GAVIN NEWSOM
GOVERNOR

NANCY WARD
DIRECTOR

Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

May 15, 2024

The Honorable Freddie Rodriguez
Chair, Assembly Committee on Emergency Management
California State Assembly
1020 N Street, Room 360B
Sacramento, CA 95814

The Honorable James Ramos
Chair, Assembly Budget Subcommittee No. 6 on Public Safety
California State Assembly Capitol Office, 1021 O Street, Suite 8310
Sacramento, CA 95814

The Honorable Bill Dodd
Chair, Senate Governmental Organization Committee
California State Assembly
1020 N Street, Room 584
Sacramento, CA 95814

The Honorable Aisha Wahab
Chair, Senate Subcommittee No. 5 on Corrections, Public Safety, Judiciary, Labor, and Transportation
1020 N Street, Room 502
Sacramento, CA 95814

Mr. Drew Soderborg
Legislative Analyst's Office
925 L Street, Suite 1000
Sacramento, CA 95814

Subject: REPORT TO CALIFORNIA LEGISLATURE REGARDING BUDGET ACT OF 2020

Dear Senators Dodd and Wahab, Assemblymembers Rodriguez and Ramos and Mr. Soderborg:

Pursuant to the California Budget Act of 2020, Item 0690-001-0001 of Section 2.0, the Governor's Office of Emergency Services (Cal-OES) is required to report annually during budget subcommittee hearings on the activities and outcomes of the California Cybersecurity Integration Center (Cal-CSIC) and the Cyber Incident Response Team (CIRT) to the appropriate policy and fiscal committees of the Legislature.

This report includes: (1) the number, source(s), and target(s) of cyber attacks in California; (2) how the center responded to each, and whether any of the center's investigations have led to prosecutions; and (3) a summary of special bulletins, notices, and awareness efforts of the center.

Should you have any questions, please contact Deputy Director of Legislative and Governmental Affairs, Bridget Kolakosky at (916) 364-4635 or bridget.kolakosky@caloes.ca.gov.

Sincerely,

Nancy Ward

NANCY WARD
Director

cc: Ann Patterson, Cabinet Secretary, Office of the Governor

REPORT TO CALIFORNIA LEGISLATURE

REGARDING BUDGET ACT OF 2020

ACTIVITIES AND OUTCOMES OF CALIFORNIA CYBERSECURITY INTEGRATION CENTER, 2021 TO 2023

February 1, 2024

Contents

EXECUTIVE SUMMARY

Pursuant to Section 2 of Chapter 7 of 2020 (AB 89, Ting). The Office of Emergency Services (Cal-OES) is required to report annually during budget subcommittee hearings on the activities and outcomes of the California Cybersecurity Integration Center (Cal-CSIC) and the Cyber Incident Response Team (CIRT) to the appropriate policy and fiscal committees of the Legislature no later than February 1, 2024.

The reporting period for this report covers calendar years 2021-2023 (January 1, 2021to December 31, 2023) and includes the required information:

(A) Tables 1-3 provides the number, source(s), and target(s) of cyber-attacks in California.
(B) Tables 4-5 address how the center responded to each, and information regarding any of the center's investigations that have led to prosecution can be found on page 12.
(C) Tables 7-8 provide a summary of special bulletins, notices, and awareness efforts of the center.
(D) A summary of the data provided during the annual reports of the prior three (3) years.

This report covers the reporting period of calendar years 2021-2023 by calendar year (January 1, 2021 to December 31, 2023). Information from the first two years was presented verbally during annual budget hearings and is summarized throughout the report. This report describes how the Cal-CSIC mitigated several major cybersecurity incidents through effective incident response and proactive threat intelligence, and how the Cal-CSIC assisted numerous impacted entities with recovery. Among these entities are the California Department of Finance[1] and several local government entities in California.

DEFINITION OF KEY TERMS

For the purpose of this report, a Cal-CSIC definition will be used to ensure continuity and alignment with the cybersecurity industry standards.

