Who Let the 'Cyber Dawg' Out?
A Live-Action Cybersecurity Exercise

NASCIO 2020 State IT Recognition Awards

CATEGORY:	Cybersecurity
STATE:	Georgia
CONTACT:	Calvin Rhodes, State CIO (404) 463-2340 calvin.rhodes@gta.ga.gov
PROJECT INITIATION DATE:	February 14, 2019
PROJECT END DATE:	May 3, 2019

EXECUTIVE SUMMARY

In early May 2019, cybersecurity professionals from state agencies and the Georgia National Guard gathered at the Georgia Cyber Center in Augusta. Some were anxious, as they were to be tested. Unaware of the details, the agency security team members were about to stare down a ransomware attack and be judged on how well they could thwart it.

That's the premise of Cyber Dawg, a live-action cybersecurity exercise led by the Georgia Technology Authority (GTA), in coordination with the Georgia National Guard and agency participants. Over an intense three days of the inaugural event, Georgia National Guard security specialists staged mock, though convincing, SamSam ransomware attacks. The exercise happened in the controlled, contained learning environment of the state's cutting-edge Cyber Center. State systems and data weren't, in fact, being threatened. But the tension and the sweat on the brows of agency cyber defenders, that was all real.

Why put the participants through the exercise? There may be no better way to prepare Georgia agencies for actual cyber attacks than to drop them into the line of fire, and let them try out their cyber defense plans. Cyber Dawg, now envisioned as an annual event, provides a safe zone where participants can practice and learn. Then they return to their respective agencies with broader experience, and new cyber defense tools at their disposal.

The exercise format was designed by the Georgia National Guard Cyber Protection Team and incorporated elements of ransomware, replicating actual attacks that took place against the City of Atlanta and Colorado's Department of Transportation. GTA's Office of Information Security hosted the event and provided cybersecurity tools used in the exercise. Participants, including Guardsmen, were divided into eight teams – some attackers, some defenders, others playing the part of intel teams and others maintaining Cyber Dawg's staged IT environment. Then, the battle was on.

Cyber Dawg Bytes:

Even in its first year, Cyber Dawg showed it has teeth and made an impression.

- Agency participants saw firsthand that cyber defense plans and tactics cannot be static. If they're to be effective, plans and tactics must constantly morph to address new attack variables and incorporate newly arising security tools.
- No one's defense was impenetrable. All had to learn to adapt quickly and often. That's where the exercise and the real world of cyber defense merge.
- Agency participants left sobered but energized, committed to holding the line and doing their part to safeguard Georgia's systems and data.

Even though the ransomware attacks were simulated, the stress and beads of sweat on the participants' foreheads were real. The agency cyber defenders were in it to win.

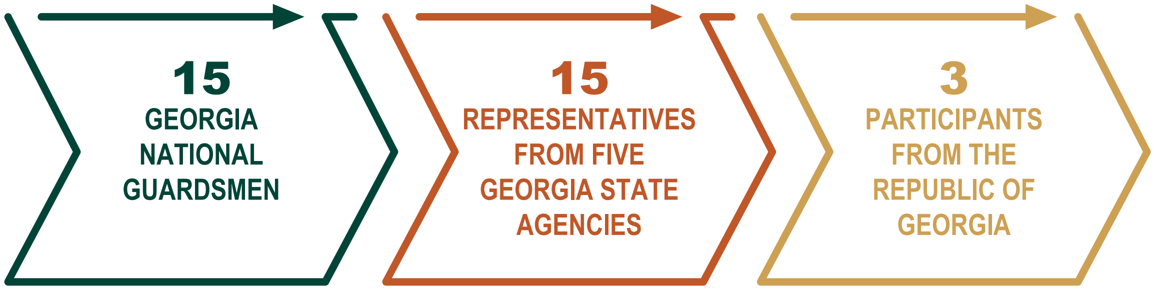
CONCEPT

The Cyber Dawg live-action security exercise was developed to support the overall mission of the Georgia Technology Authority (GTA) Office of Information Security (OIS). That is, “to protect sensitive citizen data and the IT enterprise through a multi-faceted approach.” GTA used its experience with ransomware response across the state, as well as other security work, in shaping the guidance provided to Cyber Dawg participants.

