VIRGINIA
IT AGENCY

WELCOME TO THE NOV. 2, 2022

ISOAG MEETING

VIRGINIA IT AGENCY

AGENDA	
Welcome	Ed Miller/VITA
Cloud Based Resources for Cybersecurity Education	David Raymond/Cyberrange
Understanding Today's Modern Attack and the Power of a Platform to Empower Zero Trust.	Patrick Doherty & Tracey Norris/CrowdStrike
	Grayson Walters/SAIC
Upcoming Events	Ed Miller/VITA

Cloud-based Resources for Cybersecurity Education

David Raymond, Ph.D.
Director, Virginia Cyber Range
raymondd@vt.edu

Cloud-based Resources for Cybersecurity Education

David Raymond, Ph.D.
Director, Virginia Cyber Range
raymondd@vt.edu

Cloud-based Resources for Cybersecurity Education

David Raymond, Ph.D.
Director, Virginia Cyber Range
raymondd@vt.edu

Cybersecurity Talent Shortfalls

CyberSeek™

National level

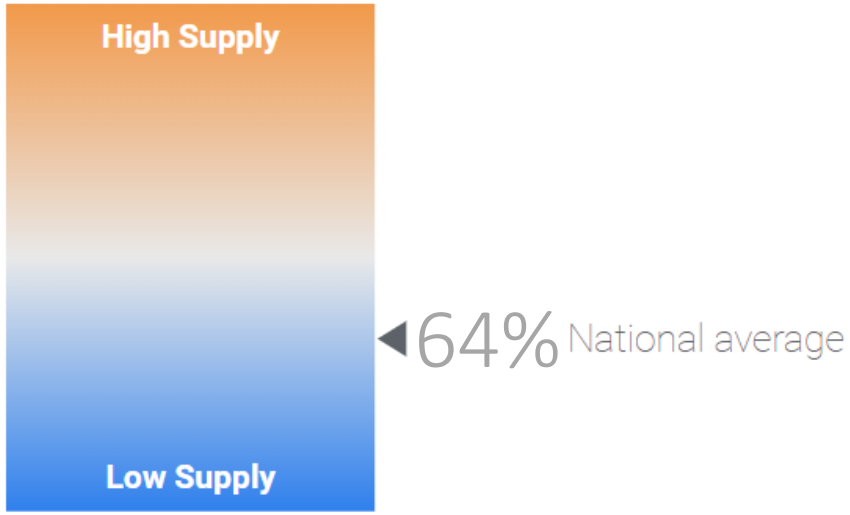
TOTAL CYBERSECURITY JOB OPENINGS

597,767

TOTAL EMPLOYED CYBERSECURITY WORKFORCE

1,053,468

SUPPLY/DEMAND RATIO



https://www.cyberseek.org/

Cybersecurity Talent Shortfalls

CyberSeek™

Virginia

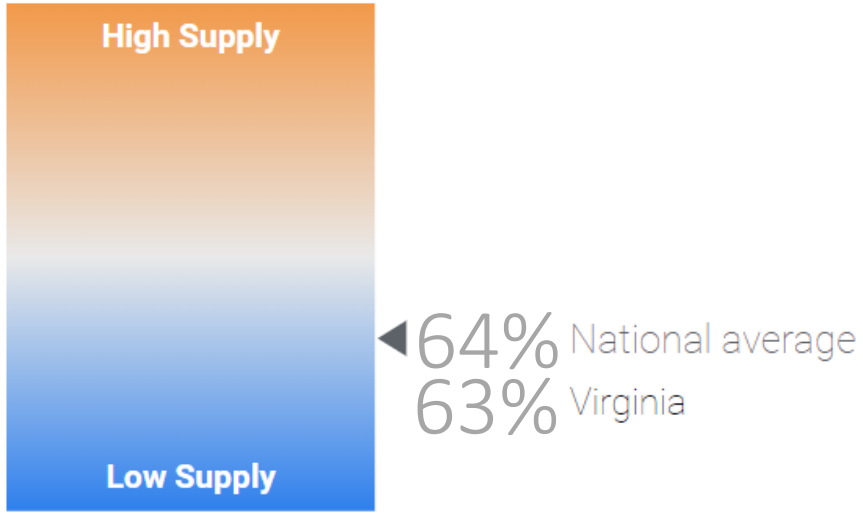
TOTAL CYBERSECURITY JOB OPENINGS

53,767

TOTAL EMPLOYED CYBERSECURITY WORKFORCE

93,225

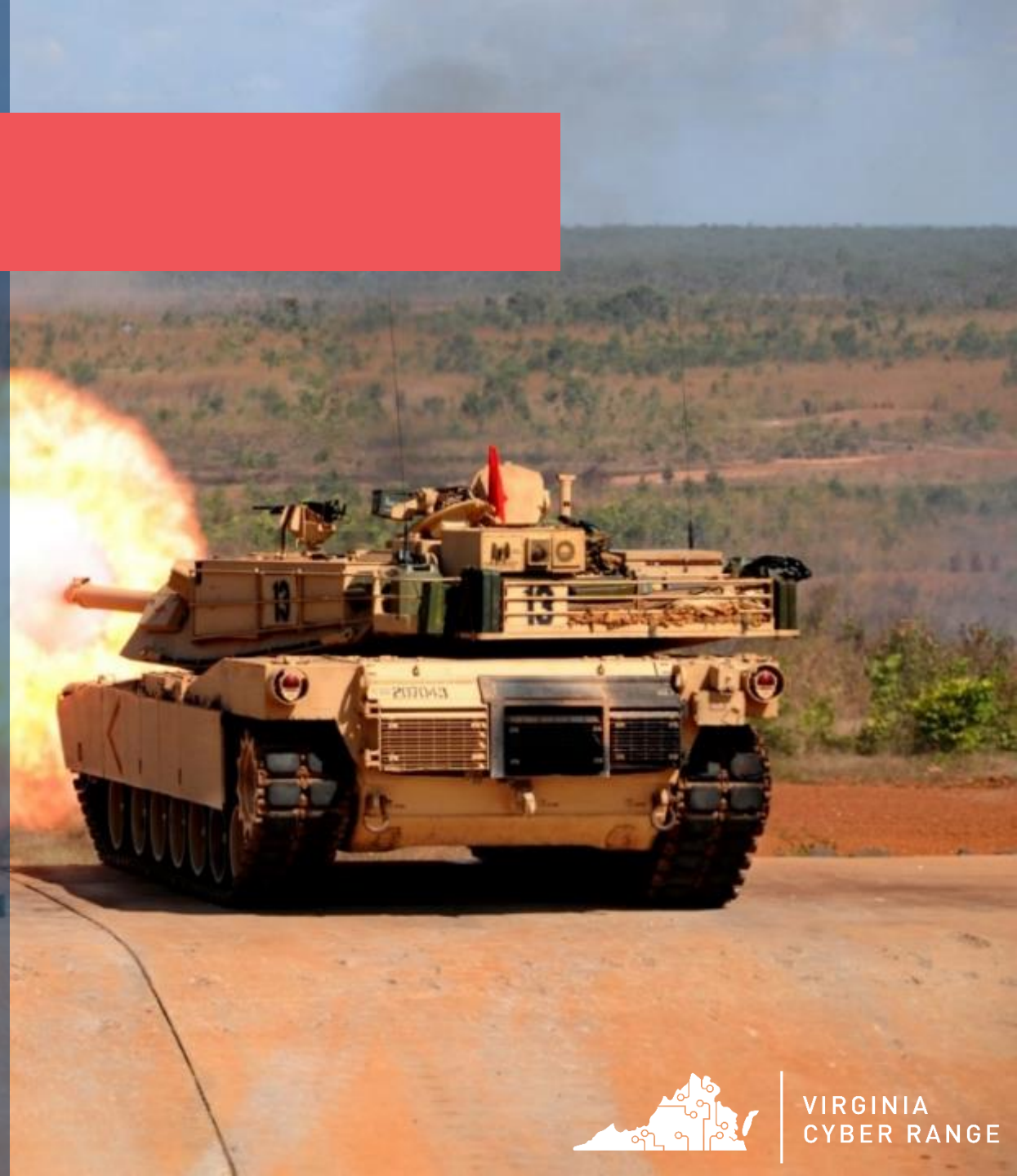
SUPPLY/DEMAND RATIO



https://www.cyberseek.org/

What is a *Cyber Range*?

