATION, UNSAFE_JNI, UNSAFE_NAMED_QUERY, UNSAFE_REFLECTION, UNSAFE_XML_PARSE_CONFIG, URL_MANIPULATION, WEAK_XML_SCHEMA, XML_EXTERNAL_ENTITY, XML_INJECTION, XPATH_INJECTION, XSS
6.5.2: Buffer overflows	Coverity has many buffer overflow checkers*: ARRAY_VS_SINGLETON, BAD_ALLOC_ARITHMETIC, BAD_SIZEOF, BUFFER_SIZE, COM.BAD_FREE, COM.BSTR.ALLOC, COM.BSTR.CONV, DC.STREAM_BUFFER, DC.STRING_BUFFER, INCOMPATIBLE_CAST, INTEGER_OVERFLOW, INVALIDATE_ITERATOR, MISMATCHED_ITERATOR, MISSING_COPY_OR_ASSIGN, NEGATIVE_RETURNS, OVERLAPPING_COPY, OVERRUN, READLINK, REVERSE_NEGATIVE, SIZECHECK, SIZEOF_MISMATCH, STRING_NULL, STRING_OVERFLOW, STRING_SIZE, TAINTED_SCALAR, UNSAFE_FUNCTIONALITY, USER_POINTER, USE_AFTER_FREE, WRAPPER_ESCAPE
6.5.3: Insecure cryptographic storage	These Coverity checkers meet this requirement: BAD_CERT_VERIFICATION, CERT MSC00-J, CERT MSC18-C, CERT MSC30-C, CERT MSC32-C, DC.WEAK_CRYPTO, HARDCODED_CREDENTIALS, INSECURE_COMMUNICATION, INSECURE_COOKIE, INSECURE_RANDOM, INSECURE_SALT, PMD.ApexBadCrypto, PMD.ApexInsecureEndpoint, PREDICTABLE_RANDOM_SEED, RAILS_DEVISE_CONFIG, RISKY_CRYPTO, SA.RISKY_CRYPTO, SENSITIVE_DATA_LEAK, SIGMA.api_key_in_query_string_openapi, SIGMA.automatic_key_rotation_disabled_cloudformation_aws_kms, SIGMA.certificate_verification_disabled_ats_local_networking, SIGMA.certificate_verification_disabled_ats_transparency, SIGMA.certificate_verification_disabled_consul, SIGMA.certificate_verification_disabled_core_java, SIGMA.certificate_verification_disabled_grails_springsecurity, SIGMA.certificate_verification_disabled_kubernetes, SIGMA.certificate_verification_disabled_node_https, SIGMA.certificate_verification_disabled_node_libcurl, SIGMA.certificate_verification_disabled_node_mysql, SIGMA.certificate_verification_disabled_node_mysql2, SIGMA.certificate_verification_disabled_node_request_reject_unauthorized, SIGMA.certificate_verification_disabled_node_request_strict_ssl, SIGMA.certificate_verification_disabled_node_restify, SIGMA.certificate_verification_disabled_node_tls, SIGMA.certificate_verification_disabled_node_ws, SIGMA.certificate_verification_disabled_openapi_x_amazon_apigateway_integration, SIGMA.certificate_verification_disabled_sequelize, SIGMA.certificate_verification_disabled_sequelize_json, SIGMA.certificate_verification_disabled_sequelize_mssql, SIGMA.certificate_verification_disabled_sequelize_mssql_json, SIGMA.certificate_verification_disabled_socket_io, SIGMA.certificate_verification_disabled_spring_boot_cloudfoundry_properties, SIGMA.certificate_verification_disabled_spring_boot_cloudfoundry_yaml, SIGMA.cloud_storage_encryption_disabled_cloudformation_aws_s3_bucket, SIGMA.cloud_storage_encryption_disabled_terraform_google_storage_bucket, SIGMA.cors_with_credentials_http_origin_core_java, SIGMA.cors_with_credentials_http_origin_express_cors, SIGMA.cors_with_credentials_http_origin_koa, SIGMA.cors_with_credentials_http_origin_nestjs, SIGMA.cors_with_credentials_http_origin_openapi_x_a127, SIGMA.cors_with_credentials_http_origin_openapi_x_amazon_apigateway, SIGMA.cors_with_credentials_http_origin_openapi_x_amazon_apigateway_integration, SIGMA.cors_with_credentials_http_origin_servlet, SIGMA.cors_with_credentials_http_origin_spring_config, SIGMA.cors_with_credentials_http_origin_spring_corsconfiguration, SIGMA.cors_with_credentials_http_origin_spring_corsregistration, (cont. on next page)

PCI DSS requirement	Addressing compliance
6.5.3: Insecure cryptographic storage (cont.)	SIGMA.cors_with_credentials_http_origin_terraform_azurerm_app_service, SIGMA.credentials_validation_disabled_node_aws_sdk, SIGMA.database_encryption_disabled_cloudformation_doc_db, SIGMA.database_encryption_disabled_cloudformation_dynamo_db, SIGMA.database_encryption_disabled_cloudformation_neptune_cluster, SIGMA.database_encryption_disabled_cloudformation_rds_cluster, SIGMA.database_encryption_disabled_cloudformation_rds_instance, SIGMA.database_encryption_disabled_cloudformation_redshift_cluster, SIGMA.database_encryption_disabled_terraform_aws_athena, SIGMA.database_encryption_disabled_terraform_aws_rds, SIGMA.deprecated_http_client_apache_default_http_client, SIGMA.deprecated_http_client_apache_system_default_http_client, SIGMA.disk_encryption_disabled_cloudformation_aws_autoscaling, SIGMA.disk_encryption_disabled_cloudformation_dax, SIGMA.disk_encryption_disabled_cloudformation_efs, SIGMA.disk_encryption_disabled_cloudformation_elastic_cache_group, SIGMA.disk_encryption_disabled_cloudformation_elastic_search, SIGMA.disk_encryption_disabled_cloudformation_workspace_volume, SIGMA.disk_encryption_disabled_terraform_aws_dax, SIGMA.disk_encryption_disabled_terraform_aws_ebs, SIGMA.disk_encryption_disabled_terraform_aws_efs, SIGMA.disk_encryption_disabled_terraform_azurerm_managed_disk, SIGMA.empty_encryption_key_node_crypto, SIGMA.encryption_disabled_cloudformation_eks, SIGMA.encryption_disabled_ios_multipeer_connection, SIGMA.encryption_disabled_spring_security, SIGMA.encryption_disabled_terraform_aws_eks, SIGMA.expect_ct_disabled_express_helmet, SIGMA.hpkp_max_age_too_long_express, SIGMA.hpkp_max_age_too_long_koa, SIGMA.hpkp_report_uri_missing_tls_express, SIGMA.hpkp_report_uri_missing_tls_koa, SIGMA.hsts_http_header_subdomains_disabled_express_helmet, SIGMA.hsts_http_header_subdomains_disabled_express_hsts, SIGMA.improper_use_of_symmetric_cryptography_hazelcast_code, SIGMA.improper_use_of_symmetric_cryptography_hazelcast_xml, SIGMA.improper_use_of_symmetric_cryptography_hazelcast_yaml, SIGMA.insecure_cipher_core_java_block_cipher, SIGMA.insecure_cipher_core_java_block_cipher_mode, SIGMA.insecure_cipher_core_java_stream_cipher, SIGMA.insecure_tls_cipher_suite_cloudformation_load_balancer, SIGMA.insecure_tls_cipher_suite_node_https, SIGMA.insecure_tls_cipher_suite_node_request, SIGMA.insecure_tls_cipher_suite_node_tls, SIGMA.insecure_tls_version_ats_exception, SIGMA.insecure_tls_version_cloudformation_cloudfront, SIGMA.insecure_tls_version_cloudformation_elastic_search, SIGMA.insecure_tls_version_cloudformation_load_balancer, SIGMA.insecure_tls_version_core_java, SIGMA.insecure_tls_version_ios_protocol_max, SIGMA.insecure_tls_version_ios_protocol_min, SIGMA.insecure_tls_version_ios_stream_property, SIGMA.insecure_tls_version_kafka, SIGMA.insecure_tls_version_node_https, SIGMA.insecure_tls_version_node_request, SIGMA.insecure_tls_version_node_tls, SIGMA.insecure_tls_version_terraform_azurerm_app_service, SIGMA.insecure_tls_version_terraform_azurerm_postgresql, SIGMA.insecure_tls_version_terraform_azurerm_storage_account, SIGMA.insufficient_asymmetric_key_size_core_java, SIGMA.insufficient_symmetric_key_size_core_java, SIGMA.jwt_untrusted_decode_io_jsonwebtoken, SIGMA.jwt_untrusted_decode_jsonwebtoken, SIGMA.kms_encryption_service_disabled_kubernetes, SIGMA.login_over_http_spring_security, SIGMA.message_encryption_disabled_cloudformation_sns, SIGMA.message_encryption_disabled_cloudformation_sqs, SIGMA.missing_mtls_consul, SIGMA.missing_mtls_istio_port, SIGMA.missing_mtls_istio_service, SIGMA.missing_mtls_istio_workload, SIGMA.missing_mtls_kafka_broker, SIGMA.missing_mtls_rabbitmq, SIGMA.missing_perfect_forward_secrecy_ats_exception, SIGMA.missing_perfect_forward_secrecy_ats_temporary_exception, SIGMA.missing_perfect_forward_secrecy_ats_temporary_third_party_exception, SIGMA.missing_perfect_forward_secrecy_ats_third_party_exception, SIGMA.missing_secure_attribute_postman, SIGMA.missing_secure_attribute_remember_me_cookie_spring_security_code, SIGMA.missing_secure_attribute_remember_me_cookie_spring_security_config, SIGMA.missing_secure_attribute_servlet, SIGMA.missing_secure_attribute_session_cookie_express, SIGMA.missing_secure_attribute_session_cookie_grails, SIGMA.missing_secure_attribute_session_cookie_servlet_xml, SIGMA.missing_secure_attribute_session_cookie_spring_boot_properties, SIGMA.missing_secure_attribute_session_cookie_spring_boot_yaml, SIGMA.missing_tls_apache_http, SIGMA.missing_tls_apache_telnet, SIGMA.missing_tls_ats_arbitrary_loads, SIGMA.missing_tls_ats_arbitrary_loads_for_media, SIGMA.missing_tls_ats_arbitrary_loads_in_web_content, SIGMA.missing_tls_ats_domain_exception, SIGMA.missing_tls_ats_localhost_exception, SIGMA.missing_tls_ats_temporary_exception, SIGMA.missing_tls_ats_temporary_third_party_exception, SIGMA.missing_tls_ats_third_party_exception, SIGMA.missing_tls_axios, (cont. on next page)

