Cyber-risk Coordination Center Tools and Services Catalog

Premier tools and services are provided to UC campuses, health centers, and labs to ensure that they are equipped with the best cybersecurity management to protect institutional information and IT resources. Learn more about these special tools and services that make UC a safer place to work, learn, and conduct research.

THREAT DETECTION AND IDENTIFICATION (TDI)

The Threat Detection and Identification (TDI) program is a collection of cybersecurity tools, services, and expertise that helps UC identify cybersecurity potential threats, provide network and endpoint visibility, and enable a better understanding of threats and vulnerabilities. TDI harnesses UC and third parties to give UC a common view of security systemwide, which is critical to informing readiness, allocating budget, and measuring risk reduction while also consistently identifying bad actors, malware, and system compromises—enabling a rapid, uniform response.

Attack Surface Management (ASM)

ASM services continuously monitor, identify, and manage the cybersecurity vulnerabilities and potential attack vectors in the cloud and on-premise infrastructures from the attackers' point of view.

Digital Threat Monitoring (DTM)

DTM provides early warning of malicious targeting and potential attacks with visibility into the open, deep, and dark web. This crucial component of the TDI program provides the ability to anticipate threats, sophisticated attack campaigns, breaches, and data leaks.

Leaked Credentials

If a compromised UC user credential is found, the relevant UC location is notified so action can be taken to determine if the password was reused and help the user reset their password.

Managed Detection andResponse (MDR)

Around-the-clock monitoring and alert prioritization working with a range of third-party network, server, and endpoint technologies—on-premise and in the cloud. This service consumes alerts, investigates and analyzes attacker behavior, and performs advanced detection and threat hunting, pairing it with rapid response and remediation to amplify each UC locations' security operations team.

Protection of Network and Endpoints

A common standard is established to leverage expertise across the UC system and to share, track, and respond to cyber incidents in a coordinated fashion. These tools that protect hardware, software, networks, servers, and endpoints are available to all UC locations.

Security Operations Platform

This smart and adaptive platform enables analysts to have visibility across environments, detecting threats with machine learning, AI, and integrated real-time cyber intelligence. It predicts and prevents emerging threats, identifies root causes, and responds in real time.

Suspicious Domain Alerts

Suspicious domains are reviewed, and when a potentially malicious domain is found, the relevant UC location is notified so action can be taken.

INCIDENT RESPONSE COORDINATION

Incident response coordination services provide an organized and systematic approach to a cybersecurity incident or breach and communicate information about the situation.

Breach Notification

This third-party streamlined notification service provides protection from all angles with data breach readiness and response strategy using the latest market insights and trends. Extensive customer notification services include call center reports, mail notification services, and identity protection services.

Incident Response Coordination and Communication

During a cyber incident, a systemwide coordination and communication process is initiated to ensure that all executive stakeholders are informed as details become known. This process also involves internal experts in legal, privacy, compliance, and communications.

Systemwide Incident Escalation Report and Notification (SIREN) Tool

During an information security incident, potentially significant incidents are recorded, updated, and managed in SIREN for shared visibility.

THREAT INTELLIGENCE

Threat intelligence services include obtaining cyber threat information from a variety of sources to protect UC.

Cyber Threat Intelligence Services

The cyber threat intelligence service uses a third party with decades of security expertise to synthesize UC's raw data and deliver improved visibility into tactics that attackers employ, actionable insights, and context around threats.

Threat Intelligence Collection and Sharing

Partnering with a wide variety of local, state, and federal organizations as well as other third-party experts, UC shares threat intelligence and gains valuable insight and visibility into threats occurring right now. Subscriptions include intelligence on cyber threats, cybercrimes, trends from global operation centers, vulnerability analysis, dark web monitoring, industry local threats, and more.

SECURITY RISK ASSESSMENTS

Security Risk Assessments performed at UC locations, supplier, and health affiliates help the University of California manage cybersecurity risks.