The Cyber Dawg exercise pitted mock attackers against real defenders in a live-action scenario. This exercise gave participating agencies an unparalleled opportunity to put their cybersecurity plans and skills to the test, and to come away better prepared to defend.

The debut exercise in 2019 drew participation from 15 Georgia National Guardsmen, 15 security professionals from five Georgia state agencies, and three from the Republic of Georgia. That’s right, the Republic of Georgia which participated through a special exchange program called the State Partnership Program (SPP), administered by the Georgia National Guard.

EXERCISE PARTICIPANTS



15
GEORGIA NATIONAL GUARDSMEN

15
REPRESENTATIVES FROM FIVE GEORGIA STATE AGENCIES

3
PARTICIPANTS FROM THE REPUBLIC OF GEORGIA

The participants were split into eight teams consisting of two to five members each, as follows:

RED TEAM: Attackers - The red team, comprised of Georgia National Guardsmen, sent the network-level threats (ransomware) that state agency teams then worked to combat. The red team was the simulated hacker.

BLUE TEAM: Defenders - The blue teams (there were several) defended against the mock attacks. They were the agency cybersecurity professionals, there to practice their skills and put their agency defense plans to the test.

WHITE TEAM: Neutral - The white team was more of a behind-the-scenes team. It was comprised of Georgia National Guardsmen and personnel from GTA. They acted as decision makers for the simulation and guided participants through the rules of the exercise.

FUSION CELL: Intel - The fusion cell, also comprised of Georgia National Guardsmen and GTA personnel, gathered information for the mock attack scenario and aided agency teams as needed. When necessary, they would drop into different agency teams and provided guidance as a learning tool.

RANGE ENGINEERING: Chairmen - These Georgia National Guardsmen were the experts on the exercise and the system. This team had authority over the closed network and ensured that tools were working correctly.

CONCEPT *(continued)*

Mock attack scenarios for the participants included Distributed Denial of Service (DDOS), malware identification, Structured Query Language (SQL) injection, Server Message Block (SMB) compromise, and brute-force attacks.

MOCK ATTACK SCENARIOS

DISTRIBUTED DENIAL OF SERVICE (DDOS),

MALWARE IDENTIFICATION

STRUCTURED QUERY LANGUAGE (SQL) INJECTION

SERVER MESSAGE BLOCK (SMB) COMPROMISE

BRUTE-FORCE ATTACKS

The Georgia National Guardsmen were valued partners in designing the idea and simulation for Cyber Dawg. They brought experience from the Army National Guard Annual Cyber Shield drill, the nation's largest cyber defense training exercise.

Georgia's exercise borrowed from Cyber Shield's design, while shifting focus to state-level security concerns. It used the Georgia-based Security Onion, an open-source intrusion protection, enterprise security monitoring, and log management tool. Thanks to the State Partnership Program (SPP), Cyber Dawg had the flexibility to involve the Republic of Georgia, as noted above. The Republic's Ministry of Defense Cybersecurity Bureau participated thanks to the strong relationship the Georgia National Guard has maintained with that nation since 1994.

Cyber Dawg, a train-together, fight-together exercise, capitalized on established military-styled cybersecurity exercises, played out in the safety of a contained environment in Georgia's Cyber Center.

CYBER DAWG

With guidance from the experts, Cyber Dawg participants practiced and refined their cyber attack response, and built a new support network of fellow cybersecurity professionals. That network can be a critical asset for agencies, so they don't have to face daunting security challenges alone.

SIGNIFICANCE

Your files have been encrypted!
01:23:59:45
What Happened to My Computer?
Can I Recover My Files?
How Do I Pay?

Cyber Dawg succeeded in its debut. Georgia created a live-action security exercise focused on state priorities. It helped prepare Georgia agencies, as well as an international participant, to combat ransomware, a persistent threat. And the event fostered stronger working relationships among security professionals in the process.