PCI DSS requirement	Addressing compliance
6.5.3: Insecure cryptographic storage (cont.)	SIGMA.missing_tls_cloudformation_cloudfront, SIGMA .missing_tls_cloudformation_doc_db, SIGMA.missing_tls_cloudformation_elastic_cache, SIGMA.missing_tls_cloudformation_elastic_search, SIGMA.missing_tls_cloudformation_elastic_search_node_to_node, SIGMA.missing_tls_cloudformation_load_balancer, SIGMA.missing_tls_cloudformation_load_balancer_classic, SIGMA.missing_tls_common_properties, SIGMA.missing_tls_consul, SIGMA.missing_tls_consul_client, SIGMA.missing_tls_core_java_httprequest, SIGMA.missing_tls_core_java_httpurlconnection, SIGMA.missing_tls_got, SIGMA.missing_tls_hapi_session_mongo, SIGMA.missing_tls_java_unirest, SIGMA.missing_tls_kafka_broker, SIGMA.missing_tls_kafka_client, SIGMA.missing_tls_kafka_listener, SIGMA.missing_tls_node_aws_sdk, SIGMA.missing_tls_node_ftp, SIGMA.missing_tls_node_grpc, SIGMA.missing_tls_node_http, SIGMA.missing_tls_node_rest_client, SIGMA.missing_tls_node_telnet, SIGMA.missing_tls_node_telnet_client, SIGMA.missing_tls_openapi_oauth2_endpoint, SIGMA.missing_tls_openapi_ref, SIGMA.missing_tls_openapi_v2_base_uri, SIGMA.missing_tls_openapi_v3_base_uri, SIGMA.missing_tls_openapi_x_a127, SIGMA.missing_tls_openapi_x_amazon_apigateway_integration, SIGMA.missing_tls_openapi_x_google_backend, SIGMA.missing_tls_openapi_x_google_jwks, SIGMA.missing_tls_openapi_x_servers, SIGMA.missing_tls_postman, SIGMA.missing_tls_sequelize, SIGMA.missing_tls_socket_io_client, SIGMA.missing_tls_spring_boot_cassandra_properties, SIGMA.missing_tls_spring_boot_cassandra_yaml, SIGMA.missing_tls_spring_boot_couchbase_properties, SIGMA.missing_tls_spring_boot_couchbase_yaml, SIGMA.missing_tls_spring_boot_elasticsearch_properties, SIGMA.missing_tls_spring_boot_elasticsearch_yaml, SIGMA.missing_tls_spring_boot_management_server_properties, SIGMA.missing_tls_spring_boot_management_server_yaml, SIGMA.missing_tls_spring_boot_properties, SIGMA.missing_tls_spring_boot_rabbitmq_properties, SIGMA.missing_tls_spring_boot_rabbitmq_yaml, SIGMA.missing_tls_spring_boot_redis_properties, SIGMA.missing_tls_spring_boot_redis_yaml, SIGMA.missing_tls_spring_boot_yaml, SIGMA.missing_tls_spring_ftp, SIGMA.missing_tls_spring_resttemplate, SIGMA.missing_tls_terraform_aws_cloudfront, SIGMA.missing_tls_terraform_aws_docdb, SIGMA.missing_tls_terraform_aws_load_balancer, SIGMA.missing_tls_terraform_azurerm_app_service, SIGMA.missing_tls_terraform_azurerm_mysql, SIGMA.missing_tls_terraform_azurerm_postgresql, SIGMA.missing_tls_terraform_azurerm_storage_account, SIGMA.missing_tls_terraform_google_sql_db, SIGMA.missing_tls_websocket, SIGMA.missing_tls_ws, SIGMA.null_cipher_used_core_java, SIGMA.plaintext_storage_sensitive_data_kubernetes, SIGMA.plaintext_storage_sensitive_data_kubernetes_env_vars, SIGMA.plaintext_storage_sensitive_data_terraform_aws_ec2_user_data, SIGMA.plaintext_storage_sensitive_data_terraform_aws_lambda_env_vars, SIGMA.plaintext_storage_sensitive_data_terraform_azurerm_vm_custom_data, SIGMA.project_encryption_disabled_cloudformation_codebuild, SIGMA.project_encryption_disabled_terraform_aws_codebuild, SIGMA.query_encryption_disabled_terraform_aws_athena, SIGMA.rsa_no_padding_core_java, SIGMA.sasl_plain_enabled_kafka_broker, SIGMA.sasl_plain_enabled_kafka_client, SIGMA.sensitive_data_in_cookie_servlet, SIGMA.sensitive_data_in_query_string_openapi, SIGMA.sensitive_data_in_query_string_spring_security, SIGMA.unprotected_master_key_cloudformation_aws_kms, SIGMA.unsafe_authentication_filter_spring_security, SIGMA.unspecified_cipher_transformation_core_java, SIGMA.vendor_provided_encryption_key_cloudformation_cloudtrail, SIGMA.vendor_provided_encryption_key_cloudformation_efs, SIGMA.vendor_provided_encryption_key_terraform_google_compute, SIGMA.weak_hash_apache_commons_codec, SIGMA.weak_hash_core_java, SIGMA.weak_hash_node_crypto, SIGMA.weak_password_hash_grails_springsecurity, SIGMA.weak_password_hash_spring_security_code, SIGMA.weak_password_hash_spring_security_config, STRICT_TRANSPORT_SECURITY, UNENCRYPTED_SENSITIVE_DATA, UNSAFE_BASIC_AUTH, UNSAFE_SESSION_SETTING, WEAK_PASSWORD_HASH

PCI DSS requirement	Addressing compliance
6.5.4: Insecure communications	These Coverity checkers meet this requirement: BAD_CERT_VERIFICATION, CERT MSC00-J, CERT MSC18-C, CORS_MISCONFIGURATION_AUDIT, HARDCODED_CREDENTIALS, IMPLICIT_INTENT, INSECURE_COMMUNICATION, INSECURE_COOKIE, INSECURE_NETWORK_BIND, INSECURE_REFERRER_POLICY, INSECURE_SALT, MISSING_PERMISSION_FOR_BROADCAST, PMD.ApexBadCrypto, PMD.ApexInsecureEndpoint, RAILS_DEVISE_CONFIG, RISKY_CRYPTO, SA.RISKY_CRYPTO, SECURE_TEMP, SENSITIVE_DATA_LEAK, SIGMA.api_key_in_query_string_openapi, SIGMA.automatic_key_rotation_disabled_cloudformation_aws_kms, SIGMA.certificate_verification_disabled_ats_local_networking, SIGMA.certificate_verification_disabled_ats_transparency, SIGMA.certificate_verification_disabled_consul, SIGMA.certificate_verification_disabled_core_java, SIGMA.certificate_verification_disabled_grails_springsecurity, SIGMA.certificate_verification_disabled_kubernetes, SIGMA.certificate_verification_disabled_node_https, SIGMA.certificate_verification_disabled_node_libcurl, SIGMA.certificate_verification_disabled_node_mysql, SIGMA.certificate_verification_disabled_node_mysql2, SIGMA.certificate_verification_disabled_node_request_reject_unauthorized, SIGMA.certificate_verification_disabled_node_request_strict_ssl, SIGMA.certificate_verification_disabled_node_restify, SIGMA.certificate_verification_disabled_node_tls, SIGMA.certificate_verification_disabled_node_ws, SIGMA.certificate_verification_disabled_openapi_x_amazon_apigateway_integration, SIGMA.certificate_verification_disabled_sequelize, SIGMA.certificate_verification_disabled_sequelize_json, SIGMA.certificate_verification_disabled_sequelize_mssql, SIGMA.certificate_verification_disabled_sequelize_mssql_json, SIGMA.certificate_verification_disabled_socket_io, SIGMA.certificate_verification_disabled_spring_boot_cloudfoundry_properties, SIGMA.certificate_verification_disabled_spring_boot_cloudfoundry_yaml, SIGMA.cloud_storage_encryption_disabled_cloudformation_aws_s3_bucket, SIGMA.cloud_storage_encryption_disabled_terraform_google_storage_bucket, SIGMA.cors_with_credentials_http_origin_core_java, SIGMA.cors_with_credentials_http_origin_express_cors, SIGMA.cors_with_credentials_http_origin_koa, SIGMA.cors_with_credentials_http_origin_nestjs, SIGMA.cors_with_credentials_http_origin_openapi_x_a127, SIGMA.cors_with_credentials_http_origin_openapi_x_amazon_apigateway, SIGMA.cors_with_credentials_http_origin_openapi_x_amazon_apigateway_integration, SIGMA.cors_with_credentials_http_origin_servlet, SIGMA.cors_with_credentials_http_origin_spring_config, SIGMA.cors_with_credentials_http_origin_spring_corsconfiguration, SIGMA.cors_with_credentials_http_origin_spring_corsregistration, SIGMA.cors_with_credentials_http_origin_terraform_azurerm_app_service, SIGMA.credentials_validation_disabled_node_aws_sdk, SIGMA.database_encryption_disabled_cloudformation_doc_db, SIGMA.database_encryption_disabled_cloudformation_dynamo_db, SIGMA.database_encryption_disabled_cloudformation_neptune_cluster, SIGMA.database_encryption_disabled_cloudformation_rds_cluster, SIGMA.database_encryption_disabled_cloudformation_rds_instance, SIGMA.database_encryption_disabled_cloudformation_redshift_cluster, SIGMA.database_encryption_disabled_terraform_aws_athena, SIGMA.database_encryption_disabled_terraform_aws_rds, SIGMA.deprecated_http_client_apache_default_http_client, SIGMA.deprecated_http_client_apache_system_default_http_client, SIGMA.disk_encryption_disabled_cloudformation_aws_autoscaling, SIGMA.disk_encryption_disabled_cloudformation_dax, SIGMA.disk_encryption_disabled_cloudformation_efs, SIGMA.disk_encryption_disabled_cloudformation_elastic_cache_group, SIGMA.disk_encryption_disabled_cloudformation_elastic_search, SIGMA.disk_encryption_disabled_cloudformation_workspace_volume, SIGMA.disk_encryption_disabled_terraform_aws_dax, SIGMA.disk_encryption_disabled_terraform_aws_ebs, SIGMA.disk_encryption_disabled_terraform_aws_efs, SIGMA.disk_encryption_disabled_terraform_azurerm_managed_disk, SIGMA.empty_encryption_key_node_crypto, SIGMA.encryption_disabled_cloudformation_eks, SIGMA.encryption_disabled_ios_multipeer_connection, SIGMA.encryption_disabled_spring_security, SIGMA.encryption_disabled_terraform_aws_eks, SIGMA.expect_ct_disabled_express_helmet, SIGMA.hpkp_max_age_too_long_express, SIGMA.hpkp_max_age_too_long_koa, SIGMA.hpkp_report_uri_missing_tls_express, SIGMA.hpkp_report_uri_missing_tls_koa, SIGMA.hsts_http_header_subdomains_disabled_express_helmet, SIGMA.hsts_http_header_subdomains_disabled_express_hsts, SIGMA.improper_use_of_symmetric_cryptography_hazelcast_code, SIGMA.improper_use_of_symmetric_cryptography_hazelcast_xml, SIGMA.improper_use_of_symmetric_cryptography_hazelcast_yaml, (cont. on next page)

