TABLETOP EXERCISE (TTX): CYBERSECURITY THREAT SIMULATION

How prepared is your organization for a cybersecurity attack, like ransomware?

UltraViolet will provide transparency into your organization's cybersecurity readiness through controlled exercises with our knowledgeable and adaptable security professionals. The UltraViolet approach is tailored per the client's top goals for the tabletop exercise (TTX). Frequently clients request the following to be included within the scope of the TTX:

REVIEW OF POLICIES, PROCEDURES, AND OTHER DOCUMENTATION

Often, clients will provide IT policies, Incident Response (IR) plans, Crisis Communications Procedures, Network Layouts with cybersecurity countermeasures and/or other relevant Standard Operation Procedures (SOPs)

INTERACTIVE WORKSHOP: SCENARIO GAMEPLAY WITH INJECTS

Evaluate and investigate your organization's crisis management capabilities in the event of a modern threat, including: when to engage with ransomware demands, breach disclosure processes and requirements, media communication best practices, and impact of containment tactics on availability.

ANNUAL COMPLIANCE FOCUSED ASSESSMENT

Identifying risk requires more than just a simple scan of your IT environment. To truly protect your environment, you need to test using advanced adversary TTPs. UltraViolet experts are focused on uncovering vulnerabilities and exploiting them in targeted information systems, networks, IoT, cloud (AWS/GCP/Azure/etc) and/or applications (web, mobile, etc.) within a set time domain to provide the highest ROI.

INNOVATION & EDUCATION

VISIBILITY

Discover gaps in processes, between what you expect to occur and what the documented response should be.

EVALUATION

Optimize Return on Investment (ROI) via these quick turnaround, non-invasive assessment

RECOMMENDATIONS

Uncover meaningful ways to improve your organizations response by strategically closing the gaps in processes.