CALIAN
Confidence. Engineered.

Purple Team Exercise

Purple Team Exercises involve the Blue Team being exposed to attack activity as it occurs and explaining it to them.

Multiple teams come together to work on

Cyber Threat Intelligence

Emulating Adversaries

Managed Security Services

TESTING CASES

Execute local endpoint security checks on a client's laptop

Use the VPN to connect to the client's Internal Network to attempt lateral propagation

Execute local endpoint security checks on the client Internal Server

Openly discussing attack techniques and defense expectations leads to improving people, processes, and technology in real-time

Step 01 Cyber Threat Intelligence is conducted under the Exercise Coordinator. The Red Team presents the adversary, tactics, techniques, and procedures (TTP), and technical details based on the outcome.

Step 02 The participants discuss security controls and expectations for TTP during a kickoff meeting.

Step 03 The Red Team emulates the bad guys by launching multi-layered attacks involving several aspects and exploiting privileged access penetration testing simultaneously.

Step 04 Analysts on the Blue Team (SOC, Hunt team, and Digital Forensics and Incident Response) are trained in the process of detecting and responding to TTP acts.

Step 05 In the event that TTP has been identified, a log has been received, or any forensic evidence has been obtained, results are documented and shared.

Step 06 Ensure security controls are adjusted or tuned in order to increase visibility and repeat the TTP.