PCI DSS requirement	Addressing compliance
6.5.4: Insecure communications (cont.)	SIGMA.insecure_cipher_core_java_block_cipher, SIGMA.insecure_cipher_core_java_block_cipher_mode, SIGMA.insecure_cipher_core_java_stream_cipher, SIGMA.insecure_tls_cipher_suite_cloudformation_load_balancer, SIGMA.insecure_tls_cipher_suite_node_https, SIGMA.insecure_tls_cipher_suite_node_request, SIGMA.insecure_tls_cipher_suite_node_tls, SIGMA.insecure_tls_version_ats_exception, SIGMA.insecure_tls_version_cloudformation_cloudfront, SIGMA.insecure_tls_version_cloudformation_elastic_search, SIGMA.insecure_tls_version_cloudformation_load_balancer, SIGMA.insecure_tls_version_core_java, SIGMA.insecure_tls_version_ios_protocol_max, SIGMA.insecure_tls_version_ios_protocol_min, SIGMA.insecure_tls_version_ios_stream_property, SIGMA.insecure_tls_version_kafka, SIGMA.insecure_tls_version_node_https, SIGMA.insecure_tls_version_node_request, SIGMA.insecure_tls_version_node_tls, SIGMA.insecure_tls_version_terraform_azurerm_app_service, SIGMA.insecure_tls_version_terraform_azurerm_postgresql, SIGMA.insecure_tls_version_terraform_azurerm_storage_account, SIGMA.insufficient_asymmetric_key_size_core_java, SIGMA.insufficient_symmetric_key_size_core_java, SIGMA.kms_encryption_service_disabled_kubernetes, SIGMA.login_over_http_spring_security, SIGMA.message_encryption_disabled_cloudformation_sns, SIGMA.message_encryption_disabled_cloudformation_sqs, SIGMA.missing_mtls_consul, SIGMA.missing_mtls_istio_port, SIGMA.missing_mtls_istio_service, SIGMA.missing_mtls_istio_workload, SIGMA.missing_mtls_kafka_broker, SIGMA.missing_mtls_rabbitmq, SIGMA.missing_perfect_forward_secrecy_ats_exception, SIGMA.missing_perfect_forward_secrecy_ats_temporary_exception, SIGMA.missing_perfect_forward_secrecy_ats_temporary_third_party_exception, SIGMA.missing_perfect_forward_secrecy_ats_third_party_exception, SIGMA.missing_secure_attribute_postman, SIGMA.missing_secure_attribute_remember_me_cookie_spring_security_code, SIGMA.missing_secure_attribute_remember_me_cookie_spring_security_config, SIGMA.missing_secure_attribute_servlet, SIGMA.missing_secure_attribute_session_cookie_express, SIGMA.missing_secure_attribute_session_cookie_grails, SIGMA.missing_secure_attribute_session_cookie_servlet_xml, SIGMA.missing_secure_attribute_session_cookie_spring_boot_properties, SIGMA.missing_secure_attribute_session_cookie_spring_boot_yaml, SIGMA.missing_tls_apache_http, SIGMA.missing_tls_apache_telnet, SIGMA.missing_tls_ats_arbitrary_loads, SIGMA.missing_tls_ats_arbitrary_loads_for_media, SIGMA.missing_tls_ats_arbitrary_loads_in_web_content, SIGMA.missing_tls_ats_domain_exception, SIGMA.missing_tls_ats_localhost_exception, SIGMA.missing_tls_ats_temporary_exception, SIGMA.missing_tls_ats_temporary_third_party_exception, SIGMA.missing_tls_ats_third_party_exception, SIGMA.missing_tls_axios, SIGMA.missing_tls_cloudformation_cloudfront, SIGMA.missing_tls_cloudformation_doc_db, SIGMA.missing_tls_cloudformation_elastic_cache, SIGMA.missing_tls_cloudformation_elastic_search, SIGMA.missing_tls_cloudformation_elastic_search_node_to_node, SIGMA.missing_tls_cloudformation_load_balancer, SIGMA.missing_tls_cloudformation_load_balancer_classic, SIGMA.missing_tls_common_properties, SIGMA.missing_tls_consul, SIGMA.missing_tls_consul_client, SIGMA.missing_tls_core_java_httprequest, SIGMA.missing_tls_core_java_httpurlconnection, SIGMA.missing_tls_got, SIGMA.missing_tls_hapi_session_mongo, SIGMA.missing_tls_java_unirest, SIGMA.missing_tls_kafka_broker, SIGMA.missing_tls_kafka_client, SIGMA.missing_tls_kafka_listener, SIGMA.missing_tls_node_aws_sdk, SIGMA.missing_tls_node_ftp, SIGMA.missing_tls_node_grpc, SIGMA.missing_tls_node_http, SIGMA.missing_tls_node_rest_client, SIGMA.missing_tls_node_telnet, SIGMA.missing_tls_node_telnet_client, SIGMA.missing_tls_openapi_oauth2_endpoint, SIGMA.missing_tls_openapi_ref, SIGMA.missing_tls_openapi_v2_base_uri, SIGMA.missing_tls_openapi_v3_base_uri, SIGMA.missing_tls_openapi_x_a127, SIGMA.missing_tls_openapi_x_amazon_apigateway_integration, SIGMA.missing_tls_openapi_x_google_backend, SIGMA.missing_tls_openapi_x_google_jwks, SIGMA.missing_tls_openapi_x_servers, SIGMA.missing_tls_postman, SIGMA.missing_tls_sequelize, SIGMA.missing_tls_socket_io_client, SIGMA.missing_tls_spring_boot_cassandra_properties, SIGMA.missing_tls_spring_boot_cassandra_yaml, SIGMA.missing_tls_spring_boot_couchbase_properties, SIGMA.missing_tls_spring_boot_couchbase_yaml, SIGMA.missing_tls_spring_boot_elasticsearch_properties, SIGMA.missing_tls_spring_boot_elasticsearch_yaml, SIGMA.missing_tls_spring_boot_management_server_properties, SIGMA.missing_tls_spring_boot_management_server_yaml, SIGMA.missing_tls_spring_boot_properties, SIGMA.missing_tls_spring_boot_rabbitmq_properties, SIGMA.missing_tls_spring_boot_rabbitmq_yaml, SIGMA.missing_tls_spring_boot_redis_properties, SIGMA.missing_tls_spring_boot_redis_yaml, SIGMA.missing_tls_spring_boot_yaml, SIGMA.missing_tls_spring_ftp, SIGMA.missing_tls_spring_resttemplate, (cont. on next page)

PCI DSS requirement	Addressing compliance
6.5.4: Insecure communications (cont.)	SIGMA.missing_tls_terraform_aws_cloudfront, SIGMA.missing_tls_terraform_aws_docdb, SIGMA.missing_tls_terraform_aws_load_balancer, SIGMA.missing_tls_terraform_azurerm_app_service, SIGMA.missing_tls_terraform_azurerm_mysql, SIGMA.missing_tls_terraform_azurerm_postgresql, SIGMA.missing_tls_terraform_azurerm_storage_account, SIGMA.missing_tls_terraform_google_sql_db, SIGMA.missing_tls_websocket, SIGMA.missing_tls_ws, SIGMA.null_cipher_used_core_java, SIGMA.plaintext_storage_sensitive_data_kubernetes, SIGMA.plaintext_storage_sensitive_data_kubernetes_env_vars, SIGMA.plaintext_storage_sensitive_data_terraform_aws_ec2_user_data, SIGMA.plaintext_storage_sensitive_data_terraform_aws_lambda_env_vars, SIGMA.plaintext_storage_sensitive_data_terraform_azurerm_vm_custom_data, SIGMA.project_encryption_disabled_cloudformation_codebuild, SIGMA.project_encryption_disabled_terraform_aws_codebuild, SIGMA.query_encryption_disabled_terraform_aws_athena, SIGMA.rsa_no_padding_core_java, SIGMA.sasl_plain_enabled_kafka_broker, SIGMA.sasl_plain_enabled_kafka_client, SIGMA.sensitive_data_in_cookie_servlet, SIGMA.sensitive_data_in_query_string_openapi, SIGMA.sensitive_data_in_query_string_spring_security, SIGMA.unprotected_master_key_cloudformation_aws_kms, SIGMA.unspecified_cipher_transformation_core_java, SIGMA.vendor_provided_encryption_key_cloudformation_cloudtrail, SIGMA.vendor_provided_encryption_key_cloudformation_efs, SIGMA.vendor_provided_encryption_key_terraform_google_compute, SIGMA.weak_hash_apache_commons_codec, SIGMA.weak_hash_core_java, SIGMA.weak_hash_node_crypto, SIGMA.weak_password_hash_grails_springsecurity, SIGMA.weak_password_hash_spring_security_code, SIGMA.weak_password_hash_spring_security_config, STRICT_TRANSPORT_SECURITY, TAINTED_SCALAR, UNENCRYPTED_SENSITIVE_DATA, UNSAFE_BASIC_AUTH, UNSAFE_BUFFER_METHOD, UNSAFE_SESSION_SETTING, WEAK_PASSWORD_HASH
6.5.5: Improper error handling	These Coverity checkers meet this requirement*: ANDROID_DEBUG_MODE, BAD_COMPARE, CHECKED_RETURN, CONFIG.ENABLED_DEBUG_MODE, CONFIG.ENABLED_TRACE_MODE, CONFIG.MISSING_CUSTOM_ERROR_PAGE, EXPRESS_WINSTON_SENSITIVE_LOGGING, FB.DE_MIGHT_DROP, FB.DE_MIGHT_IGNORE, FB.DM_EXIT, FB.REC_CATCH_EXCEPTION, FB.RV_RETURN_VALUE_IGNORED_BAD_PRACTICE, INSUFFICIENT_LOGGING, LOCK, MISSING_THROW, NEGATIVE_RETURNS, ORM_LOAD_NULL_CHECK, PMD.ApexSharingViolations, REVERSE_NEGATIVE, SENSITIVE_DATA_LEAK, SIGMA.cookie_logging_enabled_spring_boot, SIGMA.cookie_logging_enabled_spring_boot_properties, SIGMA.hide_powered_by_disabled_express_helmet, SIGMA.insufficient_log_retention_terraform_azurerm, SIGMA.insufficient_logging_terraform_aws_api_gateway, SIGMA.insufficient_logging_terraform_azurerm, SIGMA.logging_disabled_cloudformation_aws_s3_bucket, SIGMA.logging_disabled_consul, SIGMA.logging_disabled_istio, SIGMA.logging_disabled_kubernetes, SIGMA.logging_disabled_terraform_aws_load_balancer, SIGMA.logging_disabled_terraform_aws_s3_bucket, SIGMA.logging_request_parameters_grails, SIGMA.missing_default_response_object_openapi, SIGMA.missing_global_exception_handler_servlet, SIGMA.missing_global_exception_handler_struts2, SIGMA.missing_global_exception_handler_winston, SIGMA.query_logging_enabled_sequelize, SIGMA.request_logging_enabled_spring_boot, SIGMA.request_logging_enabled_spring_boot_properties, SIGMA.verbose_error_message_spring_boot_exception_code, SIGMA.verbose_error_message_spring_boot_exception_properties, SIGMA.verbose_error_message_spring_boot_exception_yaml, SIGMA.verbose_error_message_spring_boot_stacktrace_properties, SIGMA.verbose_error_message_spring_boot_stacktrace_yaml, SUPPRESSED_ERROR, TAINTED_SCALAR, UNCAUGHT_EXCEPT, UNLOGGED_SECURITY_EXCEPTION

