Imagine that you’ve taken on the mission of providing regular updates on cyber threats to state leadership. And you’re responsible for reducing the likelihood and severity of cyber incidents statewide. If that’s not enough of a challenge, consider this: You’re building a new cybersecurity center from the ground up.

That was the situation facing Keith Tresh, who was appointed commander of the California Cybersecurity Integration Center (Cal-CSIC) in the Governor’s Office of Emergency Services in the fall of 2016. “The program,” Tresh says, “was very much in its infancy.

The creation of the Cal-CSIC
On August 31, 2015, Governor Edmund Gerald “Jerry” Brown, Jr. issued Executive Order B-34-15 for the creation of the Cal-CSIC.

The Cal-CSIC’s marching orders? “Strengthening the state’s cybersecurity strategy and improving inter-agency, cross-sector coordination,” as well as facilitating “more integrated information sharing and communication with local, state and federal agencies, tribal governments, utilities and other service providers, academic institutions and non-governmental organizations.”

Because of the size of California’s economy (the fifth largest in the world), it’s a big target for cyberattacks. But due to decentralization—and the breadth of the Cal-CSIC’s mission to provide statewide support from border to border—delivering a unified view into cyber threats to California state leadership is a daunting task.

Responding to the executive order
Deloitte began working with the Cal-CSIC in May 2016 on phase one of the project. “Deloitte’s priorities in this phase were helping the Cal-CSIC conduct a gap assessment across security capabilities, design the program’s framework, and define the program development strategy and target state,” says Maxim Kovalsky, senior manager in the Cyber Risk practice of Deloitte & Touche LLP.

Deloitte worked with the Cal-CSIC to determine how to implement the executive order. Interviews with 22 information security officers across the state helped Deloitte and the Cal-CSIC identify critical business requirements for the organization:

- Provide enhanced visibility into cyber threats impacting California
- Facilitate cyber threat intelligence sharing
- Assist with incident response

Deloitte also worked with the Cal-CSIC on recognizing specific challenges:

- California’s email-based public information sharing system had difficulty keeping pace with cyberattacks—and with cyberattackers who can quickly shift their tactics.
- Many of California’s public-sector agencies have the necessary security tools. But in some cases, there weren’t enough personnel, or personnel with the correct skill set, to configure and maintain those tools effectively.
- Cybersecurity talent shortages are particularly acute within the public sector nationwide. California’s agencies are no exception.
- California’s intelligence-sharing models are based on the voluntary sharing of information. But partners may be reluctant to share information due to resource constraints or the fear of exposing vulnerabilities.

“I’ve never been a marketer,” Tresh says. “But this is really a marketing job. Because the program is voluntary, the Cal-CSIC needed to build trust. We needed to let potential partners know who we are and what we can do for them.” Furthermore, the Cal-CSIC also needs to demonstrate its value to remain relevant.

Implementing an information sharing program
The four-month conceptual phase ended in September 2016. Deloitte then recommended the implementation of an automated information sharing program, which began in March 2017.

“It was really a privilege to have been invited by the Cal-CSIC to help implement this first-of-a-kind state government program, to see the vision become reality,” Kovalsky says.

Implementation of the information sharing program encompassed:

Technology architecture focused on automation. Automating the information sharing life cycle, from incident reporting and triage to enrichment and prevention, would enable the Cal-CSIC and its partners to accomplish more with fewer resources. The technologies automated indicators of compromise (IOCs) sharing with partners. They also allowed partners to automate the sharing of security events, which were generated based on internal detection rules, back to the Cal-CSIC.

Pilot partners. Because the Cal-CSIC’s processes and technologies would take time to reach maturity, Deloitte recommended a six-month pilot program. Three agencies agreed to become pilot partners: the Franchise Tax Board, the California Department of Corrections and Rehabilitation, and the Office of Emergency Services (the broader agency that the Cal-CSIC is part of).

Security information and event management (SIEM). Deloitte helped the Cal-CSIC enhance the utility of the partner agencies’ SIEM tools and defined 20 foundational cyber threat detection use cases that each partner entity would be expected to implement. This would ensure that the partners could meaningfully leverage the IOCs shared by the Cal-CSIC.

Lessons learned. Upon completion of the pilot, Deloitte brought together the partners and the Cal-CSIC stakeholders to identify and document opportunities to streamline onboarding and integration of the next cohort. The result: a set of easy-to-follow procedures that guide analysts and partners through the entire process.

Throughout the pilot, approaches were tested and refined, with an eye to expanding the partnership model to other agencies, as well as service providers, academic institutions, and private-sector organizations.
Information sharing at machine speed

**Pilot results**
Working side by side, the Cal-CSIC, the partner agencies, and Deloitte were able to:

- Effectively onboard the three pilot partners
- Identify and procure the appropriate technologies for a threat intelligence management platform and a cybersecurity event reporting platform to aggregate partners’ security events
- Deploy both platforms within the Cal-CSIC and at each of the partner agencies
- Integrate intelligence sources into the threat management platform from private sector intelligence sources, federal government intelligence sources, and industry threat-sharing entities
- Implement 20 threat detection security use cases in the SIEM technologies used by the partners
- Develop dashboard requirements for analyzing collected data
- Document all the Cal-CSIC processes for partner onboarding to drive efficiency across future partner engagements
- Build a governance model to drive decision making and support faster issue resolution

**The Cal-CSIC’s information sharing process**

The Cal-CSIC’s integration center shares threat intelligence with partner agencies. Agencies automatically send alerts back if requirements are met, enabling the Cal-CSIC to aggregate events, conduct analysis and investigation, and support incident response as needed.
Creating a more secure California
Building on lessons learned from the pilot, which ended in September 2017, the Cal-CSIC’s information sharing program continues to grow—and demonstrate results.

The Cal-CSIC has now grown to a team of 10 strong team members. Three more partner agencies have been onboarded and 10 others are on deck, including a major utility and a bank.

The onboarding time for partner agencies has also been reduced. What took three to four months during the pilot phase is now accomplished in about two months.

And the results? Leadership now receives regular updates on cyber threats facing the State of California. Drill-downs to threats by sector will be coming soon. The Cal-CSIC has also been able to identify many phishing and ransomware attacks against partner agencies and, in some cases, prevent incidents from spreading.

“A lot of factors come into play when dealing with multiple agencies and platforms, and managing expectations on both timelines and results was a big component as well,” Tresh added. “But has this information sharing model helped California improve its cybersecurity? Absolutely.”

“Deloitte worked very closely with us on the conceptual and pilot phases of the project. They were flexible and open, and they were able to quickly pivot and change parameters as needed. They helped us get this pilot up and running—and we’re very pleased with the results.”

—Keith Tresh, commander, California Cybersecurity Integration Center, California Governor’s Office of Emergency Services