CAL-CSIC SERVICES & CAPABILITIES
CYBERSECURITY SUPPORT FOR CALIFORNIA PARTNERS

WHO ARE WE?

Our mission is to reduce the likelihood and severity of cyber incidents affecting California's economy and critical infrastructure. Through integrated threat intelligence, premier advisory services, dynamic incident response, and training, we enable coordinated action and improve California's ability to anticipate, withstand, and recover from cyber threats. For additional information & resources, please visit our **website**.

MS-ISAC STATE-WIDE MEMBERSHIP

No-cost cybersecurity services and threat intelligence to state, local, tribal and territorial governments. Benefits provided with membership include threat intelligence and distribution, incident response and forensic services, 24x7x365 access to the Security Operations Center and membership collaboration.

QR Code for Registration

CA Cybersecurity Task Force (CCTF)

QR Code to Sign Up

The California Cybersecurity Task Force is an advisory body to the State of California Senior Administration Officials in matters related to Cybersecurity

SUBCOMMITEES

- Cyber Risk Management
- Workforce Development and Education
- Election Security
- Emerging Technology
- Critical Infrastructure

Fusion Center Liaison (LNO)

Where intelligence meets action

LNO PROGRAM: Embeds cyber professionals in CA fusion centers; integrates Cal-CSIC services & CTI into all-hazards operations

BIDIRECTIONAL REPORTING: Rapid CTI/incident sharing: fusion centers ↔ state leadership ↔ pub/priv partners

CYBER SITUATIONAL AWARENESS: Fusion centers as force multipliers for statewide cyber risk reduction

FEDERAL/NATIONAL SYNC: Aligning with NFCA, CISA, FBI, InfraGard, STAS/STAC

FOCUS AREAS: Processes, authorities, data flows for timely/trusted threat & incident exchange

OPERATIONAL FRAMEWORKS: In development; enable consistent cyber services & actionable intel through fusion enterprise

CYBER OPERATIONS CENTER (CYOC)

Your central hub for cyber incident coordination

1. Central communication node for CYOC operations, synchronizing internal coordination, and external stakeholder engagement.
2. Conduct and sustain outreach to affected entities, integrate Cal-CSIC services, and ensure timely, accurate information flow across all parties.
3. Maintain continuous situational awareness and act as the enduring point of contact throughout the incident lifecycle, ensuring unity of effort and operational transparency.

CONTACT INFORMATION: calcsic@caloes.ca.gov (916) 636-2997

TLP: CLEAR

CAL-CSIC SERVICES MENU
CYBERSECURITY SUPPORT FOR CALIFORNIA PARTNERS

Cal OES
GOVERNOR'S OFFICE OF EMERGENCY SERVICES

Subscription Intelligence Services

Continuous support to maintain your security posture

AUTOMATED INDICATOR EXCHANGE

Defensive network detections and real-time state-wide intelligence sharing.

Requirements: Reports regarding malicious behavior observed in your environment, including IOCs, MITRE attack techniques, and malware samples.

Deliverables: Access to the Threat Intelligence Platform (TIP) and automated IOC integrations into defensive systems (e.g., Sentinel, Splunk).

CYBER THREAT INTELLIGENCE REPORTING

Proactive awareness of adversary behaviors and emerging cyber risks.

Requirements: Recipient name, organization title, and official email.

Deliverables: Weekly Cyber Threat Intelligence Reports and urgent Cyber Advisories (CVEs, Zero Day Exploits).

ATTACK SURFACE MONITORING

Continuous visibility into externally exposed assets to identify misconfigurations.

Requirements: External IP ranges and identification of asset types (on-premises or cloud).

Deliverables: Direct alerts and notifications of vulnerabilities affecting your environment.

Customized Intelligence Services

Tailored assessments based on specific organizational needs

DIGITAL THREAT MONITORING

Early insight into threat actor intent across digital channels and the dark web.

Requirements: Keywords (brands, executives), password policies, and authentication URLs.

Deliverables: **Time-sensitive** alerts, domain takedown notifications, and identification of compromised credentials).

PHISHING ANALYSIS INTELLIGENCE

Detects and analyzes phishing threats targeting the organization and its brand.

Requirements: Suspicious emails sent as **.msg** or **.eml** attachments to the official phishing analysis email address.

Deliverables: Analysis findings reports and targeted mitigation recommendations.

INCIDENT INTELLIGENCE SUPPORT

Analytical support during and after active security breaches to guide containment.

Requirements: Known indicators, access to logs, incident timelines, and identification of affected business units

Deliverables: Rapid threat actor identification, enriched IOCs, and a final Post-Incident Intelligence Report.