PCI DSS requirement	Addressing compliance
6.5.6: All “high risk” vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1). v	These Coverity checkers meet this requirement*: ALLOC_FREE_MISMATCH, ANDROID_CAPABILITY_LEAK, ANGULAR_BYPASS_SECURITY, ANGULAR_ELEMENT_REFERENCE, ANGULAR_EXPRESSION_INJECTION, ANGULAR_SCE_DISABLED, ANONYMOUS_DB_CONNECTION, ARRAY_VS_SINGLETON, BAD_ALLOC_ARITHMETIC, BAD_ALLOC_STRLEN, BAD_CERT_VERIFICATION, BAD_FREE, BUFFER_SIZE, COM.BAD_FREE, COM.BSTR.ALLOC, COM.BSTR.CONV, CONFIG.ASP_VIEWSTATE_MAC, CONFIG.BEEGO_CSRF_PROTECTION_DISABLED, CONFIG.CONNECTION_STRING_PASSWORD, CONFIG.COOKIE_SIGNING_DISABLED, CONFIG.DEAD_AUTHORIZATION_RULE, CONFIG.DJANGO_CSRF_PROTECTION_DISABLED, CONFIG.ENABLED_DEBUG_MODE, CONFIG.ENABLED_TRACE_MODE, CONFIG.HANA_XS_PREVENT_XSRF_DISABLED, CONFIG.HARDCODED_CREDENTIALS_AUDIT, CONFIG.HARDCODED_TOKEN, CONFIG.HTTP_VERB_TAMPERING, CONFIG.JAVAEE_MISSING_HTTPONLY, CONFIG.MISSING_CUSTOM_ERROR_PAGE, CONFIG.SYMFONY_CSRF_PROTECTION_DISABLED, CONFIG.UNSAFE_SESSION_TIMEOUT, COOKIE_INJECTION, CORS_MISCONFIGURATION, CORS_MISCONFIGURATION_AUDIT, CSRF, CSS_INJECTION, DOM_XSS, DYNAMIC_OBJECT_ATTRIBUTES, EL_INJECTION, FB.BC_NULL_INSTANCEOF, FB.BX_BOXING_IMMEDIATELY_UNBOXED_TO_PERFORM_COERCION, FB.DMI_CONSTANT_DB_PASSWORD, FB.DMI_EMPTY_DB_PASSWORD, FB.FI_PUBLIC_SHOULD_BE_PROTECTED, FB.HRS_REQUEST_PARAMETER_TO_COOKIE, FB.HRS_REQUEST_PARAMETER_TO_HTTP_HEADER, FB.ICAST_BAD_SHIFT_AMOUNT, FB.ICAST_IDIV_CAST_TO_DOUBLE, FB.ICAST_INTEGER_MULTIPLY_CAST_TO_LONG, FB.ICAST_INT_2_LONG_AS_INSTANT, FB.ICAST_INT_CAST_TO_DOUBLE_PASSED_TO_CEIL, FB.ICAST_INT_CAST_TO_FLOAT_PASSED_TO_ROUND, FB.ICAST_QUESTIONABLE_UNSIGNED_RIGHT_SHIFT, FB.NP_ALWAYS_NULL, FB.NP_ALWAYS_NULL_EXCEPTION, FB.NP_ARGUMENT_MIGHT_BE_NULL, FB.NP_BOOLEAN_RETURN_NULL, FB.NP_CLONE_COULD_RETURN_NULL, FB.NP_CLOSING_NULL, FB.NP_DEREFERENCE_OF_READLINE_VALUE, FB.NP_DOES_NOT_HANDLE_NULL, FB.NP_EQUALS_SHOULD_HANDLE_NULL_ARGUMENT, FB.NP_FIELD_NOT_INITIALIZED_IN_CONSTRUCTOR, FB.NP_GUARANTEED_DEREF, FB.NP_GUARANTEED_DEREF_ON_EXCEPTION_PATH, FB.NP_IMMEDIATE_DEREFERENCE_OF_READLINE, FB.NP_LOAD_OF_KNOWN_NULL_VALUE, FB.NP_METHOD_PARAMETER_RELAXING_ANNOTATION, FB.NP_METHOD_PARAMETER_TIGHTENS_ANNOTATION, FB.NP_METHOD_RETURN_RELAXING_ANNOTATION, FB.NP_NONNULL_FIELD_NOT_INITIALIZED_IN_CONSTRUCTOR, FB.NP_NONNULL_PARAM_VIOLATION, FB.NP_NONNULL_RETURN_VIOLATION, FB.NP_NULL_INSTANCEOF, FB.NP_NULL_ON_SOME_PATH, FB.NP_NULL_ON_SOME_PATH_EXCEPTION, FB.NP_NULL_ON_SOME_PATH_FROM_RETURN_VALUE, FB.NP_NULL_ON_SOME_PATH_MIGHT_BE_INFEASIBLE, FB.NP_NULL_PARAM_DEREF, FB.NP_NULL_PARAM_DEREF_ALL_TARGETS_DANGEROUS, FB.NP_NULL_PARAM_DEREF_NONVIRTUAL, FB.NP_OPTIONAL_RETURN_NULL, FB.NP_PARAMETER_MUST_BE_NONNULL_BUT_MARKED_AS_NULLABLE, FB.NP_STORE_INTO_NONNULL_FIELD, FB.NP_TOSTRING_COULD_RETURN_NULL, FB.NP_UNWRITTEN_FIELD, FB.NP_UNWRITTEN_PUBLIC_OR_PROTECTED_FIELD, FB.PT_ABSOLUTE_PATH_TRAVERSAL, FB.PT_RELATIVE_PATH_TRAVERSAL, FB.RCN_REDUNDANT_COMPARISON_OF_NULL_AND_NONNULL_VALUE, FB.RCN_REDUNDANT_COMPARISON_TWO_NULL_VALUES, FB.RCN_REDUNDANT_NULLCHECK_OF_NONNULL_VALUE, FB.RCN_REDUNDANT_NULLCHECK_OF_NULL_VALUE, FB.RCN_REDUNDANT_NULLCHECK_WOULD_HAVE_BEEN_A_NPE, FB.SQL_NONCONSTANT_STRING_PASSED_TO_EXECUTE, FB.SQL_PREPARED_STATEMENT_GENERATED_FROM_NONCONSTANT_STRING, FB.XSS_REQUEST_PARAMETER_TO_JSP_WRITER, FB.XSS_REQUEST_PARAMETER_TO_SEND_ERROR, FB.XSS_REQUEST_PARAMETER_TO_SERVLET_WRITER, FORMAT_STRING_INJECTION, FORWARD_NULL, HARDCODED_CREDENTIALS, HEADER_INJECTION, HOST_HEADER_VALIDATION_DISABLED, IMPLICIT_INTENT, INCOMPATIBLE_CAST, INSECURE_COMMUNICATION, INSECURE_COOKIE, INSECURE_CSP, INSECURE_DIRECT_OBJECT_REFERENCE, INSECURE_FILE_PERMISSIONS, INSECURE_RANDOM, INSECURE_SALT, INTEGER_OVERFLOW, INVALIDATE_ITERATOR, JAVA_CODE_INJECTION, JCR_INJECTION, JINJA2_AUTOESCAPE_DISABLED, JSP_DYNAMIC_INCLUDE, JSP_SQL_INJECTION, LDAP_INJECTION, LDAP_NOT_CONSTANT, LOCALSTORAGE_MANIPULATION, LOG_INJECTION, MISMATCHED_ITERATOR, MISSING_AUTHZ, MISSING_COPY_OR_ASSIGN, MISSING_PASSWORD_VALIDATOR, MISSING_PERMISSION_FOR_BROADCAST, MISSING_PERMISSION_ON_EXPORTED_COMPONENT, MOBILE_ID_MISUSE, NEGATIVE_RETURNS, NESTING_INDENT_MISMATCH, NOSQL_QUERY_INJECTION, NULL_RETURNS, OAUTH2_MISCONFIGURATION, OGNL_INJECTION, OPEN_REDIRECT, OS_CMD_INJECTION, OVERFLOW_BEFORE_WIDEN, OVERRUN, PATH_MANIPULATION, PMD.ApexBadCrypto, PMD.ApexCRUDViolation, PMD.ApexInsecureEndpoint, (cont. on next page)

PCI DSS requirement	Addressing compliance
6.5.6: All “high risk” vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1). (cont.)	PMD.ApexOpenRedirect, PMD.ApexSOQLInjection, PMD.ApexSharingViolations, PMD.ApexSuggestUsingNamedCred, PMD.ApexXSSFromEscapeFalse, PMD.ApexXSSFromURLParam, PMD.VfCsrf, PMD.VfHtmlStyleTagXss, PMD.VfUnescapeEl, PREDICTABLE_RANDOM_SEED, PW.INTEGER_OVERFLOW, PW.INTEGER_TOO_LARGE, PW.NON_CONST_PRINTF_FORMAT_STRING, PW.SHIFT_COUNT_TOO_LARGE, RAILS_DEFAULT_ROUTES, RAILS_DEVISE_CONFIG, RAILS_MISSING_FILTER_ACTION, READLINK, REGEX_INJECTION, REVERSE_INULL, REVERSE_NEGATIVE, REVERSE_TABNABBING, RISKY_CRYPTO, RUBY_VULNERABLE_LIBRARY, SA.RISKY_CRYPTO, SCRIPT_CODE_INJECTION, SENSITIVE_DATA_LEAK, SESSIONSTORAGE_MANIPULATION, SESSION_FIXATION, SIGMA.access_control_disabled_consul, SIGMA.access_control_disabled_openapi, SIGMA.access_control_disabled_openapi_x_amazon_apigateway, SIGMA.access_control_disabled_openapi_x_google, SIGMA.access_control_disabled_openapi_x_google_backend, SIGMA.access_control_disabled_openapi_x_wso2, SIGMA.access_control_disabled_zookeeper, SIGMA.admin_access_enabled_spring_boot, SIGMA.admin_dashboard_publicly_accessible_kubernetes, SIGMA.allow_all_authz_policy_istio, SIGMA.allow_all_authz_policy_node_aws_sdk_s3_bucket, SIGMA.allow_all_authz_policy_node_aws_sdk_s3_object, SIGMA.allow_all_authz_policy_node_google_cloud_storage_bucket, SIGMA.allow_all_authz_policy_terraform_aws_ecr, SIGMA.allow_all_authz_policy_terraform_google_big_query, SIGMA.allow_all_authz_policy_terraform_google_storage_bucket, SIGMA.anonymous_access_enabled_kubernetes, SIGMA.anonymous_access_enabled_rabbitmq_local, SIGMA.anonymous_access_enabled_rabbitmq_remote, SIGMA.api_key_auth_enabled_openapi_v2, SIGMA.api_key_auth_enabled_openapi_v3, SIGMA.api_key_in_query_string_openapi, SIGMA.apparmour_default_configuration_override_kubernetes, SIGMA.automatic_key_rotation_disabled_cloudformation_aws_kms, SIGMA.basic_auth_enabled_cloudformation_aws_amplify, SIGMA.basic_auth_enabled_kubernetes, SIGMA.basic_auth_enabled_openapi_v2, SIGMA.basic_auth_enabled_openapi_v3, SIGMA.basic_auth_enabled_postman, SIGMA.basic_auth_enabled_terraform_azurerm_vm, SIGMA.basic_auth_enabled_terraform_gke, SIGMA.certificate_verification_disabled_ats_local_networking, SIGMA.certificate_verification_disabled_ats_transparency, SIGMA.certificate_verification_disabled_consul, SIGMA.certificate_verification_disabled_core_java, SIGMA.certificate_verification_disabled_grails_springsecurity, SIGMA.certificate_verification_disabled_kubernetes, SIGMA.certificate_verification_disabled_node_https, SIGMA.certificate_verification_disabled_node_libcurl, SIGMA.certificate_verification_disabled_node_mysql, SIGMA.certificate_verification_disabled_node_mysql2, SIGMA.certificate_verification_disabled_node_request_reject_unauthorized, SIGMA.certificate_verification_disabled_node_request_strict_ssl, SIGMA.certificate_verification_disabled_node_restify, SIGMA.certificate_verification_disabled_node_tls, SIGMA.certificate_verification_disabled_node_ws, SIGMA.certificate_verification_disabled_openapi_x_amazon_apigateway_integration, SIGMA.certificate_verification_disabled_sequelize, SIGMA.certificate_verification_disabled_sequelize_json, SIGMA.certificate_verification_disabled_sequelize_mssql, SIGMA.certificate_verification_disabled_sequelize_mssql_json, SIGMA.certificate_verification_disabled_socket_io, SIGMA.certificate_verification_disabled_spring_boot_cloudfoundry_properties, SIGMA.certificate_verification_disabled_spring_boot_cloudfoundry_yaml, SIGMA.cloud_gateway_publicly_accessible_cloudformation_aws_apigateway, SIGMA.cloud_resource_assigned_public_ip_cloudformation_aws_ec2_subnet, SIGMA.cloud_resource_assigned_public_ip_cloudformation_aws_rds, SIGMA.cloud_resource_assigned_public_ip_cloudformation_sagemaker_notebook, SIGMA.cloud_resource_assigned_public_ip_terraform_aws_ec2, SIGMA.cloud_resource_assigned_public_ip_terraform_aws_eks, SIGMA.cloud_resource_assigned_public_ip_terraform_aws_mq_broker, SIGMA.cloud_resource_assigned_public_ip_terraform_aws_rds, SIGMA.cloud_resource_assigned_public_ip_terraform_google_compute, SIGMA.cloud_service_authn_disabled_terraform_azurerm_app_service, SIGMA.cloud_service_authz_disabled_cloudformation_aws_apigateway, SIGMA.cloud_storage_allows_public_config_cloudformation_aws_s3_bucket, SIGMA.cloud_storage_allows_public_config_terraform_aws_s3_bucket, SIGMA.cloud_storage_default_allow_all_terraform_azurerm_storage_account, SIGMA.cloud_storage_encryption_disabled_cloudformation_aws_s3_bucket, SIGMA.cloud_storage_encryption_disabled_terraform_google_storage_bucket, SIGMA.cloud_storage_publicly_accessible_cloudformation_aws_s3_bucket, SIGMA.config_browser_plugin_enabled_struts2, SIGMA.conflicting_names_servlet, SIGMA.container_empty_security_context_kubernetes, SIGMA.container_hostport_binding_kubernetes, SIGMA.container_insecure_bind_address_kubernetes, SIGMA.container_privilege_escalation_allowed_kubernetes, SIGMA.container_requesting_net_raw_kubernetes, SIGMA.container_requesting_sys_admin_kubernetes, SIGMA.container_running_as_root_kubernetes, SIGMA.container_sharing_host_ipc_namespace_kubernetes, SIGMA.container_sharing_host_pid_namespace_kubernetes, (cont. on next page)