- ❑ Isolated network
  - Activity will appear malicious
  - Actual malware sometimes used
- ❑ Usually virtualized
  - Allows for maximum configurability
- ❑ Used for:
  - Hands-on cybersecurity training
    - Defensive AND offensive
    - Classroom exercises
  - Games and competitions
    - Capture-the-flag



VIRGINIA
CYBER RANGE

Virginia Cyber Range: Background

- Recommended by the Virginia Cyber Security Commission in August 2015
- Funded by Commonwealth of Virginia starting on July 1st, 2016
- ***The only state-wide effort of its kind***

2016 Executive Budget Document, Item 224, Paragraph J:

*"Out of this appropriation, [funding is] designated to support a **cyber range platform** to be used for cyber security training by **students in Virginia's public high schools, community colleges, and four-year institutions**. **Virginia Tech shall form a consortium** among participating institutions, and shall serve as the coordinating entity for use of the platform. The consortium should initially include **all Virginia public institutions with a certification of academic excellence** from the federal government."*

VIRGINIA CYBER RANGE

Governance:
Executive Committee

- Danville Community College
- George Mason University
- Germanna Community College
- James Madison University
- Longwood University
- Lord Fairfax Community College
- New River Community College
- Norfolk State University
- Northern Virginia Community College
- Old Dominion University
- Radford University
- Southwest Virginia Community College
- Thomas Nelson Community College
- Tidewater Community College
- University of Virginia
- Virginia Commonwealth University
- Virginia Tech
- Virginia Western Community College

VIRGINIA
CYBER RANGE

Courseware Repository

- ❑ Courses, modules, and exercises for use in HS, CC, and university cybersecurity curricula
  - Instructors/professors can select course content in full or *a la carte*
- ❑ Grants offered for courseware development

Exercise Area

- ❑ Menu of per-student exercise environments for use in cybersecurity courses
- ❑ Capture-the-Flag infrastructure for cybersecurity competitions
- ❑ Developing team-based offensive and defensive, scenario-based environments

Community of Purpose

- ❑ Consortium governance
- ❑ Convene workshops and conferences to “teach the teachers” and share best practices
- ❑ Helping to expand NSA/DHS CAE certification among Virginia colleges and universities

Leveraging the Public Cloud

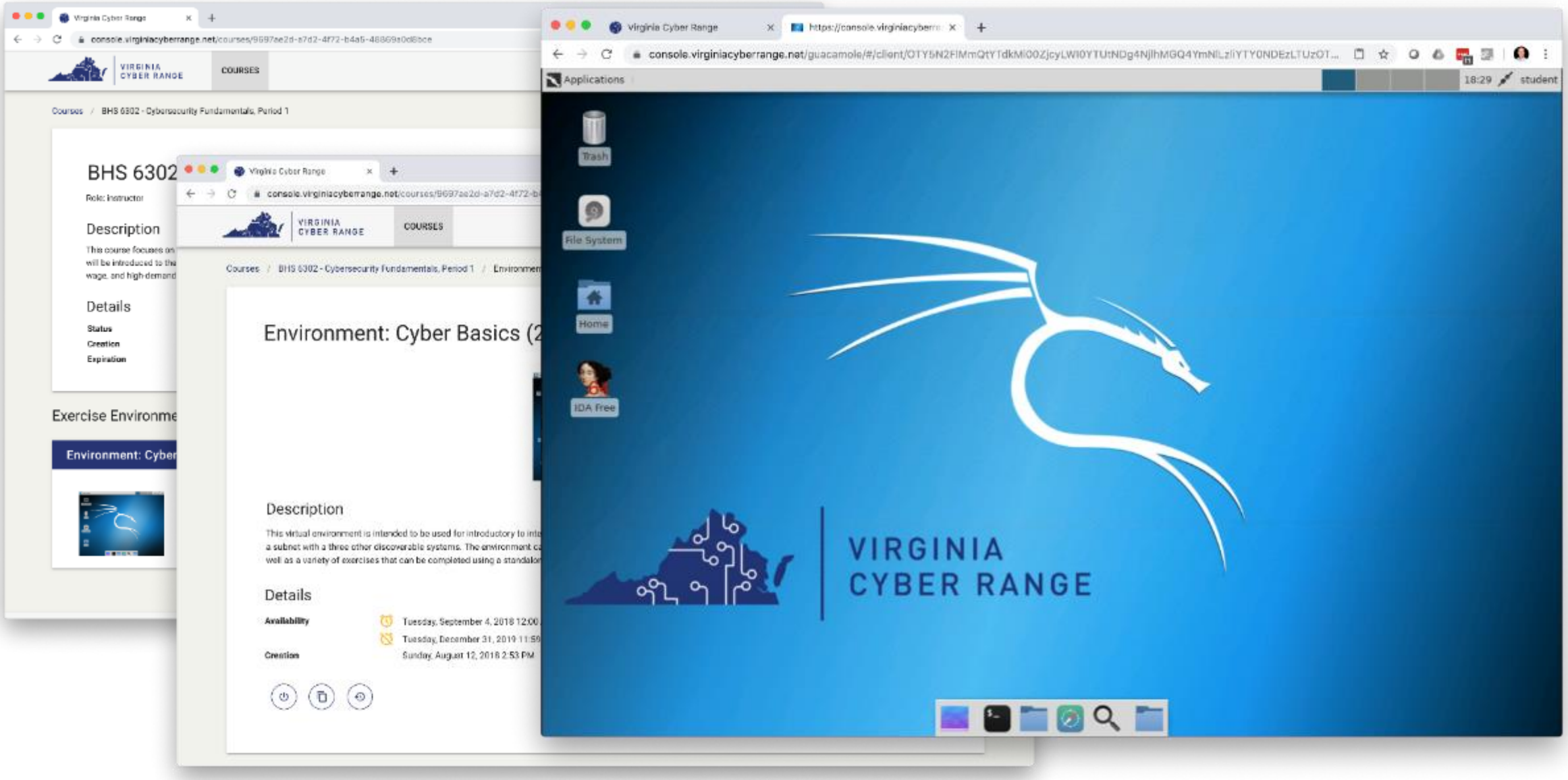
Design Requirements:

- ❑ Scale to support thousands of students
- ❑ Up and running quickly
- ❑ Completely automatable
- ❑ Cost effective
- ❑ Short-term surge capacity
- ❑ Available state-wide (or anywhere?)
- ❑ Web portal for access to content
  - Role-based access
  - Login to see user-specific content
  - Students just need a web browser and internet connection!

Why the Cloud?

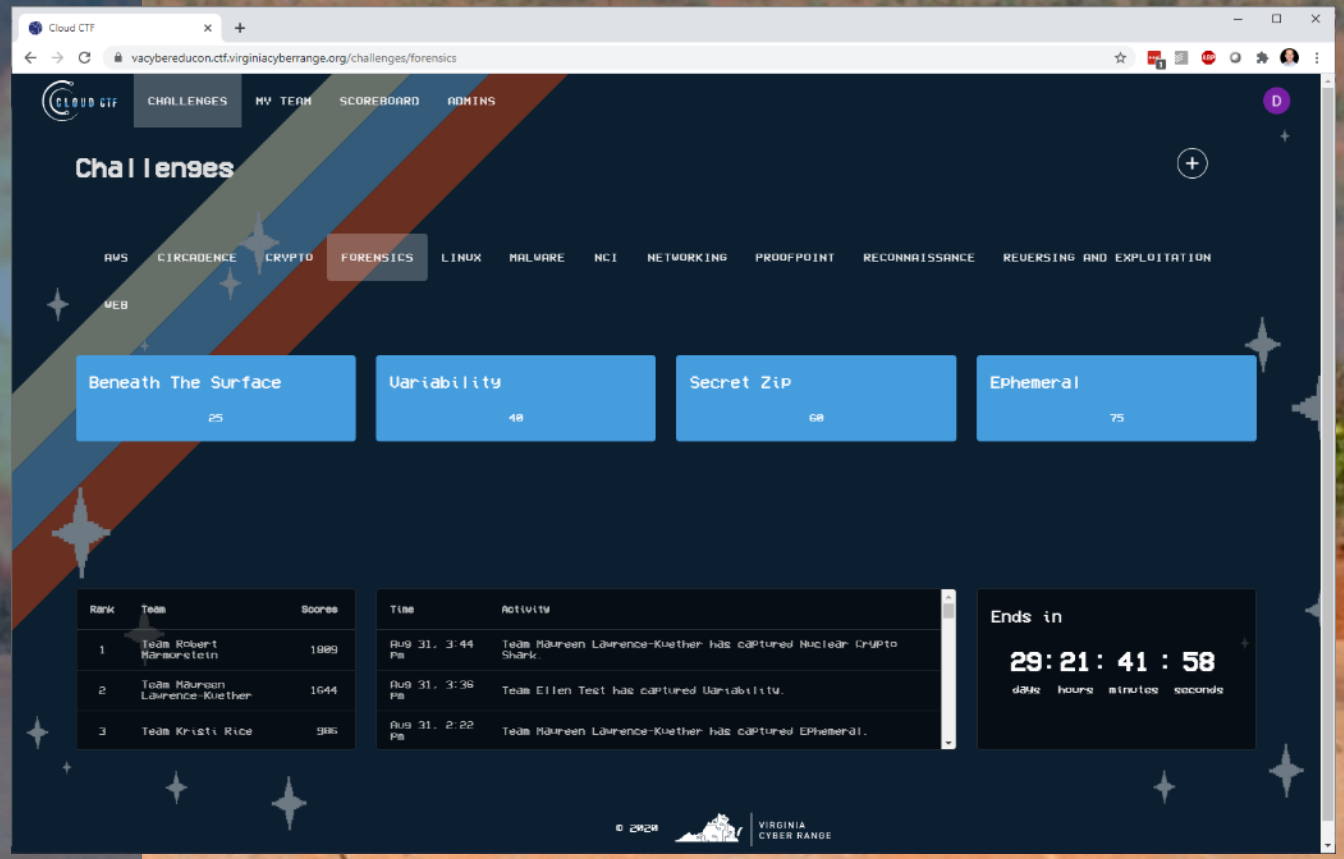
- *Unlimited scalability!*
- Quick start-up phase
- Low capital investment
- Rapid scalability
- Surge capacity
- Location independent
- Highly automated
- Available anywhere