Cyber attack is defined by the National Institute of Standards and Technology (NIST). NIST defines an "attack" in the context of information security as any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.[2] NIST further defines a "cyber attack" as an attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information. The NIST definition of "cyber attack" is derived from Committee on National Security Systems Issuance (CNSSI) No. 4009, the most recent version of which from March 2022 defines "cyber attack" as actions taken in cyberspace that create noticeable denial effects (i.e., degradation, disruption, or destruction) in cyberspace or manipulation that leads to denial that appears in a physical domain.[3] The Cal-CSIC generally uses the NIST and CNSSI definitions; however, the Cal-CSIC has standardized and widely uses the term "cyberattack" (without a space), consistent with recently enacted state law (EDC Code Section 35265), DoD Intelligence community usage, and the latest National Cybersecurity Strategy[4],

[1] https://news.caloes.ca.gov/statement-on-cybersecurity-incident/
[2] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
[3] https://www.cnss.gov/CNSS/issuances/Instructions.cfm
[4] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

due to NIST's and DoD's variable use of "cyber attack", "cybersecurity attack", "cyberspace attack" and "cyberattack".

Source is closely related to the NIST-defined word "threat source." The definition from NIST for threat source is "a malicious person with harmful intent or an unintended or unavoidable situation (such as a natural disaster, technical failure, or human error) that may trigger a vulnerability".[5]

Target the verb form, in NIST publications, (i.e., to target) and the adjective "targeted" are used far more commonly than the noun target itself in terms of the target of an attack. Enterprises, organizations, individuals, or systems can be targeted or the targets of attack. In these contexts, the specific recipient of the attack is described with the prefixes "target" or "victim."[6] For the purposes of this report, the Cal-CSIC has interpreted "target" as any targeted or victimized entity or system.

Incident is an occurrence that, actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

In its normal operations and following community best practices, the Cal-CSIC primarily tracks cybersecurity incidents. The Cal-CSIC uses the definition of an incident as defined by Federal law (see 44 U.S.C. § 3552(b)(2))[7] and guidelines from NIST[8].

Cybersecurity event is an event that has been determined to have an impact on the organization prompting the need for response and recovery.[9] As parts of a taxonomy, cyberattacks are a subset of cybersecurity incidents which are a subset of cybersecurity events. While an event or incident may actually be a cyberattack, analysts, incident responders, and investigators may not see it or count it as a cyberattack until enough information has been gathered to classify

[5] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf
[6] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf
[7] 44 USC 3552: Definitions (house.gov)
[8] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
[9] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

it definitively. The amount of time this takes varies greatly but could range from minutes to years to (effectively) never. Often, this is not evident immediately or even as events or incidents are reported. As cases proceed, an event initially counted as an incident may develop into what is considered a cyberattack. It is also possible that events initially reported as cyberattacks are actually just incidents or events upon further analysis.

Data in this report will present cyberattacks as a subset of incidents tracked by the Cal-CSIC.

CYBER INCIDENT AND CYBERATTACK SUMMARIES

The Cal-CSIC mitigated several major cybersecurity incidents through effective incident response and proactive threat intelligence. Cal-CSIC efforts likely prevented or stopped a number of imminent cyberattacks and limited the impact of attacks which did occur. If not for the timely intervention by the Cal-CSIC these attempted cyberattacks could have impacted several schools and city governments.

The number of incidents reviewed by the Cal-CSIC in the California Compliance and Security Incident Reporting System (CAL-CSIRS) increased by 21% from 2021 to 2022. The increase from 2022 to 2023 was 42%. This exponential increase over three (3) years was mitigated by Cal-CSIC efforts ranging from consultations to full-scale incident response. An example of a full scale incident response is the Department of Finance (DOF) Lockbit Black cyberattack that occurred in 2022 which resulted in data exfiltration. Due to the aid of the Cal-CSIC, the DOF was able to rebuild their entire infrastructure and meet the deadline for the constitutional mandate to publish the Governor's budget on January 10, 2023. These actions ultimately protected the citizens of the State of California from expanding cybersecurity threats.