PCI DSS requirement	Addressing compliance
6.5.6: All "high risk" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1). (cont.)	SIGMA.content_security_policy_disabled_express_helmet, SIGMA.cors_configured_globally_express_cors, SIGMA.cors_configured_globally_koa, SIGMA.cors_no_credentials_permissive_origin_apollo_graphql, SIGMA.cors_no_credentials_permissive_origin_cloudformation_aws_s3_bucket, SIGMA.cors_no_credentials_permissive_origin_core_java, SIGMA.cors_no_credentials_permissive_origin_express_cors, SIGMA.cors_no_credentials_permissive_origin_kafka_broker, SIGMA.cors_no_credentials_permissive_origin_koa, SIGMA.cors_no_credentials_permissive_origin_nestjs, SIGMA.cors_no_credentials_permissive_origin_openapi_x_a127, SIGMA.cors_no_credentials_permissive_origin_openapi_x_amazon_apigateway, SIGMA.cors_no_credentials_permissive_origin_openapi_x_amazon_apigateway_integration, SIGMA.cors_no_credentials_permissive_origin_postman, SIGMA.cors_no_credentials_permissive_origin_servlet, SIGMA.cors_no_credentials_permissive_origin_spring_config, SIGMA.cors_no_credentials_permissive_origin_spring_corsconfiguration, SIGMA.cors_no_credentials_permissive_origin_spring_corsregistration, SIGMA.cors_no_credentials_permissive_origin_terraform_aws_s3_bucket, SIGMA.cors_no_credentials_permissive_origin_terraform_azurerm_app_service, SIGMA.cors_no_credentials_permissive_origin_terraform_google_storage_bucket, SIGMA.cors_preflight_age_too_long_cloudformation_aws_s3_bucket, SIGMA.cors_preflight_age_too_long_core_java, SIGMA.cors_preflight_age_too_long_express_cors, SIGMA.cors_preflight_age_too_long_koa, SIGMA.cors_preflight_age_too_long_nestjs, SIGMA.cors_preflight_age_too_long_openapi_x_a127, SIGMA.cors_preflight_age_too_long_openapi_x_amazon_apigateway, SIGMA.cors_preflight_age_too_long_openapi_x_amazon_apigateway_integration, SIGMA.cors_preflight_age_too_long_servlet, SIGMA.cors_preflight_age_too_long_spring_config, SIGMA.cors_preflight_age_too_long_spring_corsconfiguration, SIGMA.cors_preflight_age_too_long_spring_corsregistration, SIGMA.cors_preflight_age_too_long_terraform_aws_s3_bucket, SIGMA.cors_preflight_age_too_long_terraform_google_storage_bucket, SIGMA.cors_with_credentials_all_origin_core_java, SIGMA.cors_with_credentials_all_origin_express_cors, SIGMA.cors_with_credentials_all_origin_koa, SIGMA.cors_with_credentials_all_origin_nestjs, SIGMA.cors_with_credentials_all_origin_openapi_x_a127, SIGMA.cors_with_credentials_all_origin_openapi_x_amazon_apigateway, SIGMA.cors_with_credentials_all_origin_openapi_x_amazon_apigateway_integration, SIGMA.cors_with_credentials_all_origin_servlet, SIGMA.cors_with_credentials_all_origin_spring_config, SIGMA.cors_with_credentials_all_origin_spring_corsconfiguration, SIGMA.cors_with_credentials_all_origin_spring_corsregistration, SIGMA.cors_with_credentials_all_origin_terraform_azurerm_app_service, SIGMA.cors_with_credentials_http_origin_core_java, SIGMA.cors_with_credentials_http_origin_express_cors, SIGMA.cors_with_credentials_http_origin_koa, SIGMA.cors_with_credentials_http_origin_nestjs, SIGMA.cors_with_credentials_http_origin_openapi_x_a127, SIGMA.cors_with_credentials_http_origin_openapi_x_amazon_apigateway, SIGMA.cors_with_credentials_http_origin_openapi_x_amazon_apigateway_integration, SIGMA.cors_with_credentials_http_origin_servlet, SIGMA.cors_with_credentials_http_origin_spring_config, SIGMA.cors_with_credentials_http_origin_spring_corsconfiguration, SIGMA.cors_with_credentials_http_origin_spring_corsregistration, SIGMA.cors_with_credentials_http_origin_terraform_azurerm_app_service, SIGMA.cors_with_credentials_null_origin_core_java, SIGMA.cors_with_credentials_null_origin_express_cors, SIGMA.cors_with_credentials_null_origin_koa, SIGMA.cors_with_credentials_null_origin_nestjs, SIGMA.cors_with_credentials_null_origin_servlet, SIGMA.cors_with_credentials_null_origin_spring_config, SIGMA.cors_with_credentials_null_origin_spring_corsconfiguration, SIGMA.cors_with_credentials_null_origin_spring_corsregistration, SIGMA.cors_with_credentials_null_origin_terraform_azurerm_app_service, SIGMA.cors_with_credentials_subdomain_origin_core_java, SIGMA.cors_with_credentials_subdomain_origin_servlet, SIGMA.cors_with_credentials_subdomain_origin_spring_config, SIGMA.cors_with_credentials_subdomain_origin_spring_corsconfiguration, SIGMA.cors_with_credentials_subdomain_origin_spring_corsregistration, SIGMA.credentials_validation_disabled_node_aws_sdk, SIGMA.csrf_openapi, SIGMA.csrf_protection_disabled_express_csurf, SIGMA.csrf_protection_disabled_spring_security_code, SIGMA.csrf_protection_disabled_spring_security_config, SIGMA.custom_resource_in_default_namespace_kubernetes, SIGMA.dangerous_ropc_flow_openapi_v2, SIGMA.dangerous_ropc_flow_openapi_v3, SIGMA.dangerous_ropc_flow_openapi_x_a127, SIGMA.dangerous_ropc_flow_postman, SIGMA.dangerous_ropc_flow_terraform_auth0, SIGMA.dangerously_exposed_interface_android, SIGMA.database_encryption_disabled_cloudformation_doc_db, SIGMA.database_encryption_disabled_cloudformation_dynamo_db, SIGMA.database_encryption_disabled_cloudformation_neptune_cluster, SIGMA.database_encryption_disabled_cloudformation_rds_cluster, SIGMA.database_encryption_disabled_cloudformation_rds_instance, SIGMA.database_encryption_disabled_cloudformation_redshift_cluster, (cont. on next page)

PCI DSS requirement	Addressing compliance
6.5.6: All "high risk" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1). (cont.)	SIGMA.database_encryption_disabled_terraform_aws_athena, SIGMA.database_encryption_disabled_terraform_aws_rds, SIGMA.default_allow_all_authz_policy_cloudformation_aws_webacl, SIGMA.default_allow_all_authz_policy_consul, SIGMA.default_allow_all_authz_policy_istio_envoy, SIGMA.default_allow_all_authz_policy_kafka, SIGMA.default_allow_all_authz_policy_openapi, SIGMA.deprecated_http_client_apache_default_http_client, SIGMA.deprecated_http_client_apache_system_default_http_client, SIGMA.dev_mode_enabled_struts2, SIGMA.dev_mode_enabled_struts2_properties, SIGMA.disabled_session_fixation_protection_grails_springsecurity, SIGMA.disk_encryption_disabled_cloudformation_aws_autoscaling, SIGMA.disk_encryption_disabled_cloudformation_dax, SIGMA.disk_encryption_disabled_cloudformation_efs, SIGMA.disk_encryption_disabled_cloudformation_elastic_cache_group, SIGMA.disk_encryption_disabled_cloudformation_elastic_search, SIGMA.disk_encryption_disabled_cloudformation_workspace_volume, SIGMA.disk_encryption_disabled_terraform_aws_dax, SIGMA.disk_encryption_disabled_terraform_aws_ebs, SIGMA.disk_encryption_disabled_terraform_aws_efs, SIGMA.disk_encryption_disabled_terraform_azurerm_managed_disk, SIGMA.duplicate_validation_forms_struts, SIGMA.empty_encryption_key_node_crypto, SIGMA.empty_password_core_java_sql, SIGMA.encryption_disabled_cloudformation_eks, SIGMA.encryption_disabled_ios_multipeer_connection, SIGMA.encryption_disabled_spring_security, SIGMA.encryption_disabled_terraform_aws_eks, SIGMA.expect_ct_disabled_express_helmet, SIGMA.exposed_privileged_account_cloudformation_aws_iam, SIGMA.exposed_privileged_account_cloudformation_ecs, SIGMA.file_upload_misconfiguration_of_file_path_busboy, SIGMA.file_upload_misconfiguration_of_file_path_express, SIGMA.file_upload_misconfiguration_of_file_path_multer, SIGMA.file_upload_misconfiguration_of_safe_file_names_express, SIGMA.gateway_exposes_all_hosts_istio, SIGMA.hardcoded_credentials_uri_core_java, SIGMA.hardcoded_remember_me_key_spring_security, SIGMA.hardcoded_secret_cloudformation, SIGMA.hardcoded_secret_core_swift, SIGMA.hardcoded_secret_express_jwt, SIGMA.hardcoded_secret_kubernetes, SIGMA.hardcoded_secret_passport, SIGMA.hardcoded_secret_postman, SIGMA.hardcoded_secret_rabbitmq, SIGMA.hardcoded_secret_spring_security, SIGMA.hardcoded_secret_spring_security_ldap, SIGMA.hardcoded_secret_terraform, SIGMA.hpkp_max_age_too_long_express, SIGMA.hpkp_max_age_too_long_koa, SIGMA.hpkp_report_uri_missing_tls_express, SIGMA.hpkp_report_uri_missing_tls_koa, SIGMA.hsts_http_header_short_max_age_express_helmet, SIGMA.hsts_http_header_subdomains_disabled_express_helmet, SIGMA.hsts_http_header_subdomains_disabled_express_hsts, SIGMA.http_firewall_allow_any_http_method_spring, SIGMA.http_firewall_allow_any_http_method_spring_config, SIGMA.http_header_validation_disabled_netty, SIGMA.http_method_missing_authz_openapi, SIGMA.http_method_missing_authz_terraform_aws_api_gateway, SIGMA.http_verb_tampering_method_inclusion_servlet, SIGMA.http_verb_tampering_method_omission_servlet, SIGMA.iam_role_allows_open_access_cloudformation_aws_iam, SIGMA.improper_use_of_symmetric_cryptography_hazelcast_code, SIGMA.improper_use_of_symmetric_cryptography_hazelcast_xml, SIGMA.improper_use_of_symmetric_cryptography_hazelcast_yaml, SIGMA.insecure_cipher_core_java_block_cipher, SIGMA.insecure_cipher_core_java_block_cipher_mode, SIGMA.insecure_cipher_core_java_stream_cipher, SIGMA.insecure_file_permission_core_java, SIGMA.insecure_tls_cipher_suite_cloudformation_load_balancer, SIGMA.insecure_tls_cipher_suite_node_https, SIGMA.insecure_tls_cipher_suite_node_request, SIGMA.insecure_tls_cipher_suite_node_tls, SIGMA.insecure_tls_version_ats_exception, SIGMA.insecure_tls_version_cloudformation_cloudfront, SIGMA.insecure_tls_version_cloudformation_elastic_search, SIGMA.insecure_tls_version_cloudformation_load_balancer, SIGMA.insecure_tls_version_core_java, SIGMA.insecure_tls_version_ios_protocol_max, SIGMA.insecure_tls_version_ios_protocol_min, SIGMA.insecure_tls_version_ios_stream_property, SIGMA.insecure_tls_version_kafka, SIGMA.insecure_tls_version_node_https, SIGMA.insecure_tls_version_node_request, SIGMA.insecure_tls_version_node_tls, SIGMA.insecure_tls_version_terraform_azurerm_app_service, SIGMA.insecure_tls_version_terraform_azurerm_postgresql, SIGMA.insecure_tls_version_terraform_azurerm_storage_account, SIGMA.insecure_xss_filter_express_helmet, SIGMA.insufficient_asymmetric_key_size_core_java, SIGMA.insufficient_brute_force_protection_terraform_auth0, SIGMA.insufficient_symmetric_key_size_core_java, SIGMA.insufficient_token_entropy_hapi_crumb, SIGMA.javascript_code_in_description_openapi, SIGMA.jwt_untrusted_decode_io_jsonwebtoken, SIGMA.jwt_untrusted_decode_jsonwebtoken, SIGMA.kms_encryption_service_disabled_kubernetes, SIGMA.legacy_attribute_based_access_control_terraform_gke, SIGMA.login_over_http_spring_security, SIGMA.markdown_allow_dangerous_html_react, SIGMA.message_encryption_disabled_cloudformation_sns, SIGMA.message_encryption_disabled_cloudformation_sqs, SIGMA.middleware_applied_globally_express_multer, SIGMA.missing_httponly_attribute_postman, SIGMA.missing_httponly_attribute_servlet, (cont. on next page)