VIRGINIA
CYBER RANGE


VIRGINIA CYBER RANGE
COURSES
BHS 6302
Description
Details
Environment: Cyber Basics
Applications
Trash
File System
Home
IDA Free
VIRGINIA
CYBER RANGE

Capture the Flag

- CloudCTF platform deployed in Summer 2020
- Players solve “challenges” in various categories
  - Networking
  - Cryptography
  - Web
  - Reverse Engineering
  - Reconnaissance.
- Used for:
  - In-class gamification and topic reinforcement
  - Cybersecurity clubs and teams
  - Conferences and other outreach



VIRGINIA CYBER RANGE

Commonwealth Cyber Fusion CTF

George Mason University CTF team hoisting the Virginia Cyber Cup

University tier

1. George Mason University
2. Liberty University
3. University of Virginia

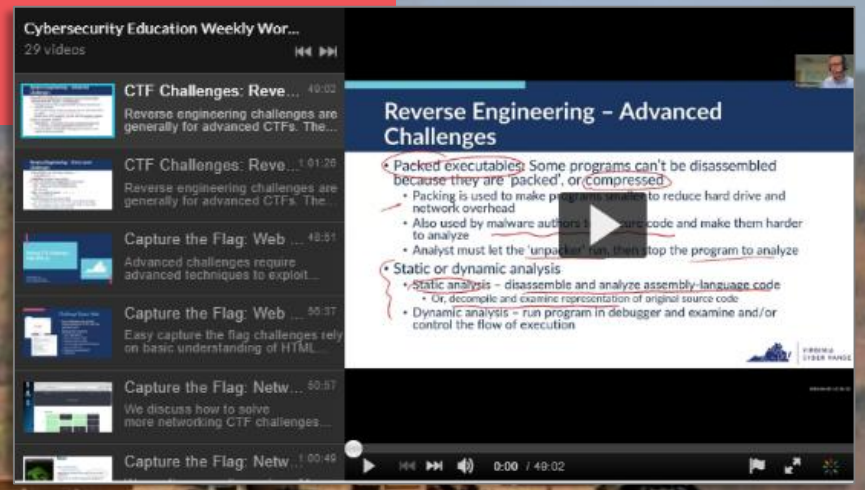
Community College Tier

1. Lord Fairfax CC
2. Danville CC
3. Northern Virginia CC

VIRGINIA CYBER RANGE

Outreach

Teacher Camps and Live Conference Workshops



Online "Weekly Workshops" (Recorded)

Video Series

VIRGINIA CYBER RANGE

VIRGINIA CYBER RANGE

Virginia Cybersecurity Education Conference

2018

James Madison University

2019

George Mason University

2020

Virtual

2021

Virtual

2022

Old Dominion University

July 20-21

SyCom Connected.

NCI OPPORTUNITY. GROWTH. SUCCESS.

aws

GEORGE MASON UNIVERSITY | Volgenau School of Engineering

VIRGINIA TECH

ISACA Virginia Chapter

proofpoint.

