Blue Team Testing

offerings.**infotex**.com

The Next Generation of Incident Response Testing is here!

Staying in front of the bad actors.

We here at infotex have long made the case that if you were only allowed one single test throughout the year that the Incident Response Test would be that "One Test." When we exercise our Incident Response Team, we educate, motivate, and activate our entire institution, from teller to the Board. By walking through technical and non-technical scenarios, we gain confidence on how to handle tough decisions, like when to notify customers. This is accomplished by regular testing and pinpointing areas of improvement. By adding Grey Box and Blue Team procedure exercises to the process, we are substantially improving our already stellar process.

What our Clients are saying:

Our new approach to Incident Response Testing has already proven its worth. Generally, the inclusion of the Blue Team demonstration, using the MITRE framework, helps your technical team exercise detection, containment, and escalation against controls we confirm are working, before we bypass them. Whatever keeps you up at night, we can test it! We have already had great success with this new exercise with some Clients that were excited to see the Next Generation of Incident Response Testing in action. Here are their testimonials!

"We engaged infotex to perform a Blue Team Exercise to see if the security posture we think is in place truly is. The test started out using a normal user account and PC setup then incrementally removed security layers to see at each point what our exposure was until ultimately giving full admin rights. The exercise was enlightening and while we had a few small takeaways overall it confirmed our security performed as we intended. It was a good exercise and plan on performing yearly as just another check to confirm we are doing what we can to keep our customers information safe."

Gregg Feigh, First Internet Bank

"We went through a Blue Team Exercise as part of a facilitated incident response test with infotex. We were very happy with the results, as we learned new things about our network and what would happen if key controls failed. Our technical team practiced detecting, containing, and escalating incidents in a safe manner. That the controls we bypassed were confirmed prior really helped. As a community bank, we value our audit relationship, but it does not allow us to test the parts of our system that we are truly concerned about, or to see what happens when a control breaks. The blue team demonstration did that."

Brett Gallion, Commercial and Savings Bank

Blue Team Testing

offerings.**infotex**.com

What makes Blue Team Testing different?

Most banks are exercising their Incident Response Team, from escalation of a potential incident through the board reporting process. But what about the Blue Team? What about the detection, containment, and escalation processes? That's where Blue Team Testing comes in because it establishes:

- The functional testing of the detection, containment, and triage process of an incident.
- The expected function of controls, we will be able to see where these controls are broken if they are.
- That proper and timely escalation processes are followed. Improper and untimely escalation can increase the impact and severity of an incident as the time a bad actor has in your system the more damage they can do.
- The implementation of technical jargon, acronyms, and inclusion of technical team members that will be involved.
- The Board's Response to an incident, current practices allow the Client to present the post-test review to their board.

What the Blue Team Testing flow looks like:

- Kickoff Meeting
- Playbook, etc. Walkthrough
- Test Plan Presentation
- Test Plan Approval
- Functional Test Period
- Grey Box Interview

- Demonstration
  - Detection
  - Containment
- Escalation Tabletop Test
  - Escalation
  - Custom comprehension exercises
- Technical Exercise Post-Mortem Review
- Backdoors & Breaches on night of exercise

- Day after Technical Exercise
- Plan Walkthrough
- Tabletop Test Plan Presentation
- Tabletop Test Plan Approval
- Exercise bringing the team up to speed on what happened (Escalation)
- Tabletop Test
  - Ideally continues at least the Technical Test Scenario

- Will have its own Technical Exercise section.
- Will be reviewed with Incident Response Team, modified as an internal document, and used in the board exercise.
- Documents all controls bypassed in the exercise.

- Appropriate Meeting
- Review board role in incident response.
- Teach board how to determine appropriate questions.
- Custom Comprehension Exercise
- Facilitate Management's presentation of the Post-Mortem Review.
- Kept to 35 minutes.

If you are interested in our Blue Team Testing, SIEM, or any other services, please visit:

offerings.infotex.com