During the reporting period, ransomware and data breaches dominated the cybersecurity threat environment. Ransomware attacks grew by 57% from 2021 to 2023. The increase in attacks is accounted for by the Cal-CSIC's improved operational processes which captured more information. However, it should be noted there continues to be a significant upward trend in ransomware attacks. Moreover, during that same period, data breach incidents grew by 35%.

Phishing, an electronically delivered social engineering technique, continues to be a prevalent and effective tactic.

The Cal-CSIC's tracking methodology for cyber events has changed over the last three years, causing a disparity between cyber incident/attacks and the total number of targets identified.

Table 1: Cyber Incident/Attacks by Year and Type

Cyber Incident/Attacks	2021	2022	2023	Total
Ransomware	185	169	290	644
Corporate Data Breach[A]	137	162	185	484
Social Engineering (Phishing variants)	56	41	55	152
Other[B]	13	55	62	130
Malware variants (other than ransomware)	5	7	39	51
Denial of Service variants	5	17	27	49
Website Defacement	9	10	8	27
Total Cyber Incident/Attacks	**410**	**461**	**666**	**1537**

A. Corporate data breach reflects the threshold of 500 impacted individuals. California law requires a business or state or local agency to notify any California resident whose unencrypted personal information, as defined, was acquired, or reasonably believed to have been acquired, by an unauthorized person. Pursuant to California Civil Code Section 1798.29(a) for state agencies and Section 1798.82(a) for businesses or persons.
B. There are a large number of incident/attack categories that can be considered here but are less prevalent and are grouped as 'other'.

Table 2: Threat Sources Identified During Cyber Incidents/Attacks

Threat Sources by Year	2021	2022	2023
Top Threat Actors[A]	FIN11	Black Basta	CL0P
	Bitwise Spider	Karakurt	8Base
	Vice Society	Vice Society	BianLian
	Marketo Marketplace	Lazarus	Play
	KURDISH H4xOR (aka 0x1998)	0ktapus	Anonymous Sudan
Top Malware	Lockbit	Lockbit	Lockbit
	Conti	ALPHV	ALPHAVM/BlackCat
	CL0P	Conti	Akira
	DoppelPaymer	Hive (or HiveLocker)	Black Basta
	Pysa	Quantum	Cactus

A. "Threat Actor" is an individual or group with malicious intent and is generally the ultimate "source" of a cyberattack, regardless of the route, mechanisms, or tactics, techniques, and procedures (TTPs) used to execute the attack.

Table 3: Target(s) of Cyber attacks

Critical Infrastructure Sector	2021 Number of Targets	2022 Number of Targets	2023 Number of Targets
Chemical	0	2	6
Commercial Facilities	67	55	60
Communications	2	2	7
Critical Manufacturing	37	17	38
Dams	0	0	0
Defense Industrial Base	1	6	1
Emergency Services	2	2	6
Energy	2	5	4
Financial Services	35	35	50
Food and Agriculture	21	15	22
Government Facilities	53	54	163
Healthcare and Public Health	68	52	81

Information Technology	40	119	93
Nuclear Reactors, Materials, and Waste	0	0	0
Other - targets that are not considered critical infrastructure sector entities	69	86	118
Transportation Systems	12	8	16
Water and Wastewater Systems	1	3	1

INCIDENT RESPONSE

The Cal-CSIC has seen a significant increase in both incidents tracked and incidents responded to. Incident response activity includes incident response actions triggered by information reported in CAL-CSIRS, direct requests for assistance by entities experiencing a cybersecurity event, incident, or cyberattack, and proactive services intended to prevent cyberattacks.