ABS TECHNOLOGY

LFCC Lord Fairfax Community College

SANS

IEEE

Virginia Cyber Range By the Numbers*

Total User Accounts

30,683

Current Semester Enrollments

9,985

Students: 9,537
Instructors: 400
TAs: 48

Active Courses Mar 2022

395

Current VMs Deployed

20,304

Lifetime
VMs Deployed:
202,888

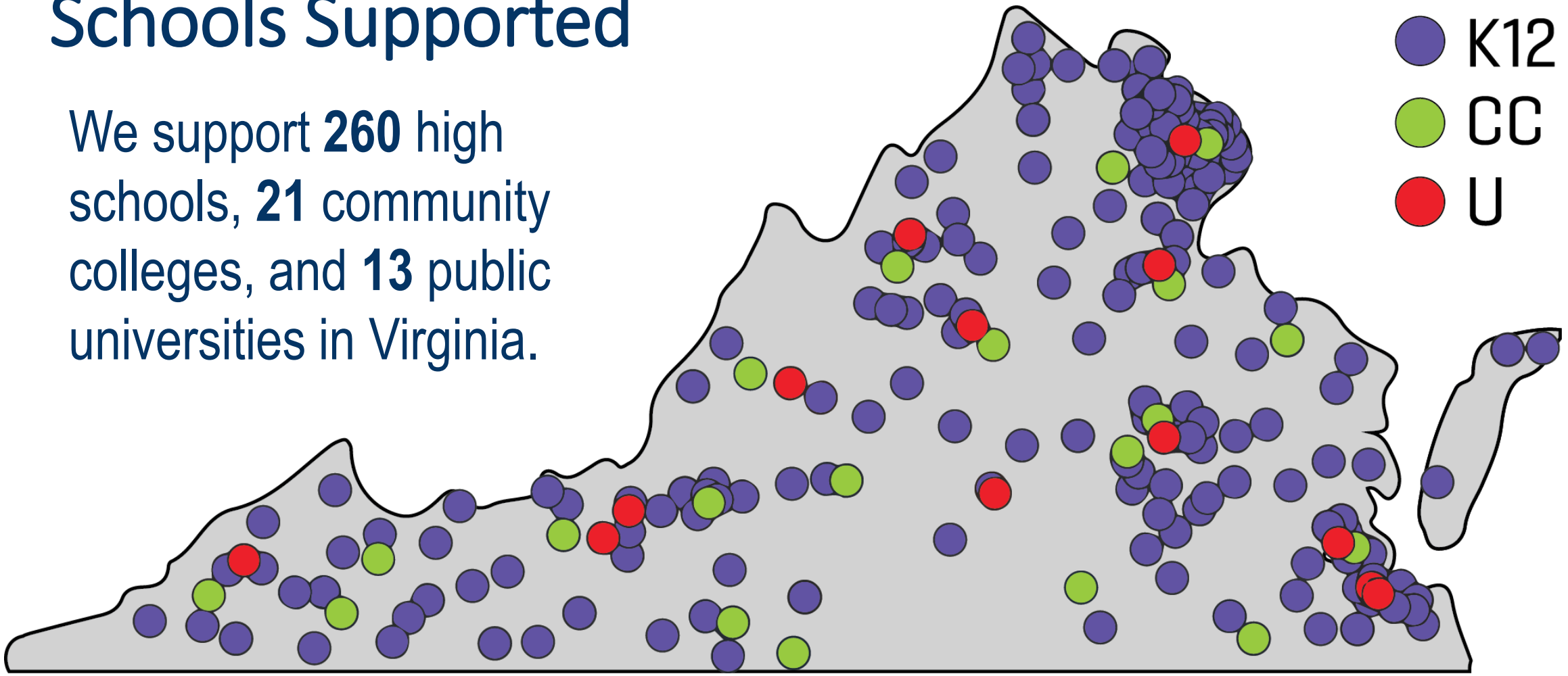
Repository Files Downloaded AY2021

20,367

* As of 5/3/2022

Schools Supported

We support **260** high schools, **21** community colleges, and **13** public universities in Virginia.



* Each dot represents a different Virginia high school, community college, or university.