PCI DSS requirement	Addressing compliance
6.5.6: All "high risk" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1). (cont.)	SIGMA.missing_httponly_attribute_session_cookie_express, SIGMA.missing_httponly_attribute_session_cookie_grails, SIGMA.missing_httponly_attribute_session_cookie_servlet, SIGMA.missing_httponly_attribute_session_cookie_spring_boot_properties, SIGMA.missing_httponly_attribute_session_cookie_spring_boot_yaml, SIGMA.missing_mfa_cloudformation_aws_cognito, SIGMA.missing_mtls_consul, SIGMA.missing_mtls_istio_port, SIGMA.missing_mtls_istio_service, SIGMA.missing_mtls_istio_workload, SIGMA.missing_mtls_kafka_broker, SIGMA.missing_mtls_rabbitmq, SIGMA.missing_perfect_forward_secrecy_ats_exception, SIGMA.missing_perfect_forward_secrecy_ats_temporary_exception, SIGMA.missing_perfect_forward_secrecy_ats_temporary_third_party_exception, SIGMA.missing_perfect_forward_secrecy_ats_third_party_exception, SIGMA.missing_secure_attribute_postman, SIGMA.missing_secure_attribute_remember_me_cookie_spring_security_code, SIGMA.missing_secure_attribute_remember_me_cookie_spring_security_config, SIGMA.missing_secure_attribute_servlet, SIGMA.missing_secure_attribute_session_cookie_express, SIGMA.missing_secure_attribute_session_cookie_grails, SIGMA.missing_secure_attribute_session_cookie_servlet_xml, SIGMA.missing_secure_attribute_session_cookie_spring_boot_properties, SIGMA.missing_secure_attribute_session_cookie_spring_boot_yaml, SIGMA.missing_security_constraint_jsf2, SIGMA.missing_servlet_mapping_servlet, SIGMA.missing_tls_apache_http, SIGMA.missing_tls_apache_telnet, SIGMA.missing_tls_ats_arbitrary_loads, SIGMA.missing_tls_ats_arbitrary_loads_for_media, SIGMA.missing_tls_ats_arbitrary_loads_in_web_content, SIGMA.missing_tls_ats_domain_exception, SIGMA.missing_tls_ats_localhost_exception, SIGMA.missing_tls_ats_temporary_exception, SIGMA.missing_tls_ats_temporary_third_party_exception, SIGMA.missing_tls_ats_third_party_exception, SIGMA.missing_tls_axios, SIGMA.missing_tls_cloudformation_cloudfront, SIGMA.missing_tls_cloudformation_doc_db, SIGMA.missing_tls_cloudformation_elastic_cache, SIGMA.missing_tls_cloudformation_elastic_search, SIGMA.missing_tls_cloudformation_elastic_search_node_to_node, SIGMA.missing_tls_cloudformation_load_balancer, SIGMA.missing_tls_cloudformation_load_balancer_classic, SIGMA.missing_tls_common_properties, SIGMA.missing_tls_consul, SIGMA.missing_tls_consul_client, SIGMA.missing_tls_core_java_httprequest, SIGMA.missing_tls_core_java_httpurlconnection, SIGMA.missing_tls_got, SIGMA.missing_tls_hapi_session_mongo, SIGMA.missing_tls_java_unirest, SIGMA.missing_tls_kafka_broker, SIGMA.missing_tls_kafka_client, SIGMA.missing_tls_kafka_listener, SIGMA.missing_tls_node_aws_sdk, SIGMA.missing_tls_node_ftp, SIGMA.missing_tls_node_grpc, SIGMA.missing_tls_node_http, SIGMA.missing_tls_node_rest_client, SIGMA.missing_tls_node_telnet, SIGMA.missing_tls_node_telnet_client, SIGMA.missing_tls_openapi_oauth2_endpoint, SIGMA.missing_tls_openapi_ref, SIGMA.missing_tls_openapi_v2_base_uri, SIGMA.missing_tls_openapi_v3_base_uri, SIGMA.missing_tls_openapi_x_a127, SIGMA.missing_tls_openapi_x_amazon_apigateway_integration, SIGMA.missing_tls_openapi_x_google_backend, SIGMA.missing_tls_openapi_x_google_jwks, SIGMA.missing_tls_openapi_x_servers, SIGMA.missing_tls_postman, SIGMA.missing_tls_sequelize, SIGMA.missing_tls_socket_io_client, SIGMA.missing_tls_spring_boot_cassandra_properties, SIGMA.missing_tls_spring_boot_cassandra_yaml, SIGMA.missing_tls_spring_boot_couchbase_properties, SIGMA.missing_tls_spring_boot_couchbase_yaml, SIGMA.missing_tls_spring_boot_elasticsearch_properties, SIGMA.missing_tls_spring_boot_elasticsearch_yaml, SIGMA.missing_tls_spring_boot_management_server_properties, SIGMA.missing_tls_spring_boot_management_server_yaml, SIGMA.missing_tls_spring_boot_properties, SIGMA.missing_tls_spring_boot_rabbitmq_properties, SIGMA.missing_tls_spring_boot_rabbitmq_yaml, SIGMA.missing_tls_spring_boot_redis_properties, SIGMA.missing_tls_spring_boot_redis_yaml, SIGMA.missing_tls_spring_boot_yaml, SIGMA.missing_tls_spring_ftp, SIGMA.missing_tls_spring_resttemplate, SIGMA.missing_tls_terraform_aws_cloudfront, SIGMA.missing_tls_terraform_aws_docdb, SIGMA.missing_tls_terraform_aws_load_balancer, SIGMA.missing_tls_terraform_azurerm_app_service, SIGMA.missing_tls_terraform_azurerm_mysql, SIGMA.missing_tls_terraform_azurerm_postgresql, SIGMA.missing_tls_terraform_azurerm_storage_account, SIGMA.missing_tls_terraform_google_sql_db, SIGMA.plaintext_storage_sensitive_data_terraform_aws_lambda_env_vars, SIGMA.plaintext_storage_sensitive_data_terraform_azurerm_vm_custom_data, SIGMA.privileged_container_allowed_kubernetes, SIGMA.project_encryption_disabled_cloudformation_codebuild, SIGMA.project_encryption_disabled_terraform_aws_codebuild, SIGMA.query_encryption_disabled_terraform_aws_athena, SIGMA.remote_access_via_guest_account_rabbitmq_default_mqtt, SIGMA.remote_access_via_guest_account_rabbitmq_loopback_users, SIGMA.remote_execution_enabled_consul, SIGMA.request_allows_any_media_type_openapi, SIGMA.rsa_no_padding_core_java, SIGMA.sasl_plain_enabled_kafka_broker, SIGMA.sasl_plain_enabled_kafka_client, (cont. on next page)

PCI DSS requirement	Addressing compliance
6.5.6: All "high risk" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1). (cont.)	SIGMA.script_checks_enabled_consul, SIGMA.sensitive_data_in_cookie_servlet, SIGMA.sensitive_data_in_query_string_openapi, SIGMA.sensitive_data_in_query_string_spring_security, SIGMA.session_fixation_protection_disabled_spring_security, SIGMA.socket_accepts_all_origins_socket_io, SIGMA.ssh_publicly_accessible_cloudformation_eks, SIGMA.state_changing_get_request_grails_springsecurity, SIGMA.stripe_validation_disabled_openapi_x_stripe, SIGMA.tag_authorization_disabled_spring_security, SIGMA.tiller_service_exposed_kubernetes, SIGMA.undefined_oauth2_scope_openapi_v2, SIGMA.undefined_oauth2_scope_openapi_v3, SIGMA.unprotected_admin_operation_openapi, SIGMA.unprotected_master_key_cloudformation_aws_kms, SIGMA.unrestricted_egress_cloudformation_aws_ec2, SIGMA.unrestricted_egress_cloudformation_aws_ec2_security_group, SIGMA.unrestricted_egress_cloudformation_aws_ec2_security_group_default, SIGMA.unrestricted_egress_istio, SIGMA.unrestricted_ingress_cloudformation_aws_ec2, SIGMA.unrestricted_ingress_cloudformation_aws_ec2_security_group, SIGMA.unrestricted_ingress_cloudformation_aws_ec2_security_group_default, SIGMA.unrestricted_ingress_terraform_aws_eks, SIGMA.unrestricted_ingress_terraform_aws_security_group, SIGMA.unrestricted_ingress_terraform_azurerm_kubernetes_cluster, SIGMA.unrestricted_ingress_terraform_gke, SIGMA.unrestricted_ingress_terraform_google_compute, SIGMA.unrestricted_ingress_terraform_google_sql_db, SIGMA.unsafe_innerhtml_manipulation_react, SIGMA.unsafe_innerhtml_manipulation_vue_jsx, SIGMA.unsafe_innerhtml_manipulation_vue_vhtml_directive, SIGMA.unsafe_xml_canonicalization_spring_saml_code, SIGMA.unsafe_xml_canonicalization_spring_saml_config, SIGMA.unspecified_cipher_transformation_core_java, SIGMA.vendor_provided_encryption_key_cloudformation_cloudtrail, SIGMA.vendor_provided_encryption_key_cloudformation_efs, SIGMA.vendor_provided_encryption_key_terraform_google_compute, SIGMA.weak_biometric_authentication_ios, SIGMA.weak_hash_apache_commons_codec, SIGMA.weak_hash_core_java, SIGMA.weak_hash_node_crypto, SIGMA.weak_password_hash_grails_springsecurity, SIGMA.weak_password_hash_spring_security_code, SIGMA.weak_password_hash_spring_security_config, SIGMA.weak_password_policy_terraform_auth0, SIGMA.weak_password_policy_terraform_aws_iam, SIGMA.weak_security_constraint_servlet, SIGMA.weak_xss_protection_servlet, SIGMA.webview_file_access_android, SIGMA.xss_filter_disabled_express_helmet, SIZECHECK, SOCKET_ACCEPT_ALL_ORIGINS, SQLI, SQL_NOT_CONSTANT, STATIC_API_KEY, STRICT_TRANSPORT_SECURITY, STRING_NULL, STRING_OVERFLOW, STRING_SIZE, SYMFONY_EL_INJECTION, TAINTED_ENVIRONMENT_WITH_EXECUTION, TAINTED_SCALAR, TAINTED_STRING, TEMPLATE_INJECTION, UNCHECKED_ORIGIN, UNENCRYPTED_SENSITIVE_DATA, UNESCAPED_HTML, UNINIT_NONNULL, UNKNOWN_LANGUAGE_INJECTION, UNLESS_CASE_SENSITIVE_ROUTE_MATCHING, UNRESTRICTED_DISPATCH, UNSAFE_BASIC_AUTH, UNSAFE_FUNCTIONALITY, UNSAFE_JNI, UNSAFE_NAMED_QUERY, UNSAFE_REFLECTION, UNSAFE_SESSION_SETTING, URL_MANIPULATION, USER_POINTER, USE_AFTER_FREE, WEAK_GUARD, WEAK_PASSWORD_HASH, WEAK_URL_SANITIZATION, WEAK_XML_SCHEMA, WRAPPER_ESCAPE, XML_INJECTION, XPATH_INJECTION, XSS
6.5.7: Cross-site scripting (XSS)	These Coverity checkers meet this requirement: ANGULAR_BYPASS_SECURITY, ANGULAR_ELEMENT_REFERENCE, ANGULAR_SCE_DISABLED, DOM_XSS, FB.XSS_REQUEST_PARAMETER_TO_JSP_WRITER, FB.XSS_REQUEST_PARAMETER_TO_SEND_ERROR, FB.XSS_REQUEST_PARAMETER_TO_SERVLET_WRITER, INSECURE_CSP, JINJA2_AUTOESCAPE_DISABLED, PMD.ApexXSSFromEscapeFalse, PMD.ApexXSSFromURLParam, PMD.VfHtmlStyleTagXss, RUBY_VULNERABLE_LIBRARY, SIGMA.content_security_policy_disabled_express_helmet, SIGMA.dangerously_exposed_interface_android, SIGMA.insecure_xss_filter_express_helmet, SIGMA.javascript_code_in_description_openapi, SIGMA.markdown_allow_dangerous_html_react, SIGMA.no_sniff_disabled_express_helmet, SIGMA.unsafe_innerhtml_manipulation_react, SIGMA.unsafe_innerhtml_manipulation_vue_jsx, SIGMA.unsafe_innerhtml_manipulation_vue_vhtml_directive, SIGMA.weak_xss_protection_servlet, SIGMA.xss_filter_disabled_express_helmet, TEMPLATE_INJECTION, UNESCAPED_HTML, XSS

