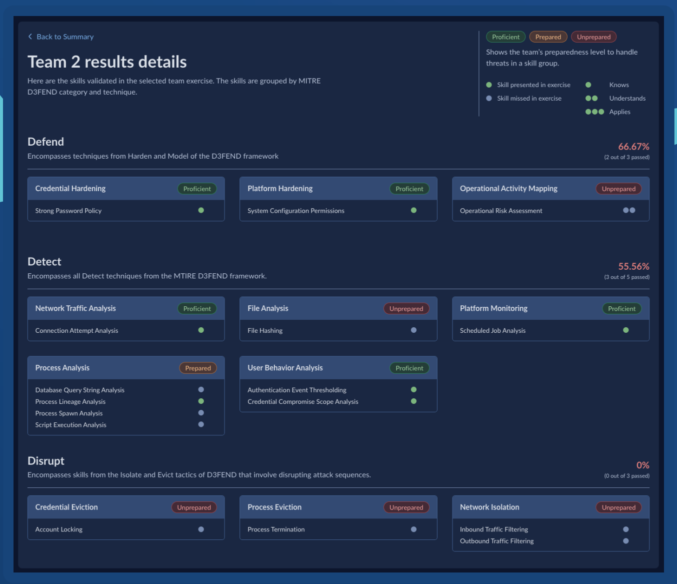
RANGEFORCE

Team Exercises

Validate and optimize your team's security operations against real threats.



‹ Back to Summary

Team 2 results details

Here are the skills validated in the selected team exercise. The skills are grouped by MITRE D3FEND category and technique.

Proficient | Prepared | Unprepared

Shows the team's preparedness level to handle threats in a skill group.

● Skill presented in exercise
○ Skill missed in exercise

● Knows
●● Understands
●●● Applies

Defend

Encompasses techniques from Harden and Model of the D3FEND framework

66.67%
(2 out of 3 passed)

Credential Hardening — Proficient	Platform Hardening — Proficient	Operational Activity Mapping — Unprepared
Strong Password Policy ●	System Configuration Permissions ●	Operational Risk Assessment ○○

Detect

Encompasses all Detect techniques from the MTIRE D3FEND framework.

55.56%
(3 out of 5 passed)

Network Traffic Analysis — Proficient	File Analysis — Unprepared	Platform Monitoring — Proficient
Connection Attempt Analysis ●	File Hashing ○	Scheduled Job Analysis ●

Process Analysis — Prepared	User Behavior Analysis — Proficient
Database Query String Analysis ○ Process Lineage Analysis ● Process Spawn Analysis ○ Script Execution Analysis ○	Authentication Event Thresholding ● Credential Compromise Scope Analysis ●

Disrupt

Encompasses skills from the Isolate and Evict tactics of D3FEND that involve disrupting attack sequences.

0%
(0 out of 3 passed)

Credential Eviction — Unprepared	Process Eviction — Unprepared	Network Isolation — Unprepared
Account Locking ○	Process Termination ○	Inbound Traffic Filtering ○ Outbound Traffic Filtering ○

Featured Scenario: Phoenix

1. Adversary delivers a spear phishing attack. Infects a workstation with a malware backdoor
2. Malware executes, takes over workstation and calls back to C2
3. Adversary takes control of machine to try & escalate privileges
4. Adversary dumps local credentials and begins lateral movement
5. Credentials are used to access file shares & databases – files are then moved for exfiltration

1. Sensors and logs capture IOCs. Blue Team SIEM operator receives first set of alerts
2. Alerts are sent out; response playbooks begin executing
3. Blue Team must find and correlate multiple IOCs to recognize exfiltration events, identify C2 attack vector
4. Blue team defeats attack by deploying firewall rule changes, identifying, and isolating the infected machine

Post Exercise After-Action Report

After-Action Reports are an exercise tell-all and are hosted by RangeForce engineers. Review your team's successes, areas of improvement, and the technical breakdown of the exercise (filenames, users and systems compromised, etc.).

Understanding the Threat Story

Threat actor motivation & context

Identifying the Threat

IoiCs, technical details, queries, etc.

Threat Remediation

Review Tactics for containing and remediating the threat and associated attack vectors

sales@rangeforce.com www.rangeforce.com (877) 716 - 4342