

# The Most Common Attacks in A Global Crisis & Controls to Prioritize



**CyberSaint**  
S E C U R I T Y





# Phishing

AT-2

## Security Awareness Training

*Provide basic security awareness training to all information system users.*

IA-2

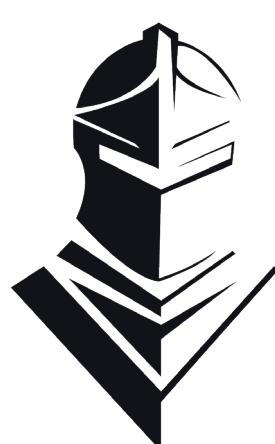
## Identification And Authentication

*The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).*

PM-16

## Threat Awareness Program

*Implement a threat awareness program that includes a cross-organization information-sharing capability.*





# Ransomware

CM-8

## Information System Component Inventory

*Create an information system component inventory that accurately reflects the current system under review.*

RA-5

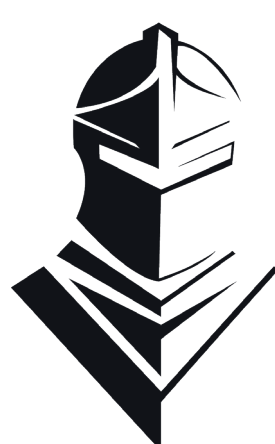
## Vulnerability Scanning

*Scan for vulnerabilities in the system and hosted applications regularly and/or randomly.*

SC-7

## Boundary Protection

*Monitor and control communications at the external boundary of the system and at key internal boundaries within the system.*





# Disseminating False Information

AC-17

## Remote Access

*Develops a remote access policy that covers usage restrictions, connection requirements, and implementation guidance.*

CP-10

## Information System Recovery And Reconstitution

*Provide for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.*

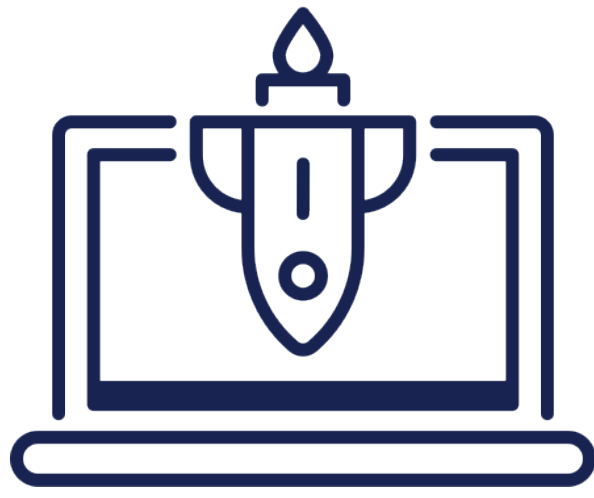
SI-4

## System Monitoring

*Monitor the information system to detect attacks and indicators of potential attacks.*







# Denial of Service

CP-2

## Contingency Plan

*Develop a contingency plan for the information system that identifies essential missions and business functions and associated contingency requirements.*

SC-5

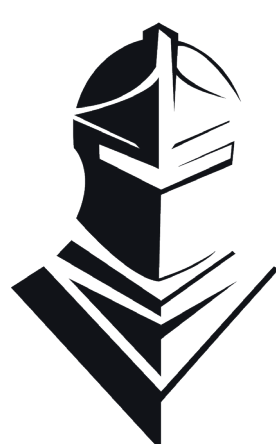
## Denial Of Service Protection

*The information system protects against or limits the effects of denial of service attacks by employing security safeguards.*

SI-5

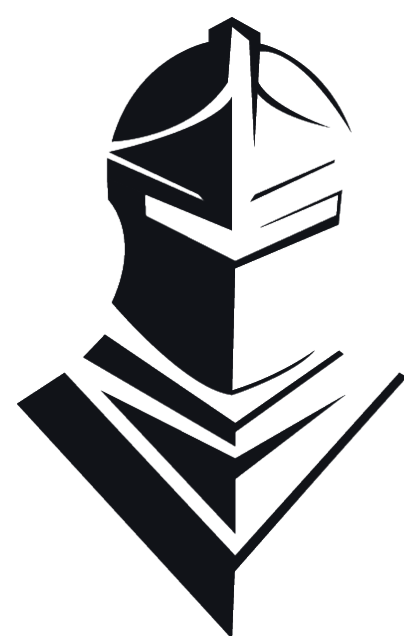
## Security Alerts, Advisories, And Directives

*Receive information system security alerts, advisories, and directives from organization-defined external organizations on an ongoing basis.*



During this time, resources must be allocated to the most critical areas to protect against the most prevalent cyber threats.

**We've launched a practical set of security controls pulled from the NIST Cybersecurity Framework that demonstrates where immediate resource allocation and responses should be taken, prioritizing controls that cover 80% of the impact of the NIST CSF by using 20% of the effort, clearly presented in a way that is actionable for both security teams and executive management.**



**CyberSaint**  
S E C U R I T Y