PCI DSS requirement	Addressing compliance
6.5.8: Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions).	These Coverity checkers meet this requirement: ANDROID_CAPABILITY_LEAK, ANONYMOUS_DB_CONNECTION, AUDIT.SPECULATIVE_EXECUTION_DATA_LEAK, AUTOSAR C++14 A20-8-2, AUTOSAR C++14 A20-8-3, AUTOSAR C++14 A20-8-4, AUTOSAR C++14 A20-8-7, BAD_CERT_VERIFICATION, CERT ENV03-J, CERT FIO01-J, CERT MSC03-J, CERT POS37-C, CERT SEC00-J, CERT SEC01-J, CERT SEC02-J, CERT SEC06-J, CERT SER08-J, CONFIG.CONNECTION_STRING_PASSWORD, CONFIG.COOKIE_SIGNING_DISABLED, CONFIG.DEAD_AUTHORIZATION_RULE, CONFIG.DYNAMIC_DATA_HTML_COMMENT, CONFIG.ENABLED_TRACE_MODE, CONFIG.HARDCODED_CREDENTIALS_AUDIT, CONFIG.HARDCODED_TOKEN, CONFIG.UNSAFE_SESSION_TIMEOUT, CORS_MISCONFIGURATION, CORS_MISCONFIGURATION_AUDIT, DNS_PREFETCHING, EXPOSED_PREFERENCES, FB.DMI_CONSTANT_DB_PASSWORD, FB.DMI_EMPTY_DB_PASSWORD, FB.PT_ABSOLUTE_PATH_TRAVERSAL, FB.PT_RELATIVE_PATH_TRAVERSAL, HARDCODED_CREDENTIALS, HOST_HEADER_VALIDATION_DISABLED, IMPLICIT_INTENT, INSECURE_COMMUNICATION, INSECURE_COOKIE, INSECURE_DIRECT_OBJECT_REFERENCE, INSECURE_FILE_PERMISSIONS, INSECURE_NETWORK_BIND, INSECURE_REFERRER_POLICY, JAVA_CODE_INJECTION, JSP_DYNAMIC_INCLUDE, JSP_SQL_INJECTION, MISSING_AUTHZ, MISSING_IFRAME_SANDBOX, MISSING_PASSWORD_VALIDATOR, MISSING_PERMISSION_FOR_BROADCAST, MISSING_PERMISSION_ON_EXPORTED_COMPONENT, OAUTH2_MISCONFIGURATION, OPEN_REDIRECT, PATH_MANIPULATION, PMD.ApexBadCrypto, PMD.ApexCRUDViolation, PMD.ApexOpenRedirect, PMD.ApexSharingViolations, PMD.ApexSuggestUsingNamedCred, RAILS_DEFAULT_ROUTES, RAILS_DEVISE_CONFIG, RAILS_MISSING_FILTER_ACTION, REVERSE_TABNABBING, RISKY_CRYPTO, RUBY_VULNERABLE_LIBRARY, SA.RISKY_CRYPTO, SECURE_TEMP, SENSITIVE_DATA_LEAK, SESSION_FIXATION, SIGMA.access_control_disabled_consul, SIGMA.access_control_disabled_openapi, SIGMA.access_control_disabled_openapi_x_amazon_apigateway, SIGMA.access_control_disabled_openapi_x_google, SIGMA.access_control_disabled_openapi_x_google_backend, SIGMA.access_control_disabled_openapi_x_wso2, SIGMA.access_control_disabled_zookeeper, SIGMA.admin_access_enabled_spring_boot, SIGMA.admin_dashboard_publicly_accessible_kubernetes, SIGMA.allow_all_authz_policy_istio, SIGMA.allow_all_authz_policy_node_aws_sdk_s3_bucket, SIGMA.allow_all_authz_policy_node_aws_sdk_s3_object, SIGMA.allow_all_authz_policy_node_google_cloud_storage_bucket, SIGMA.allow_all_authz_policy_terraform_aws_ecr, SIGMA.allow_all_authz_policy_terraform_google_big_query, SIGMA.allow_all_authz_policy_terraform_google_storage_bucket, SIGMA.anonymous_access_enabled_kubernetes, SIGMA.anonymous_access_enabled_rabbitmq_local, SIGMA.anonymous_access_enabled_rabbitmq_remote, SIGMA.api_key_auth_enabled_openapi_v2, SIGMA.api_key_auth_enabled_openapi_v3, SIGMA.apparmour_default_configuration_override_kubernetes, SIGMA.basic_auth_enabled_cloudformation_aws_amplify, SIGMA.basic_auth_enabled_kubernetes, SIGMA.basic_auth_enabled_openapi_v2, SIGMA.basic_auth_enabled_openapi_v3, SIGMA.basic_auth_enabled_postman, SIGMA.basic_auth_enabled_terraform_azurerm_vm, SIGMA.basic_auth_enabled_terraform_gke, SIGMA.cloud_gateway_publicly_accessible_cloudformation_aws_apigateway, SIGMA.cloud_resource_assigned_public_ip_cloudformation_aws_ec2_subnet, SIGMA.cloud_resource_assigned_public_ip_cloudformation_aws_rds, SIGMA.cloud_resource_assigned_public_ip_cloudformation_sagemaker_notebook, SIGMA.cloud_resource_assigned_public_ip_terraform_aws_ec2, SIGMA.cloud_resource_assigned_public_ip_terraform_aws_eks, SIGMA.cloud_resource_assigned_public_ip_terraform_aws_mq_broker, SIGMA.cloud_resource_assigned_public_ip_terraform_aws_rds, SIGMA.cloud_resource_assigned_public_ip_terraform_google_compute, SIGMA.cloud_service_authn_disabled_terraform_azurerm_app_service, SIGMA.cloud_service_authz_disabled_cloudformation_aws_apigateway, SIGMA.cloud_storage_allows_public_config_cloudformation_aws_s3_bucket, SIGMA.cloud_storage_allows_public_config_terraform_aws_s3_bucket, SIGMA.cloud_storage_default_allow_all_terraform_azurerm_storage_account, SIGMA.cloud_storage_publicly_accessible_cloudformation_aws_s3_bucket, SIGMA.config_browser_plugin_enabled_struts2, SIGMA.container_empty_security_context_kubernetes, SIGMA.container_hostport_binding_kubernetes, SIGMA.container_insecure_bind_address_kubernetes, SIGMA.container_privilege_escalation_allowed_kubernetes, SIGMA.container_requesting_net_raw_kubernetes, SIGMA.container_requesting_sys_admin_kubernetes, SIGMA.container_running_as_root_kubernetes, SIGMA.container_sharing_host_ipc_namespace_kubernetes, SIGMA.container_sharing_host_pid_namespace_kubernetes, SIGMA.cors_configured_globally_express_cors, SIGMA.cors_configured_globally_koa, SIGMA.cors_no_credentials_permissive_origin_apollo_graphql, (cont. on next page)

PCI DSS requirement	Addressing compliance
6.5.8: Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions). (cont.)	SIGMA.cors_no_credentials_permissive_origin_cloudformation_aws_s3_bucket, SIGMA.cors_no_credentials_permissive_origin_core_java, SIGMA.cors_no_credentials_permissive_origin_express_cors, SIGMA.cors_no_credentials_permissive_origin_kafka_broker, SIGMA.cors_no_credentials_permissive_origin_koa, SIGMA.cors_no_credentials_permissive_origin_nestjs, SIGMA.cors_no_credentials_permissive_origin_openapi_x_a127, SIGMA.cors_no_credentials_permissive_origin_openapi_x_amazon_apigateway, SIGMA.cors_no_credentials_permissive_origin_openapi_x_amazon_apigateway_integration, SIGMA.cors_no_credentials_permissive_origin_postman, SIGMA.cors_no_credentials_permissive_origin_servlet, SIGMA.cors_no_credentials_permissive_origin_spring_config, SIGMA.cors_no_credentials_permissive_origin_spring_corsconfiguration, SIGMA.cors_no_credentials_permissive_origin_spring_corsregistration, SIGMA.cors_no_credentials_permissive_origin_terraform_aws_s3_bucket, SIGMA.cors_no_credentials_permissive_origin_terraform_azurerm_app_service, SIGMA.cors_no_credentials_permissive_origin_terraform_google_storage_bucket, SIGMA.cors_preflight_age_too_long_cloudformation_aws_s3_bucket, SIGMA.cors_preflight_age_too_long_core_java, SIGMA.cors_preflight_age_too_long_express_cors, SIGMA.cors_preflight_age_too_long_koa, SIGMA.cors_preflight_age_too_long_nestjs, SIGMA.cors_preflight_age_too_long_openapi_x_a127, SIGMA.cors_preflight_age_too_long_openapi_x_amazon_apigateway, SIGMA.cors_preflight_age_too_long_openapi_x_amazon_apigateway_integration, SIGMA.cors_preflight_age_too_long_servlet, SIGMA.cors_preflight_age_too_long_spring_config, SIGMA.cors_preflight_age_too_long_spring_corsconfiguration, SIGMA.cors_preflight_age_too_long_spring_corsregistration, SIGMA.cors_preflight_age_too_long_terraform_aws_s3_bucket, SIGMA.cors_preflight_age_too_long_terraform_google_storage_bucket, SIGMA.cors_with_credentials_all_origin_core_java, SIGMA.cors_with_credentials_all_origin_express_cors, SIGMA.cors_with_credentials_all_origin_koa, SIGMA.cors_with_credentials_all_origin_nestjs, SIGMA.cors_with_credentials_all_origin_openapi_x_a127, SIGMA.cors_with_credentials_all_origin_openapi_x_amazon_apigateway, SIGMA.cors_with_credentials_all_origin_openapi_x_amazon_apigateway_integration, SIGMA.cors_with_credentials_all_origin_servlet, SIGMA.cors_with_credentials_all_origin_spring_config, SIGMA.cors_with_credentials_all_origin_spring_corsconfiguration, SIGMA.cors_with_credentials_all_origin_spring_corsregistration, SIGMA.cors_with_credentials_all_origin_terraform_azurerm_app_service, SIGMA.cors_with_credentials_null_origin_core_java, SIGMA.cors_with_credentials_null_origin_express_cors, SIGMA.cors_with_credentials_null_origin_koa, SIGMA.cors_with_credentials_null_origin_nestjs, SIGMA.cors_with_credentials_null_origin_servlet, SIGMA.cors_with_credentials_null_origin_spring_config, SIGMA.cors_with_credentials_null_origin_spring_corsconfiguration, SIGMA.cors_with_credentials_null_origin_spring_corsregistration, SIGMA.cors_with_credentials_null_origin_terraform_azurerm_app_service, SIGMA.cors_with_credentials_subdomain_origin_core_java, SIGMA.cors_with_credentials_subdomain_origin_servlet, SIGMA.cors_with_credentials_subdomain_origin_spring_config, SIGMA.cors_with_credentials_subdomain_origin_spring_corsconfiguration, SIGMA.cors_with_credentials_subdomain_origin_spring_corsregistration, SIGMA.custom_resource_in_default_namespace_kubernetes, SIGMA.dangerous_ropc_flow_openapi_v2, SIGMA.dangerous_ropc_flow_openapi_v3, SIGMA.dangerous_ropc_flow_openapi_x_a127, SIGMA.dangerous_ropc_flow_postman, SIGMA.dangerous_ropc_flow_terraform_auth0, SIGMA.default_allow_all_authz_policy_cloudformation_aws_webacl, SIGMA.default_allow_all_authz_policy_consul, SIGMA.default_allow_all_authz_policy_istio_envoy, SIGMA.default_allow_all_authz_policy_kafka, SIGMA.default_allow_all_authz_policy_openapi, SIGMA.dev_mode_enabled_struts2, SIGMA.dev_mode_enabled_struts2_properties, SIGMA.disabled_session_fixation_protection_grails_springsecurity, SIGMA.empty_password_core_java_sql, SIGMA.exposed_privileged_account_cloudformation_aws_iam, SIGMA.exposed_privileged_account_cloudformation_ecs, SIGMA.file_upload_misconfiguration_of_file_path_busboy, SIGMA.file_upload_misconfiguration_of_file_path_express, SIGMA.file_upload_misconfiguration_of_file_path_multer, SIGMA.file_upload_misconfiguration_of_safe_file_names_express, SIGMA.file_upload_misconfiguration_of_storage_multer, SIGMA.gateway_exposes_all_hosts_istio, SIGMA.hardcoded_credentials_uri_core_java, SIGMA.hardcoded_remember_me_key_spring_security, SIGMA.hardcoded_secret_cloudformation, SIGMA.hardcoded_secret_core_swift, SIGMA.hardcoded_secret_express_jwt, SIGMA.hardcoded_secret_kubernetes, SIGMA.hardcoded_secret_passport, SIGMA.hardcoded_secret_postman, SIGMA.hardcoded_secret_rabbitmq, SIGMA.hardcoded_secret_spring_security, SIGMA.hardcoded_secret_spring_security_ldap, SIGMA.hardcoded_secret_terraform, SIGMA.hsts_http_header_short_max_age_express_helmet, SIGMA.http_method_missing_authz_openapi, SIGMA.http_method_missing_authz_terraform_aws_api_gateway, SIGMA.iam_role_allows_open_access_cloudformation_aws_iam, SIGMA.insecure_file_permission_core_java, (cont. on next page)