US Cyber Range

- National outreach
  - Provides Cyber Range as a Service outside of Virginia
  - Charges to cover operating costs
- Established in July 2019
  - Almost 200 customers in 47 states
- Working with National courseware partners

CYBER.ORG

TEACH CYBER

VIRGINIA CYBER RANGE

USCR By the Numbers*

Total User Accounts

7,395

Current Semester Enrollments

2,654

Students: 2,472
Instructors: 174
TAs: 8

Active Courses
April 2022

176

Current VMs Deployed

6,475

Lifetime
VMs Deployed:
23,748

Repository Files Downloaded
AY2021

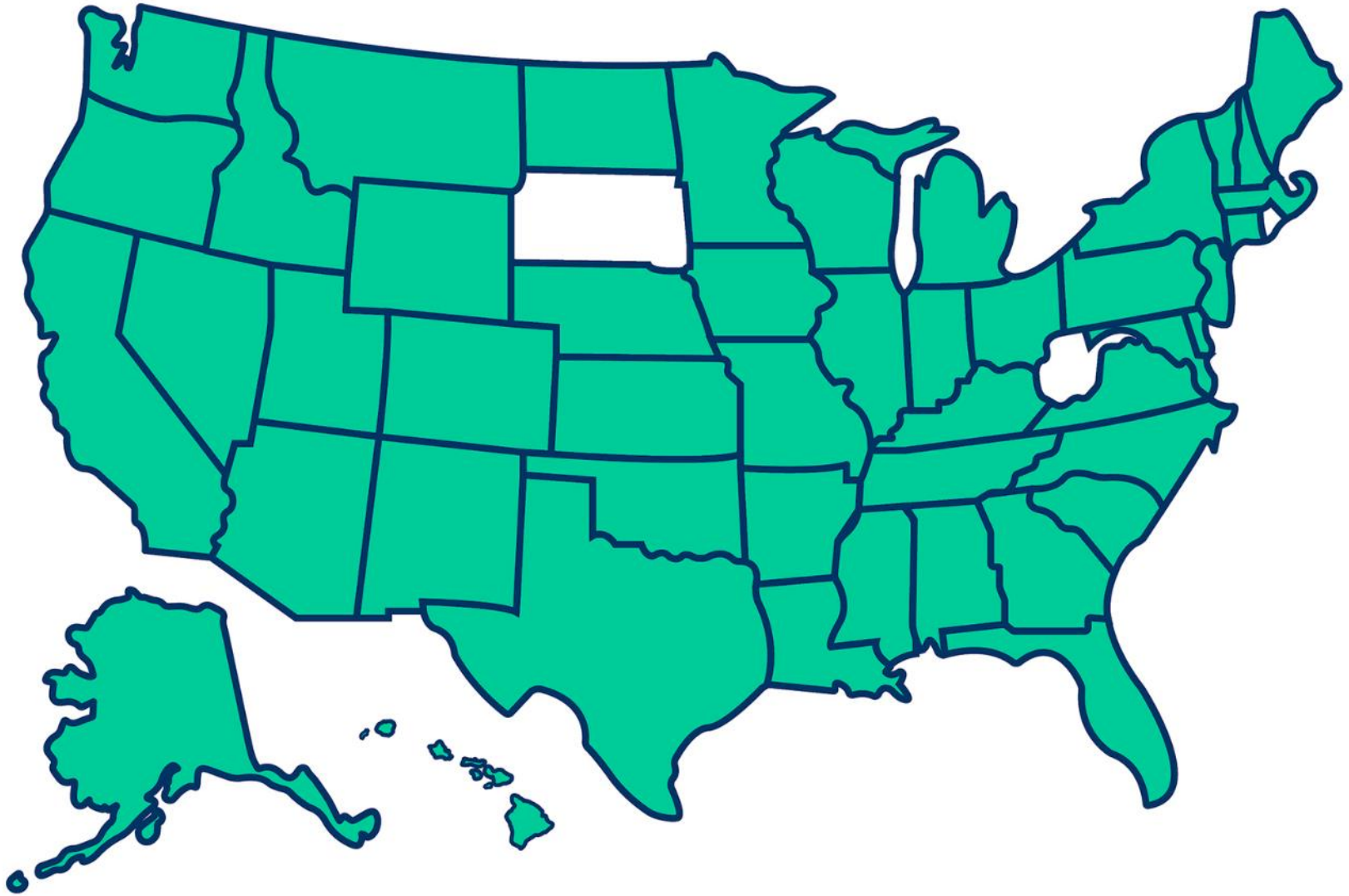
11,490

* As of 5/3/2022

U.S. CYBER RANGE

VIRGINIA CYBER RANGE

States Powered by the US Cyber Range, 2022



U.S. CYBER RANGE

VIRGINIA CYBER RANGE

Commonwealth Cyber Initiative Collaboration

- CCI grant to support web accessibility for web portal and courseware
- Diversity video series
- CTFs in support of CCI student summer camps
- Collaborating with CCI-funded research initiatives at various nodes

VIRGINIA CYBER RANGE

In the News . . .