IMPORTANT: Meeting these requirements ensures lawful collection and analytic validity. Incomplete or restricted inputs may limit visibility and reduce the overall effectiveness of the service.

TLP: CLEAR

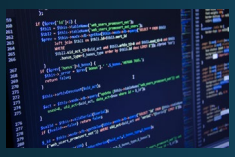
CAL-CSIC SERVICES MENU
CYBERSECURITY SUPPORT FOR CALIFORNIA PARTNERS

Cal OES
GOVERNOR'S OFFICE OF EMERGENCY SERVICES

Cyber Advisory Team (CAT)

Sharpening your defenses before the fight begins

PROGRAM AND SECURITY ASSESSMENT

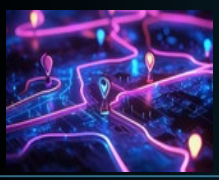


A strong defense starts with knowing your weaknesses. We evaluate your security program's maturity, identify critical gaps, and provide actionable insights to strengthen your overall posture.

ADVISORY BRIEFINGS & THREAT AWARENESS

The threat landscape never stops evolving. We deliver expert briefings tailored to your environment, so your leadership and teams are always informed and prepared.

REMEDIATION ROADMAPS



Findings mean nothing without a plan. We translate scan results and assessment findings into a clear, prioritized roadmap so your team knows exactly what to fix and when.

ADVOCACY SUPPORT

Cybersecurity initiatives need a champion. We work alongside you to build the case for security investments and drive alignment across leadership and stakeholders.

VULNERABILITY SCANNING & PENETRATION TESTING

Attackers are always looking for a way in. We systematically scan your internal and external environments to surface hidden vulnerabilities before they can be exploited. This includes **penetration testing**, where we simulate real-world attacks to validate findings and uncover weaknesses that automated scans alone may miss.

EXTERNAL & INTERNAL VULNERABILITY SCANNING: We conduct comprehensive internal and external vulnerability assessments to identify security gaps across networks, systems, applications, and internet-facing assets. Findings are prioritized by severity and paired with actionable remediation guidance to help reduce risk efficiently.

PENETRATION TESTING: Our penetration testing services simulate real-world attack scenarios to validate vulnerabilities, test defensive controls, and uncover weaknesses that automated scans alone may miss. This provides a deeper understanding of exploitable risk within your environment.

Requirements: Formal written consent and authorized IP ranges/domains are required prior to testing.

Deliverables:

- External and internal vulnerability assessment reports
- Severity-ranked findings with risk ratings
- Actionable remediation guidance and recommendations
- Executive summary outlining key risks and priorities

TLP: CLEAR

CAL-CSIC SERVICES MENU
CYBERSECURITY SUPPORT FOR CALIFORNIA PARTNERS

Digital Forensics & Incident Response (DFIR)

OES DFIR report of findings meets specific requirements designed to serve legal, financial, and claims-based purposes — not just technical remediation

INCIDENT RESPONSE

RANSOMWARE: A ransomware attack can cripple operations in minutes. Our team deploys rapidly to contain the threat, recover critical systems, and get you back online with minimal disruption.

INSIDER THREATS: Not every threat comes from outside. We investigate and neutralize malicious or negligent insider activity before it escalates into a larger crisis.

DATA BREACH / EXFILTRATION: Covers the unauthorized access and removal of sensitive data including PII, PHI, financial records, intellectual property, and credentials whether conducted by external threat actors or malicious insiders.

NETWORK INTRUSION: When attackers breach your perimeter, speed is everything. We detect, contain, and analyze unauthorized access to stop data loss in its tracks.

CLOUD/SAAS INCIDENTS: Covers account compromise and takeover of cloud platforms and SaaS environments, including AWS, Azure, and GCP account compromise, as well as Office 365 and Google Workspace compromise.

NETWORK TRAFFIC INTELIGENCE (NETFLOW ANALYSIS): Detect anomalies, suspicious behaviors, and lateral movement within network patterns.
Requirements: **Formal written consent** and specific CIDR ranges to be scanned.
Deliverables: Malicious traffic findings, enriched indicators, and mitigation recommendations.

DIGITAL FORENSICS

MALWARE ANALYSIS: Understanding your enemy is the first step to defeating it. We dissect malicious software to uncover its behavior, origin, and full scope of impact.

MULTI-PLATFORM FORENSICS: Threats don't discriminate by device. We conduct thorough forensic investigations across Windows, Unix, iOS, Android, and Mac environments to leave no stone unturned.