GOLFING WITH DRAGONS

BUILDING SECURE ENVIRONMENTS FOR CTF COMPETITIONS

JARED STROUD
DANIEL ZAIFRAN

THE EXERCISE:
- Need a network
- Network and software have flaws and vulnerabilities
- Teams exploit them

AUTHORIZATION FOR PARTICIPANT LOGIN WAS DONE BY GITHUB ACCOUNTS AND SSO

CHALLENGES:
- Who is responsible for which network features
- ID communications platforms for incidents
- A plan for failure

CAPTURE THE FLAG EVENTS
TEACH PARTICIPANTS ABOUT INFORMATION SECURITY - I PROTECT MY INFRASTRUCTURE AND HACK YOURS

GHIDRA GOLF: A JEOPARDY-STYLE CTF

THUNK!
PYTHON OR JAVA SCRIPTS CAN EXPLOIT VULNERABILITIES IN INFRASTRUCTURE

CONTAINER SCANNING

OWASP TRIVY TOOLS

DAST
SAST
Analysis to scan code
Container scanning
Firewall & host scanning looking for malware

SAST RULES
PATTERNS THAT HELP IDENTIFY TARGETED ATTACKS

YARA /
RULES

/* YARA */