The Cal-CSIC established a Cyber Incident Response Team (CIRT)to serve as California's primary unit to lead cyber threat detection, reporting, and response in coordination with public and private entities across the state. The Cal-CSIC CIRT has been actively engaged in responding to, assisting with recovery from, and in some cases preventing cybersecurity incidents and cyberattacks during the reporting period.

Cybersecurity tickets forwarded by Department of Technology (CDT) through the CAL-CSIRS system increased by 86% from 2021 to 2023. While most of these did not involve deployment of incident response teams, the Cal-CSIC analyzed the reports and determined the level of response needed. This often required extensive coordination with CDT and other partner agencies. The portion of these which the Cal-CSIC did provide response services for increased from 2022 to 2023 by 26%. Additional reports or requests for assistance come to the Cal-CSIC from outside CAL-CSIRS, and this increased 220% from 2021 to 2023, as shown in Table 4.

Table 4: Incident Response* Activity by Year

CALENDAR YEAR	2021	2022	2023
CAL-CSIRS Incidents Analyzed [A]	2158	2621	4014
CAL-CSIRS Incidents Responded To	316	224	219
Non-CAL-CSIRS Incidents Responded To	88	104	92
Total Cal-CSIC Incident Response Events	404	328	311

*Considerations for reported metrics should include variations in the classification of an 'event' as breaches may include multiple IR events.

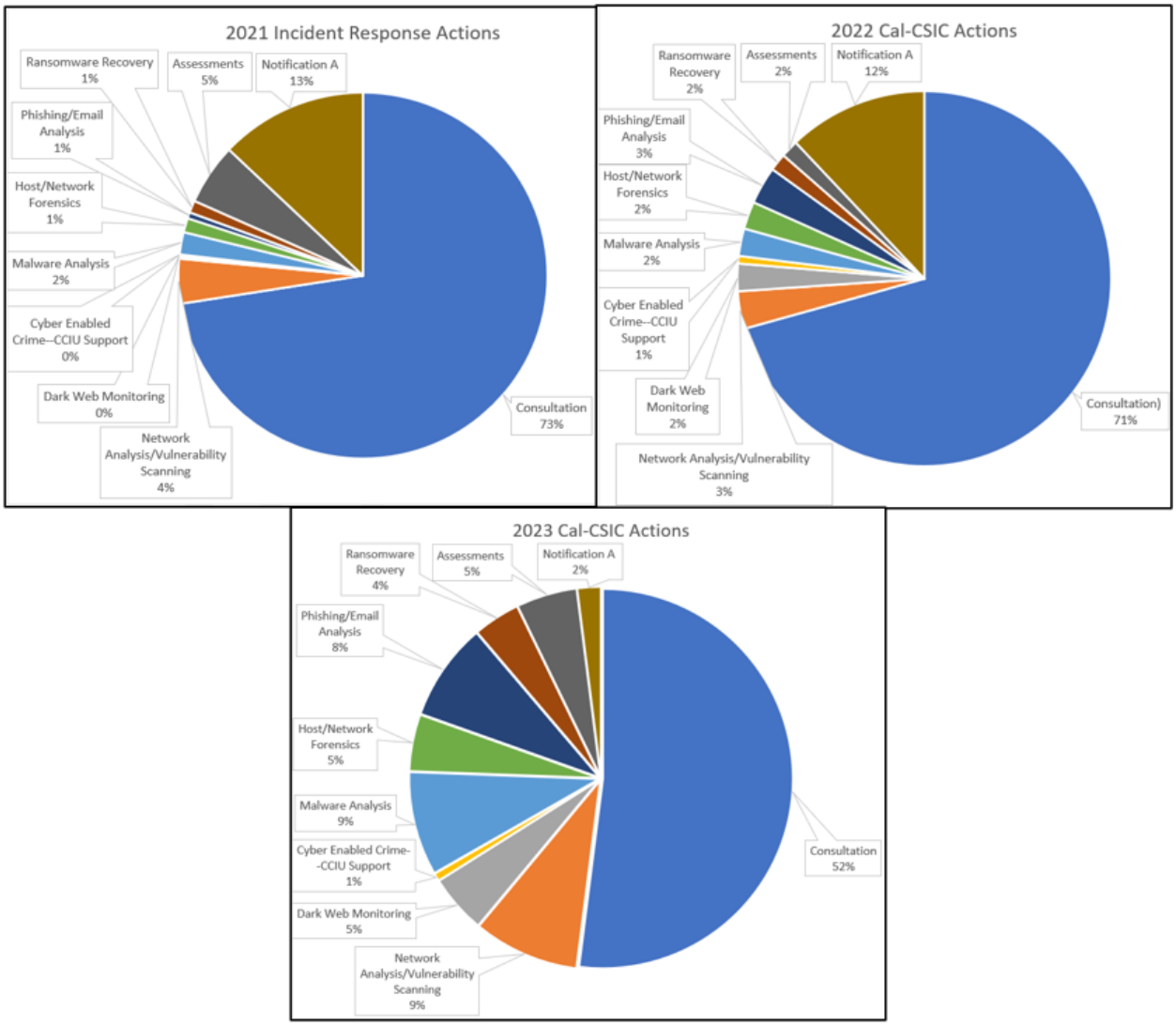
A. Subset of all Cal-CSIRS incidents identified as cybersecurity and forwarded to Cal-CSIC for analysis and appropriate follow up.

