Cybersecurity Incident Response Capability Level Evaluation

CIRCLE

How capable is your organization at effectively responding to cyber incidents?

Through Dean Dorton's **Cybersecurity Incident Response Capability Level Evaluation (CIRCLE)**, we evaluate the capability of your technical team to effectively identify, investigate, contain, and recover from active cyber threats, and we evaluate your executive team to properly handle the compliance, communications, and fallout of a successful attack.

STEP 1 TECHNICAL RESPONSE

We'll work with your technical team to introduce the scenario through a mixture of tabletop scenarios and real-world alerts and artifacts planted on your production network. This incorporation of **digital breadcrumbs** helps provide a thorough evaluation of your technical team's capabilities to provide timely and accurate data to your executive team.

STEP 2 EXECUTIVE RESPONSE

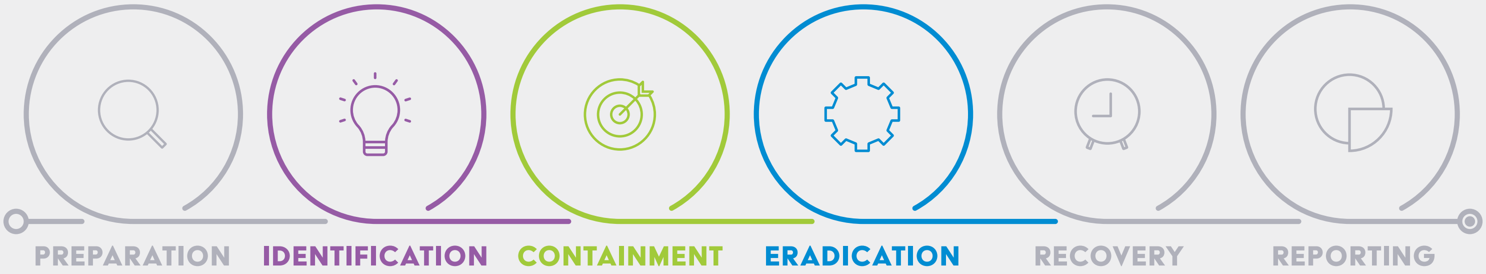
We'll then evaluate how your executive team responds to the cyber threat. Information provided to the executive team will come either directly from the technical team's observations and notes, or through injections (also known as wrenches) thrown into the scenario.

STEP 3 RESULTS & REPORTING

Lastly, we'll provide an on-site exit brief with initial observations and feedback to address any critical coverage gaps or concerns. We'll also provide a full report that includes strategic and technical observations, as well as a high-level project plan to move forward with any recommended improvements.

DIGITAL BREADCRUMBS

We'll plant digital breadcrumbs during the CIRCLE evaluation, making the simulation realistic by leveraging your production security controls to raise alarms and alert the technical team that something is wrong. Digital breadcrumbs vary based on the scenario employed; they are used as a metric to evaluate the capability of your technical team to identify, contain, and eradicate threats.



PREPARATION IDENTIFICATION CONTAINMENT ERADICATION RECOVERY REPORTING

Command and Control
Traffic simulators are used to emulate common C2 protocols and general intrusion detection alarms

Propagation
Benign "malware" samples are dropped on identified hosts through common lateral movement techniques

Artifacts
Persistence mechanisms used by threat actors and common malware are planted on the "infected" hosts

DEANDORTON
TECHNOLOGY

Lexington ▪ Louisville ▪ Raleigh ▪ **deandorton**tech.com