PCI DSS requirement	Addressing compliance
6.5.8: Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions). (cont.)	SIGMA.insufficient_brute_force_protection_terraform_auth0, SIGMA.insufficient_token_entropy_hapi_crumb, SIGMA.legacy_attribute_based_access_control_terraform_gke, SIGMA.middleware_applied_globally_express_multer, SIGMA.missing_httponly_attribute_postman, SIGMA.missing_httponly_attribute_servlet, SIGMA.missing_httponly_attribute_session_cookie_express, SIGMA.missing_httponly_attribute_session_cookie_grails, SIGMA.missing_httponly_attribute_session_cookie_servlet, SIGMA.missing_httponly_attribute_session_cookie_spring_boot_properties, SIGMA.missing_httponly_attribute_session_cookie_spring_boot_yaml, SIGMA.missing_mfa_cloudformation_aws_cognito, SIGMA.missing_mtls_consul, SIGMA.missing_mtls_istio_port, SIGMA.missing_mtls_istio_service, SIGMA.missing_mtls_istio_workload, SIGMA.missing_mtls_kafka_broker, SIGMA.missing_mtls_rabbitmq, SIGMA.missing_security_constraint_jsf2, SIGMA.missing_servlet_mapping_servlet, SIGMA.no_password_change_on_first_login_cloudformation_aws_iam, SIGMA.no_rate_limiting_openapi, SIGMA.oauth2_pkce_plaintext_challenge_postman, SIGMA.password_change_without_old_password_openapi, SIGMA.privileged_container_allowed_kubernetes, SIGMA.remote_access_via_guest_account_rabbitmq_default_mqtt, SIGMA.remote_access_via_guest_account_rabbitmq_loopback_users, SIGMA.remote_execution_enabled_consul, SIGMA.session_fixation_protection_disabled_spring_security, SIGMA.socket_accepts_all_origins_socket_io, SIGMA.ssh_publicly_accessible_cloudformation_eks, SIGMA.state_changing_get_request_grails_springsecurity, SIGMA.tag_authorization_disabled_spring_security, SIGMA.tiller_service_exposed_kubernetes, SIGMA.undefined_oauth2_scope_openapi_v2, SIGMA.undefined_oauth2_scope_openapi_v3, SIGMA.unprotected_admin_operation_openapi, SIGMA.unrestricted_egress_cloudformation_aws_ec2, SIGMA.unrestricted_egress_cloudformation_aws_ec2_security_group, SIGMA.unrestricted_egress_cloudformation_aws_ec2_security_group_default, SIGMA.unrestricted_egress_istio, SIGMA.unrestricted_ingress_cloudformation_aws_ec2, SIGMA.unrestricted_ingress_cloudformation_aws_ec2_security_group, SIGMA.unrestricted_ingress_cloudformation_aws_ec2_security_group_default, SIGMA.unrestricted_ingress_terraform_aws_eks, SIGMA.unrestricted_ingress_terraform_aws_security_group, SIGMA.unrestricted_ingress_terraform_azurerm_kubernetes_cluster, SIGMA.unrestricted_ingress_terraform_gke, SIGMA.unrestricted_ingress_terraform_google_compute, SIGMA.unrestricted_ingress_terraform_google_sql_db, SIGMA.unsafe_xml_canonicalization_spring_saml_code, SIGMA.unsafe_xml_canonicalization_spring_saml_config, SIGMA.weak_biometric_authentication_ios, SIGMA.weak_password_hash_grails_springsecurity, SIGMA.weak_password_hash_spring_security_code, SIGMA.weak_password_hash_spring_security_config, SIGMA.weak_password_policy_terraform_auth0, SIGMA.weak_password_policy_terraform_aws_iam, SIGMA.weak_security_constraint_servlet, SIGMA.webview_file_access_android, SOCKET_ACCEPT_ALL_ORIGINS, SQLI, SQL_NOT_CONSTANT, STATIC_API_KEY, STRICT_TRANSPORT_SECURITY, UNCHECKED_ORIGIN, UNENCRYPTED_SENSITIVE_DATA, UNLESS_CASE_SENSITIVE_ROUTE_MATCHING, UNRESTRICTED_ACCESS_TO_FILE, UNRESTRICTED_DISPATCH, UNSAFE_BASIC_AUTH, UNSAFE_BUFFER_METHOD, UNSAFE_SESSION_SETTING, UNSAFE_XML_PARSE_CONFIG, WEAK_GUARD, WEAK_URL_SANITIZATION, XML_EXTERNAL_ENTITY
6.5.9: Cross-site request forgery (CSRF)	These Coverity checkers meet this requirement: CONFIG.BEEGO_CSRF_PROTECTION_DISABLED, CONFIG.DJANGO_CSRF_PROTECTION_DISABLED, CONFIG.HANA_XS_PREVENT_XSRF_DISABLED, CONFIG.SYMFONY_CSRF_PROTECTION_DISABLED, CSRF, PMD.VfCsrf, RUBY_VULNERABLE_LIBRARY, SIGMA.csrf_openapi, SIGMA.csrf_protection_disabled_express_csurf, SIGMA.csrf_protection_disabled_spring_security_code, SIGMA.csrf_protection_disabled_spring_security_config
6.5.10: Broken authentication and session management.	These Coverity checkers meet this requirement: ANONYMOUS_DB_CONNECTION, AUTOSAR C++14 A26-5-2, CERT MSC02-J, CERT MSC03-J, CERT MSC11-J, CERT MSC30-C, CERT MSC32-C, CERT MSC50-CPP, CERT MSC51-CPP, CERT SEC02-J, CONFIG.CONNECTION_STRING_PASSWORD, CONFIG.COOKIES_MISSING_HTTPONLY, CONFIG.COOKIE_SIGNING_DISABLED, CONFIG.HARDCODED_CREDENTIALS_AUDIT, CONFIG.HARDCODED_TOKEN, CONFIG.JAVAEE_MISSING_HTTPONLY, CONFIG.UNSAFE_SESSION_TIMEOUT, CORS_MISCONFIGURATION, CORS_MISCONFIGURATION_AUDIT, FB.DMI_CONSTANT_DB_PASSWORD, FB.DMI_EMPTY_DB_PASSWORD, HARDCODED_CREDENTIALS, HOST_HEADER_VALIDATION_DISABLED, INSECURE_COMMUNICATION, INSECURE_RANDOM, INSECURE_SALT, MISSING_AUTHZ, MISSING_PASSWORD_VALIDATOR, MOBILE_ID_MISUSE, PMD.ApexBadCrypto, PMD.ApexSuggestUsingNamedCred, PREDICTABLE_RANDOM_SEED, RAILS_DEVISE_CONFIG, RUBY_VULNERABLE_LIBRARY, SENSITIVE_DATA_LEAK, SESSION_FIXATION, SIGMA.access_control_disabled_consul, SIGMA.access_control_disabled_openapi, SIGMA.access_control_disabled_openapi_x_amazon_apigateway, SIGMA.access_control_disabled_openapi_x_google, (cont. on next page)

PCI DSS requirement	Addressing compliance
6.5.10: Broken authentication and session management. (cont.)	SIGMA.access_control_disabled_openapi_x_google_backend, SIGMA.access_control_disabled_openapi_x_wso2, SIGMA.access_control_disabled_zookeeper, SIGMA.anonymous_access_enabled_kubernetes, SIGMA.anonymous_access_enabled_rabbitmq_local, SIGMA.anonymous_access_enabled_rabbitmq_remote, SIGMA.api_key_auth_enabled_openapi_v2, SIGMA.api_key_auth_enabled_openapi_v3, SIGMA.basic_auth_enabled_cloudformation_aws_amplify, SIGMA.basic_auth_enabled_kubernetes, SIGMA.basic_auth_enabled_openapi_v2, SIGMA.basic_auth_enabled_openapi_v3, SIGMA.basic_auth_enabled_postman, SIGMA.basic_auth_enabled_terraform_azurerm_vm, SIGMA.basic_auth_enabled_terraform_gke, SIGMA.cache_ttl_too_long_openapi_x_a127, SIGMA.cloud_service_authn_disabled_terraform_azurerm_app_service, SIGMA.disabled_session_fixation_protection_grails_springsecurity, SIGMA.empty_password_core_java_sql, SIGMA.excessive_session_lifetime_connect_mongo, SIGMA.excessive_session_lifetime_connect_redis, SIGMA.excessive_session_lifetime_express_client_sessions, SIGMA.excessive_session_lifetime_express_cookie_session, SIGMA.excessive_session_lifetime_express_session, SIGMA.excessive_session_lifetime_google_cloud_datastore, SIGMA.excessive_token_lifetime_node_aws_sdk, SIGMA.excessive_token_lifetime_openapi_x_a127, SIGMA.excessive_token_lifetime_terraform_auth0, SIGMA.hardcoded_credentials_uri_core_java, SIGMA.hardcoded_remember_me_key_spring_security, SIGMA.hardcoded_secret_cloudformation, SIGMA.hardcoded_secret_core_swift, SIGMA.hardcoded_secret_express_jwt, SIGMA.hardcoded_secret_kubernetes, SIGMA.hardcoded_secret_passport, SIGMA.hardcoded_secret_postman, SIGMA.hardcoded_secret_rabbitmq, SIGMA.hardcoded_secret_spring_security, SIGMA.hardcoded_secret_spring_security_ldap, SIGMA.hardcoded_secret_terraform, SIGMA.hsts_http_header_short_max_age_express_helmet, SIGMA.insufficient_brute_force_protection_terraform_auth0, SIGMA.insufficient_presigned_url_timeout_node_aws_sdk, SIGMA.insufficient_presigned_url_timeout_node_google_cloud_storage, SIGMA.insufficient_token_entropy_hapi_crumb, SIGMA.jwt_ignored_expiration_time_hapi, SIGMA.jwt_ignored_expiration_time_jsonwebtoken, SIGMA.jwt_ignored_start_time_hapi, SIGMA.jwt_ignored_start_time_jsonwebtoken, SIGMA.jwt_non_expiring_token_jsonwebtoken, SIGMA.jwt_revoke_missing_express_jwt, SIGMA.middleware_applied_globally_express_multer, SIGMA.missing_mfa_cloudformation_aws_cognito, SIGMA.missing_security_constraint_jsf2, SIGMA.no_password_change_on_first_login_cloudformation_aws_iam, SIGMA.no_rate_limiting_openapi, SIGMA.password_change_without_old_password_openapi, SIGMA.session_fixation_protection_disabled_spring_security, SIGMA.unsafe_xml_canonicalization_spring_saml_code, SIGMA.unsafe_xml_canonicalization_spring_saml_config, SIGMA.weak_biometric_authentication_ios, SIGMA.weak_password_hash_grails_springsecurity, SIGMA.weak_password_hash_spring_security_code, SIGMA.weak_password_hash_spring_security_config, SIGMA.weak_password_policy_terraform_auth0, SIGMA.weak_password_policy_terraform_aws_iam, STATIC_API_KEY, STRICT_TRANSPORT_SECURITY, UNENCRYPTED_SENSITIVE_DATA, UNLESS_CASE_SENSITIVE_ROUTE_MATCHING, UNSAFE_BASIC_AUTH, UNSAFE_SESSION_SETTING, WEAK_GUARD, WEAK_PASSWORD_HASH, WEAK_URL_SANITIZATION
6.6: For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes • Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.	Web-facing applications are exposed to ongoing threats and can be under attack any time. Such attacks often succeed because of insecure coding practices. A regular review of these applications is therefore crucial in preventing attacks from succeeding. Between the two methods suggested by PCI DSS, code review with a static analysis tool is the easiest and most straightforward to adopt, for two reasons: First, every software project has code that you can review. Second, you can partially automate code review with sophisticated tools. It's important not only to review your web application code but also to use an automated technical solution that detects and prevents web-based attacks, such as interactive application security testing or a WAF.

This datasheet applies to Coverity 2021.12.0 and later versions.

* These PCI DSS requirements are also partially covered by some checkers for SEI CERT C/C++, SEI CERT JAVA, MISRA, and AUTOSAR standards. Contact Synopsys to obtain a full list of checkers that address the issues related to the PCI DSS requirements 6.5.1, 6.5.2, 6.5.5, and 6.5.6. Synopsys customers can also find this list in the Checker Reference technical guide.

The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations optimize security and quality in DevSecOps and throughout the software development life cycle.

For more information, go to www.synopsys.com/software.

Synopsys, Inc.
690 E Middlefield Road
Mountain View, CA 94043 USA

Contact us:
U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com