Table 5: Incident Response Actions by Year and Type (2021-2023)

Cal-CSIC Incident Response Action	2021	2022	2023
Consultation	404	328	311
Network Analysis/Vulnerability Scanning	22	15	54
Dark Web Monitoring	1	11	30
CCIU Investigation Support	1	3	4
Malware Analysis	11	11	53
Host/Network Forensics	7	11	29
Phishing/Email Analysis	7	15	50
Ransomware Recovery	6	7	24
Assessments	30	20	31
Notification [A]	72	56	12
Subtotal [B]	**561**	**477**	**598**
Total Cybersecurity Incidents Observed Statewide [C]	**420**	**480**	**702**

A. Notifications are cyber events where Cal-CSIC discovered a threat or vulnerability using threat monitoring services—such as bug bounty and passive threat warning systems—resulting in the notification of effected agencies. Due to the Cal-CSIC's limited insight into an effected entities network, the Cal-CSIC's ability to categorize or rate the severity of these events is limited.
B. Total incident response actions by the Cal-CSIC incident response team (Cyber Operations Branch)
C. Total Cybersecurity Incidents observed through threat intelligence

Note: This data was tracked differently prior to 2021 as internal processes were still being developed.



A portion of incident response events also include Mission Resource Taskings (MRT). MRTs require resources drawn from outside Cal-CSIC, typically from the California Military Department (CMD) to include additional personnel not already assigned to Cal-CSIC. MRTs can be used when a cyber incident exceeds Cal-CSIC's capacity to respond. During this reporting period, the Cal-CSIC leveraged this resource three times, once in 2021, and twice in 2022.

PROSECUTIONS RELATED TO INVESTIGATIONS SUPPORTED BY CAL-CSIC

Due to the complexity of a cyber crime, coupled with multijurisdictional and often multinational aspects, threat actor attribution and identification is complex. Cyber related crimes typically require longer investigations and prosecutive timelines. Once threat actor attribution is obtained, actual arrest and subsequent extradition is a lengthy process. We work closely with our allied law enforcement partners to either enhance their on-going investigations or initiate new criminal investigations. As of the date of this report, the Cal-CSIC is unable to report any prosecution results from our law enforcement, District Attorney Offices, and United States Attorney Office partners.

If a cybersecurity incident is determined to have a criminal nexus, Cal-CSIC law enforcement partners (California Highway Patrol, Federal Bureau of Investigation (FBI), Department of Homeland Security, Homeland Security Investigations, etc.) would determine the appropriate investigative lead, with support by Cal-CSIC, if needed.

