ResearchSOC Helps You Comply with NIST 800-171

Meeting regulatory requirements in grants and contracts is becoming increasingly challenging as research institutions face new types of regulated data, such as Controlled Unclassified Information (CUI). Protecting CUI requires implementing roughly a hundred controls described in NIST Special Publication 800-171. ResearchSOC (and OmniSOC) can bolster your compliance effort by fully or partially addressing nearly 20% of these controls in control families such as awareness and training, audit and accountability, incident response, security and risk assessment, systems and communication protection, and system and information integrity.

The following lists NIST 800-171 controls and relevant ResearchSOC services.

CONTROL FAMILY	CONTROL	SERVICE
Awareness & Training	3.2.1. Ensure that managers, system administrators, and users of the organizational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organizational information systems.	OmniSOC - Sharing of timely and routine briefings, reports, and other published products to provide insight into security trends, events, incidents, threats, and threat actors. ResearchSOC - Training on cybersecurity best practices for research.
	3.2.2. Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.	
Audit & 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.	OmniSOC – Processing event data and creating threat intelligence, proactive threat hunting, security event analysis.
	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.	
	3.3.5. Use automated mechanisms to integrate and correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.	

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.	OmniSOC – Proactive threat hunting, notification to incident response teams of adverse events or incidents, monitoring and triaging security events, security event analysis, call center services.
	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.	
Risk Assessment	3.11.2. Scan for vulnerabilities in the information system and application periodically and when new vulnerabilities affecting the system are identified.	ResearchSOC – Vulnerability identification service at Three Rivers Optical Exchange (3ROX).
	3.11.3. Remediate vulnerabilities in accordance with assessments of risk.	
Security Assessment	3.12.1. Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems.	ResearchSOC – Vulnerability identification service at Three Rivers Optical Exchange (3ROX). OmniSOC – Processing event data and creating threat intelligence, proactive threat hunting, security event analysis.
	3.12.2. Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of controls.	
Systems 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.	OmniSOC – Proactive threat hunting, security event analysis. STINGAR – Honeypots to monitor attackers. ResearchSOC - Training on cybersecurity best practices for research.
	3.13.2. Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.	

System and Information Integrity	3.14.3. Monitor information system security alerts and advisories and take appropriate actions in response.	OmniSOC - Sharing of timely and routine briefings, reports, and other published products to provide insight into security trends, events, incidents, threats, and threat actors. ResearchSOC - Vulnerability identification service at Three Rivers Optical Exchange (3ROX).
	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.	
	3.14.7. Identify unauthorized users of the information system.	

For more information, contact the
ResearchSOC Communications & Outreach Manager
Todd Stone: toddston@iu.edu