Security Risk Assessments at Health Affiliates

Security Risk Assessments at existing and new health affiliates are coordinated on a regular basis to identify, evaluate, and control potential vulnerabilities to information assets at UC health centers.

Supplier Risk Assessments

The cyber risk assessment unit works with UC locations on supplier risk to analyze threats introduced to UC via relationships from suppliers, partners, affiliates, contractors, or service providers. Assessments follow an established systemwide methodology with standard metric tracking.

UC Location Risk Assessments

Campuses, health centers, and labs across UC work together to identify, evaluate, and prioritize potential threats, vulnerabilities, and risks to information assets.

CONSULTING SERVICES

Consulting services are available to assist UC locations in assessing their readiness levels. Services are paired with existing technologies, services, and operations with mitigation practices to manage the financial impacts of data breaches.

Digital Forensics

Digital forensics (also known as computer and network forensics) services involve coordination with forensics experts to perform investigations during and after an incident. These investigations help determine what happened, how and why it happened, and whether/what data was extracted.

Penetration Tests

Penetration tests leverage deep knowledge of threats and attack behavior using the tools, tactics, and procedures seen daily during incident response engagements. UC locations use penetration testing to identify vulnerable assets and receive strategic recommendations for security improvements.

Tabletop Exercises

Tabletop exercises are learning activities led by a third-party facilitator to simulate a real cyber event. These exercises evaluate cyber crisis responses and are invaluable to ensure stakeholders understand their roles, test communication and knowledge, uncover process gaps, and showcase how much is already known from the past.

TRAINING AND AWARENESS

Mandatory and customized cyber security training includes a mix of coaching, courses, and certifications to raise awareness and bridge skill gaps. Events, programs, communities, and tools provide additional opportunities for education and knowledge sharing.

Applied Intelligence Mentorship Program

The eight-month UC Tech Academy: Applied Intelligence Mentorship program consists of monthly modules or workshops that help attendees build and improve their UC locations' Cyber Threat Intelligence (CTI) programs, advance workflows, align CTI initiatives with business needs, and enhance systemwide communication.

Customized Training Modules

In addition to mandatory training, optional modules are available on a range of topics including cyberattacks, remote work habits, social media, phishing, ransomware, data protection, deepfakes, AI, password security, privacy rules and regulations, and much more. Over 1400 knowledge articles provide an opportunity for self-learning.

Information Technology Policy and Security Community (ITPS)

The ITPS group is focused on sharing information related to the cybersecurity community, such as best practices, case studies, regulatory changes, initiatives, training, and more.

Mandatory Cybersecurity Training

Faculty and staff participate in an annual mandatory training that provides up-to-date security awareness education that meets UC standards.

Phishing Simulation Tools

UC leverages some of the world's leading phishing simulation tools to educate users, find vulnerabilities, and protect the UC system from threats as they emerge.

Systemwide Cyber Champions

Cyber Champions is a systemwide workgroup whose goal is to strengthen UC's culture of cybersecurity by empowering employees to help ensure safe computing. Champion team members partner with campus locations and health centers to create systemwide resources and provide support as cybersecurity enhancements are made.

UC Cyber Risk Program Annual Report

The UC Cyber Risk Program Annual Report features stories from all over the UC system, spotlighting the cybersecurity programs, initiatives, tools and services available to the UC system, and people making UC cyber safe.

UC Cyber Security Summit

The UC Cyber Security Summit is a forum for stakeholders and thought leaders to gather and share perspectives, discuss the latest in cybersecurity, network and meet new professionals, and learn practical day-to-day security tips to stay ahead of the curve.

POLICIES, STANDARDS, AND GUIDELINES

Protecting institutional information and IT resources is a collective responsibility shared across the UC system. C3 leads changes to policies, standards, and guidelines through a collaborative community and communicates updates systemwide. Changes in regulations are reviewed, and updates to content are made as necessary.