The Cal-CSIC has supported twenty- one[10] federal law enforcement cybersecurity investigations within the reporting period. Half of these investigations involved critical infrastructure sectors. Of the twenty-one investigations, the Cal-CSIC supported these investigations in three ways: Investigative Leads (ten), Victim Notifications (nine), and Evidence Collection (two).

Investigative Leads involve the Cal-CSIC notifying our federal law enforcement partners, most typically the FBI, results of our forensic analysis produced during the course of a cyber incident response event when threat actor attribution or ransomware variant aligns with an already existing on-going investigation.

Victim Notification involve the sharing of cyber threat information received from our federal partners and Cal-CSIC conducting notification to potential victim entities.

[10] These are separate and distinct from the 21 ransomware recovery efforts mentioned earlier in this report – that they are the same count is a coincidence.

Evidence Collection involves the Cal-CSIC through its normal course of incident response and forensic analysis activities, sharing results of our analysis, such as Indicators of Compromise (IOC) to our law enforcement partners.

SPECIAL BULLETINS, NOTICES, AND AWARENESS EFFORTS

Cal-CSIC's Cyber Threat Intelligence (CTI) Branch provides bulletins, notices, and awareness efforts which are summarized in Table 7. CTI's portfolio includes Morning Reports, Monthly Threat Briefs, other cyber threat intelligence production, and an intelligence product distribution list to distribute these products to a broad array of stakeholders. These products share cyber threat intelligence on emerging threats, new malware, tactics, techniques, and procedures (TTPs), or vulnerabilities, and include threat mitigation recommendations. Information is sourced from federal partners, commercial feeds, and open-source intelligence.

CTI also provides proactive notifications where Cal-CSIC discovered a threat or vulnerability using threat monitoring services resulting in the notification of affected agencies. These notifications include vulnerabilities, vulnerability assessments and malicious activity notifications. All these services have generally grown across every category over the reporting period.

Table 7: Cyber Threat Intelligence Production

Categories Of Bulletins, Notices, And Awareness Efforts	**2021**	**2022**	**2023**
Cyber Intelligence Service Subscribers: Morning Reports (2021-2023)	854	1321	1103[A]
Cyber Intelligence Service Subscribers: Monthly Threat Brief (2021-2023)	880	1337	1596
Cyber Intelligence Service Subscribers: Intel Product Distro List (2021-2023)	1317	1820	1320
Cyber Threat Intelligence Production (2021-2023)	439	413	920
Major Joint Events Supported - Exercises, National Security Events (2021-2023)	7	5	18
Threat Intelligence Platform – Automated Information Sharing [B]	-	-	125
Proactive Notifications [C]	374	360	617

A. The decrease in this reported number, as compared to 2022 is a result of the implementation of a new email distribution list management system.
B. The Cal-CSIC has implemented an Automated Information Sharing service through its Threat Intelligence Platform. This service enables automated, real-time sharing of tactical cyberthreat intelligence and other relevant information that is incorporated into the network defense and network monitoring systems of the agencies and organizations that are subscribed to it. This system was implemented in 2023 and therefore data is not available for prior years.
C. Proactive Notifications are cyber events where Cal-CSIC discovered a threat or vulnerability using threat monitoring services—such as bug bounty and passive threat warning systems—resulting in the notification of affected agencies that covers vulnerabilities, vulnerability assessments and malicious activity notifications. Due to the Cal-CSIC's limited insight into affected entities' networks, the Cal-CSIC's ability to categorize or rate the severity of these events is limited.

The Cal-CSIC also supports major joint events such as exercises and National Security Special Events (NSSEs) which has increased significantly over the reporting period by a staggering 157%. These events involve information sharing, training, professional networking, opportunities to exercise realistic cybersecurity scenarios or apply skills and training to real-world events with partners across many agencies and organizations. The data relating to these events are detailed in Table 8 below.