The exercise benefitted not just participating agencies, but also the Georgia National Guard and host GTA, which extended its engagement with state agencies and introduced them to additional cybersecurity resources and tools.

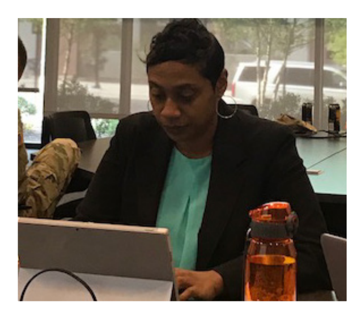
Georgia government is focused on enhancing the technical skills of its information security professionals, and interacting with true "cyber-warriors" is providing a great foundation for that effort.

GTA and the Georgia National Guard didn't just teach at Cyber Dawg. They also learned from participating agencies, and left better integrated into the state government cybersecurity community, bonded by a shared goal of defense.

Event participants left the exercise with an expanded knowledge of cybersecurity tools available to them through the state. They built a repertoire of new defense and training techniques, and they gained insights into how hackers think. They were equipped to take that learning back to their respective entities and share it with colleagues. They can contribute now more capably to the cybersecurity professionals community that is in such demand in Georgia, and beyond.

Plans are to invest in developing cyber scenarios that can be used in subsequent training at the Georgia Cyber Center. As these offerings expand, training cost per participant could shrink, making it even more attractive for agencies.

IMPACT



Cyber Dawg is more than a live-action cyber exercise. It provides a forum for collaboration among security professionals from state agencies, the Georgia National Guard, and even other nations. Its positive impact is broad-ranging.

GEORGIA CYBER CENTER

Cyber Dawg put the new Georgia Cyber Center in the spotlight. The center is a unique resource among Georgia's cybersecurity assets. Since construction in 2018 of this state-of-the-art facility, Georgia has worked to demonstrate its capabilities for hosting events like Cyber Dawg. It provided an ideal setting for the live-action exercise.

It's not over when Cyber Dawg is over. Exercise participants then take all they've experienced back to their respective agencies, and the learning starts again as they share knowledge gained with colleagues.

EXERCISE PARTICIPANTS

Georgia Emergency Management and Homeland Security Agency (GEMA/HS):

Georgia Emergency Management and Homeland Security Agency (GEMA/HS) was able to highlight gaps as well as strengths in their incident response plan and their enterprise security approach, giving agency leaders opportunity to address weaknesses. In the year since GEMA/HS' participation, the agency has already implemented some of the open-source tools used during the exercise, and the agency is now better able to monitor for potential threats within the network before they cause issues.

Georgia Department of Transportation (GDOT):

Georgia Department of Transportation (GDOT) capitalized on the opportunity to build strategic relationships. Making connections with cybersecurity experts from other agencies and the Republic of Georgia allowed GDOT participants to build on their networks.

Georgia Bureau of Investigation (GBI):

GBI's participation allowed it to practice digital forensics and to introduce other participants to specialized investigative techniques GBI uses in combatting actual cyber crimes. GBI operates a Cyber Crime Unit from the Cyber Center, so they were in familiar surroundings.

Cyber Dawg debuted strong and looks likely to grow. Cyber threats won't soon disappear, so cyber defenses have to be invigorated and constantly renewed. The Cyber Dawg exercise gives Georgia another invaluable means of preparation.

THE STATE OF GEORGIA

Cyber Dawg organizers envision expanding the circle of participants to include local government security teams. All across Georgia, they're facing damaging cyber attacks comparable to what state agencies see. And those local governments are often sorely in need of the cyber defense resources and training the Cyber Dawg exercise can deliver. State IT security leaders are working to ensure local governments aren't left to go it alone.

Cyber Dawg puts participants through their paces. It makes 'em sweat by practicing cyber defense in a live-action setting. It brings security professionals together to learn from each other. And it acquaints participants with cybersecurity tools and resources available to them through GTA and the state of Georgia. It's a multi-dimensional addition to the state's investment in bolstering the cybersecurity community and safeguarding government systems and data. The 'Cyber Dawg' is off and running.