CASE STUDY

SHADOWHQ

US-Based Bank Reinforces Incident Response with Secure Out-of-Band Coordination and Communication Capabilities

ShadowHQ additionally streamlines and strengthens incident preparedness with tasking and timeline metrics

Customer

ShadowHQ's customer is an established, century old bank serving more than 20,000 customers across the Midwest United States. The bank has more than 700 employees across 38 branch locations and specializes in commercial accounts. The company's Chief Security Officer's (CSO) responsibilities go beyond cybersecurity to include legal, physical security and fraud departmental oversight. The bank's cybersecurity team consists of seven full-time staff and several external partners that support security operations (SOC) and forensics initiatives.

As a financial institution, the bank is governed by the Office of the Comptroller of the Currency (OCC) and Federal Financials Institutions Examination Council (FFIEC). The bank has a robust incident response plan in place and approximately 30 stakeholders on the incident response team, which includes internal staff, external partners and law enforcement contacts.

INDUSTRY

Finance - Banking

HEADQUARTERS

United States

COMPANY SIZE

- 700+ employees
- $179M+ in annual revenue
- 38 branch locations
- 20,000+ customers

In the event of a cyber incident, if the adversary is on your network, you can't trust it.

Challenge

The CSO joined the bank two years ago. Prior to his arrival, the company conducted tabletop exercises through external partners. The exercises were scheduled by convenience and conducted in a company conference room. The process was standard and involved the company's incident response team and other key stakeholders. As a former military officer, the CSO was familiar with recall rosters, phone trees and having primary, secondary and tertiary communication plans in place. Upon joining the bank, the CSO realized that these components weren't included in the company's tabletop exercises and incident response planning.

> "In the military, our communications planning accounted for unpredictable situations where standard communications channels wouldn't or couldn't apply," said the CSO.

> "When I joined the bank, the approach to tabletops was very much convenience based, and managed around staff schedules and the standard tools the bank had in place like phone bridges and Microsoft Teams. But that's not the real world. If we're all working remotely, if there's a snowstorm or if something happens the middle of the night, the plan wouldn't cut it."

The CSO notes concern that the corporate tools were tied to the company's network saying: "In the event of a cyber incident, if the adversary is on your network, you can't trust it."

Other tools the bank used including AlertMedia (for emergency communications) are tied to the company's active directory. "Every platform I looked at was the same thing," said the CSO. "In order to ensure network separation, I would have to stand up my own Amazon cloud instance to support it."

Solution

The CSO discovered ShadowHQ as a tool that operates securely outside the network. “We wanted a completely separate platform that wasn’t associated with our authentication and log on services and processes. In a cyber-related situation, when investigators or analysts start logging on to systems to investigate or monitor a situation, they can inadvertently tip their hat to the adversary, and point them to what’s going on.”

The CSO routinely appreciates the platform’s ability to facilitate discreet investigations. “A significant number of the incidents we investigate are benign,” said the CSO. “Having the ability to declare an internal investigation inside the platform helps us investigate an event without impacting our authentication or ticketing systems, and without giving the event more visibility than it warrants.”

The platform has replaced the bank’s previous tabletop exercises, which are now run in-house. Additionally, the CSO has migrated siloed and separate planning tools and documents to the platform, which now serves at the bank’s ‘single source of truth’ for response and event handling.

ShadowHQ captures data throughout the response process, so we now have concrete performance metrics.

> “The platform’s tasking and check-in capabilities allow me to control and monitor which stakeholders get involved in the process, when it’s appropriate to do so,” said the CSO. “For example, our CEO doesn’t have to get involved when an event is declared, rather they get the details they need when they need to act. The platform’s check-in feature allows me to see exactly when the CEO or other stakeholders have joined and are aware of the situation.”

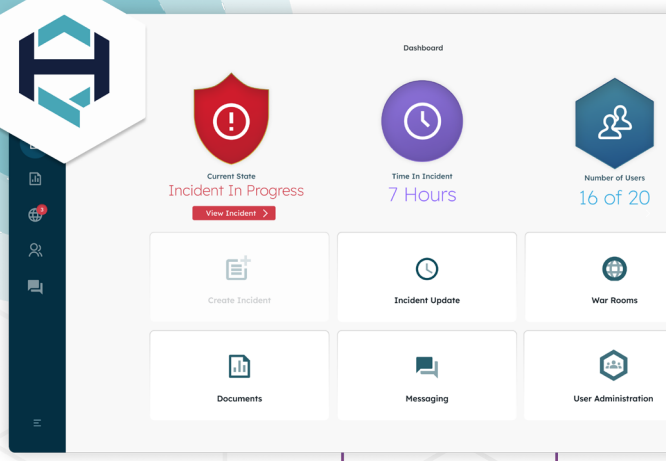
The platform’s timeline capabilities have helped the CSO better understand response and stakeholder processes, which have helped him finetune tasking saying: “After every tabletop we’ll look at the timeline to note which team member was assigned a task and at what point in the response process the task was performed. ShadowHQ captures data throughout the response process, so we now have concrete performance metrics. It’s been a gamechanger in terms of understanding response times.”

Results

The CSO updates the bank's incident response plan monthly and notes that "just having a secure cloud platform where these documents are stored, and having the ability to communicate securely with bank employees is critical."

For the CSO and his team, ShadowHQ has become the bank's primary response and communication tool. "Knowing that I have a platform to immediately alert, involve and triage an incident is the equivalent to having the bat signal," said the CSO. "Having that capability — as a CSO I can't put a price tag on that."

The CSO highlights the number of new features incorporated throughout his time using ShadowHQ saying: "**I don't know any other vendor that does what ShadowHQ offers.** This is also one of the few vendors I've worked with who actually asks me what they can do to make the product better, and then almost immediately implements that feedback. It's a sense of partnership — it's pretty awesome, and the platform just keeps getting better."



> **"Knowing I have a platform to immediately alert, involve and triage an incident is the equivalent to having the bat signal. Having that capability — as a CSO I can't put a price tag on that."**

SHADOWHQ

ShadowHQ is a secure, out-of-band platform that helps CISOs and disaster recovery teams achieve incident preparedness. **Learn more at www.shadowhq.io.**

Schedule a demo at **shadowhq.io/book-a-demo/**