Table 8: Major Joint Events Supported

Event Type	Description	2021 - 2023
Conference/Symposium	An event where Cal-CSIC personnel presented and/or met with industry professionals to engage on cybersecurity issues.	6
Tabletop Exercise	A discussion-based exercise where Cal-CSIC met with various organizations to understand respective roles in cyber events, incidents or attacks and response plans.	8
Major Exercise	A comprehensive, real-world simulation of a cyber incident involving Cal-CSIC, and multi-agency personnel designed to evaluate and train to response plans.	3
Cal-CSIC Hosted Awareness Events	An event where external partners and organizations visit the Cal-CSIC for a tour and capability discussion.	16
Special Event support (SEAR, NSSE)	An event with an elevated risk rating that required Cal-CSIC personnel to monitor and report on cyber events, incidents or attacks.	5
Other	Various exercises and awareness/support events, categorized differently in prior years.	12

ADDITIONAL PROACTIVE EFFORTS

In addition to reactive incident response services, the Cal-CSIC has also been engaged in proactive services intended to prevent cyberattacks. These include Victim Notifications, Ransomware Recovery, and Assessments.

Victim Notifications are cyber events in which the Cal-CSIC is notified by law enforcement, or other sources, about an entity that may have an undetected cyber event impacting their network.

In 2023, CDT in coordination with the Cal-CSIC introduced a Bug Bounty program which contributed to preventative measures customers could take to remediate vulnerabilities in their networks to avoid becoming victims. This contributed to a significant increase in Victim Notifications.

Also introduced for the first time in 2023, the Cal-CSIC has supported the FBI with distribution of decryption keys to victims of the Blackcat ransomware campaign. This was due to collaborative efforts between the Cal-CSIC, Fusion Centers, and the FBI and represents a success in mitigating the impacts of incidents, such as ransomware.

