ALERT LOGIC®

SERVICE OVERVIEW:

ALERT LOGIC® FOR NIST 800-171

WHAT IS NIST 800-171?

NIST 800-171 refers to National Institute of Standards and Technology Special Publication NIST 800-171, and is basically a set of standards and processes for protecting information that is sensitive, but not "classified." Organizations that process, store, or transmit Controlled Unclassified Information (CUI) data for most federal and state agencies must comply with NIST 800-171. Even if your organization is not required to comply with NIST 800-171, it provides a solid blueprint for establishing an IT cybersecurity program with the framework for addressing: access control, audit and accountability, configuration management, identification and authentication, incident response, risk assessment, security assessment, and system integrity.

However following NIST 800 171 can be confusing, complex and expensive for many companies, especially those with limited staff and security expertise. The Alert Logic SIEMless Threat Detection portfolio addresses a broad range of regulatory compliance requirements to help you prevent incidents, such as a data breach, that threaten the security, availability, integrity and privacy of customer data. Alert Logic connects a security platform, threat intelligence, and cybersecurity experts to provide the best level of security and compliance coverage your workloads require across any environment.

Alert Logic delivers a solution that provides asset discovery, vulnerability assessment, threat detection, and application security. Our solution can help you map to NIST 800-171 standards and quickly understand the state of compliance without hiring new staff. Our expert services augment your in-house security team by monitoring your workloads and environment 24/7. Analysts investigate alerts and contact you within 15 minutes if we detect suspicious activity such as: unauthorized access, exposure or modification of accounts, controls or configurations.

ADVANCE YOUR COMPLIANCE program in record time quickly understand the state of compliance without hiring new staff.

REDUCE YOUR RISK with an improved security posture, reduced attack surface, and risk of data breach.

PROTECT CUSTOMER DATA from network and OWASP Top 10 attacks with web application scanning, a robust vulnerability library, and access to security consultants 24/7 to keep data safe..

PREPARE FOR AUDITS, ANYTIME with audit-ready audit preparedness reporting that helps IT staff stay one step ahead of requirements, mandates, and auditors.

FREE UP RESOURCES and implement compliance best practices with informed advice and remediation steps from our compliance experts..

Alert Logic maintains strict compliance with internal and external regulatory requirements for our IT operations and services, including: PCI DSS 3.2 Level 2 Audit, AICPA SOC 1 & 2 Audit, and ISO 27001-2013 certification for UK Operations.

ALERT LOGIC NIST 800-171 SOLUTIONS MAPPING

The integrated services that make up Alert Logic address a broad range of SNIST 800-171 to help you prevent incidents that threaten the security, availability, integrity and privacy of customer data.

ALERT LOGIC	NIST 800-171
Alert Logic Essentials *Vulnerability & Asset Visibility* - Asset discovery - Vulnerability scanning - Cloud configuration checks - Extended Endpoint protection - Threat Risk Index - Compliance scanning and reporting	Access Control Audit and Accountability Configuration Management Risk Assessment Security Assessment System and Communications Protection System and Information Integrity
Alert Logic Professional **Includes Essentials** *24/7 Managed Threat Detection and Incident Management* - 24/7 Incident Monitoring & Management - Security Analytics & Threat Intelligence - Log Collection and Monitoring - Intrusion Detection - Security Event Insights and Analysis - Office 365 Log Collection & Search - Cloud Vendor Security Integrations - AWS User Behavior Anomaly Detection - Anti-Virus Integration	Identification and Authentication Incident Response
Alert Logic Enterprise **Includes Professional** *Managed Web Application Firewall and Assigned SOC Analyst with Threat Hunting* - Always-on Managed WAF Defense - Assigned SOC Analyst - Controlled Threat Hunting - Dark Web Scanning	

NIST 800-171	ESSSENTIALS	PROFESSIONAL (INCLUDES ESSENTIALS)	ENTERPRISE (INCLUDES PROFESSIONAL)
3.1 ACCESS CONTROL			
3.1.7 Prevent non-privileged users from executing privileged functions and audit the execution of such functions.	●	●	●
3.1.8 Limit unsuccessful logon attempts.	●	●	●
3.1.11 Terminate (automatically) a user session after a defined condition.	●	●	●
3.1.12 Monitor and control remote access sessions.	●	●	●
3.3 AUDIT AND ACCOUNTABILITY			
3.3.1 Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.	●	●	●
3.3.2 Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	●	●	●
3.3.3 Review and update audited events.	●	●	●
3.3.4 Alert in the event of an audit process failure.	●	●	●
3.3.5 Correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.		●	●
3.3.6 Provide audit reduction and report generation to support on-demand analysis and reporting.		●	●
3.3.8 Protect audit information and audit tools from unauthorized access, modification, and deletion.		●	●
3.4 CONFIGURATION MANAGEMENT			
3.4.3 Track, review, approve/disapprove, and audit changes to information systems.	●	●	●
3.4.7 Restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services.	●	●	●
3.4.8 Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny- all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	●	●	●
3.5 IDENTIFICATION AND AUTHENTICATION			
3.5.2 Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.		●	●
3.5.3 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.		●	●
3.6 INCIDENT RESPONSE			
3.6.1 Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.		●	●
3.6.2 Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization.		●	●
3.6.3 Test the organizational incident response capability.		●	●
3.11 RISK ASSESSMENT			
3.11.2 Scan for vulnerabilities in the information system and applications periodically and when new vulnerabilities affecting the system are identified.	●	●	●
3.11.3 Remediate vulnerabilities in accordance with assessments of risk.	●	●	●
3.12 SECURITY ASSESSMENT			
3.12.3 Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.	●	●	●
3.13 SYSTEM AND COMMUNICATIONS PROTECTION			
3.13.1 Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	●	●	●
3.13.6 Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).		●	●
3.13.7 Prevent remote devices from simultaneously establishing non-remote connections with the information system and communicating via some other connection to resources in external networks.		●	●
3.14 SYSTEM AND INFORMATION INTEGRITY			
3.14.1 Identify, report, and correct information and information system flaws in a timely manner.		●	●
3.14.2 Provide protection from malicious code at appropriate locations within organizational information systems.		●	●
3.14.3 Monitor information system security alerts and advisories and take appropriate actions in response.	●	●	●
3.14.4 Update malicious code protection mechanisms when new releases are available.	●	●	●
3.14.5 Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.	●	●	●
3.14.6 Monitor the information system including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.		●	●
3.14.7 Identify unauthorized use of the information system.		●	●

ALERT LOGIC®