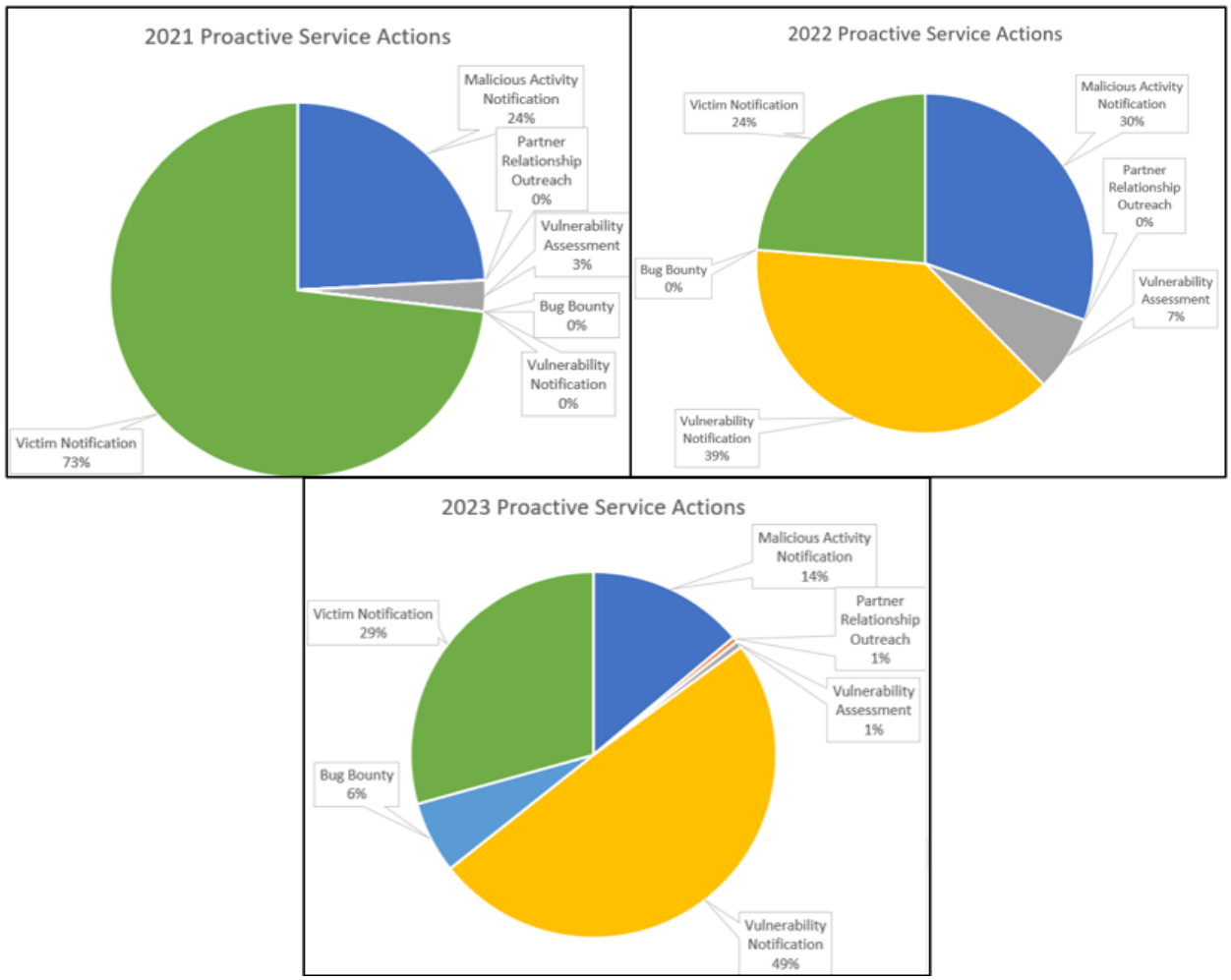
The assessments described above are proactive consulting sessions with entities which have requested cybersecurity assistance and do not require incident response. The Cal-CSIC provides Victim Notifications where the Cal-CSIC is notified by law enforcement or other sources about an entity that may have an undetected cyber event impacting their network and the Cal-CSIC alerts that entity. These proactive threat mitigation actions are separated by year and described in Table 9 below.

Table 9: Proactive Threat Mitigation Actions by Year and Type (2021-2023)

Cal-CSIC Proactive Threat Mitigation Actions	**2021**	**2022**	**2023**
Malicious Activity Notification	72	118	208
Partner Relationship Outreach	0	0	7
Vulnerability Assessment	8	28	9
Vulnerability Notification	0	150	739
Bug Bounty	0	0	95
Victim Notification	218	92	439
Total Actions *	**298**	**388**	**1,497**

Cal-CSIC Proactive Threat Mitigation Actions	2021	2022	2023
*Considerations for reported metrics should include the Cal-CSICs maturity and variations in how data was and is now classified.			

The pie-charts below are a visual representation of the data presented in Table 9 above, by percentage.



CONCLUSION

The Cal-CSIC in coordination with its key partners is committed to reducing the frequency and severity of cyberattacks in California. The Cal-CSIC assisted in mitigating several major cybersecurity incidents through rapid and effective incident response and by preventing potential cyberattacks through proactive sharing of threat intelligence. Over the course of the past three years, the Cal-CSIC and CIRT teams have continuously improved their data collection process and data categorization. The data has shown that the Cal-CSIC has consistently provided support year over year to local, state, and federal entities. This support has substantially increased in both quantity and quality. The Cal-CSIC is continuing to improve how cybersecurity incidents are tracked, analyzed, and responded to. Amplifying this process is the Cal-CSIC's continued and expanding engagement with critical partners including federal and state law enforcement, other state agencies, tribal governments, local governments, non-governmental organizations, private industry, and a diverse array of experts and stakeholders through the California Cybersecurity Task Force. In a few short years, the Cal-CSIC has grown from a small "start-up" organization to become the "go-to" state authority on cybersecurity incident response and threat intelligence.