THE ROANOKE TIMES
roanoke.com

THE WALL STREET JOURNAL.
WSJ

VIRGINIA ECONOMIC REVIEW

WSLS 10

edscoop

WHSV 3 abc

VIRGINIA BUSINESS

siliconANGLE

theCUBE®

WVTF PUBLIC RADIO

WFXR FOX

EdSurge

“The Virginia Cyber Range has enabled me to teach a Cybersecurity class without needing expensive hardware and software.”

“Without this environment, my students would have only learned theory and seen pictures of what a professional might use in this work.”

“The Virginia Cyber Range is a definite game changer!”

“There are a variety of big-ticket range products out there that are just unwieldy and hard to implement. This is quick, easy, and to the point!”

VIRGINIA
CYBER RANGE

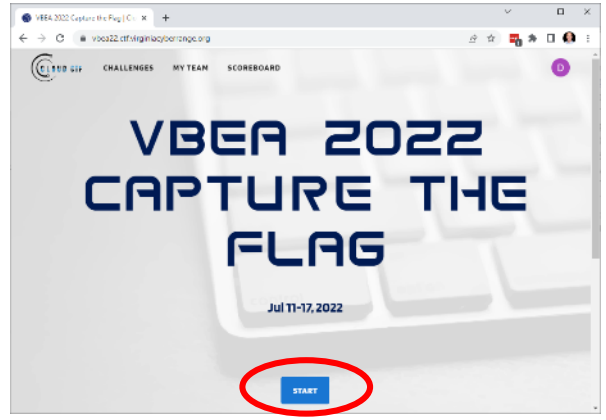
Introduction to Capture-the-Flag

David Raymond, Ph.D.
Director, Virginia Cyber Range
draymond@virginiacyberrange.org

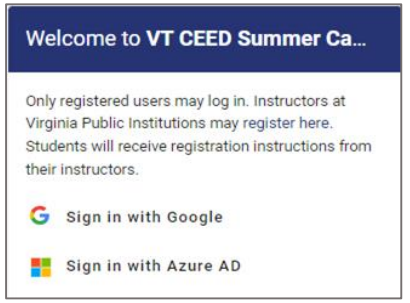
Play a CTF Today!

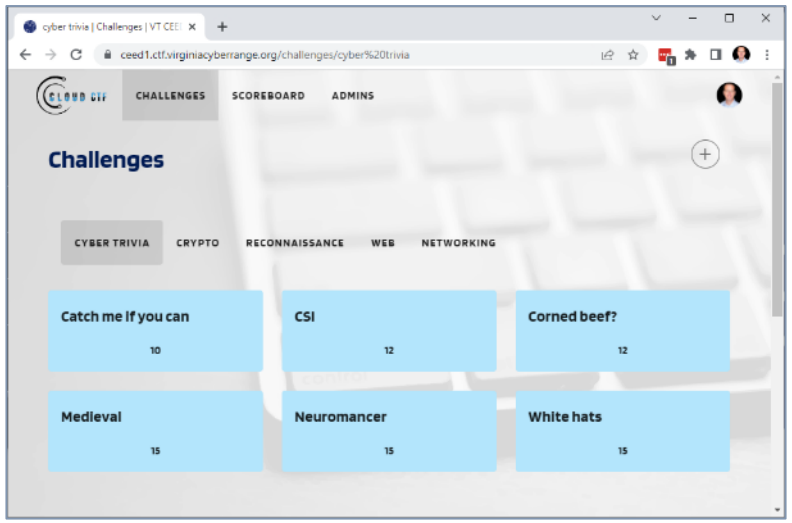
1. Browse to https://vacr.io/ctf and click “START”
2. Login with Google or Microsoft

1.



2.





Playing the Game

1. Select a Category
2. Click on a Challenge
3. Find and enter the flag

* Google is a great tool for finding resources to solve challenges!

What is *Capture-the-Flag*?

- ❑ Cybersecurity Competition
  - Can be individual or team-based
  - Sometimes in-person, often remote
- ❑ Various formats
  - ***Jeopardy-style. Most popular and easiest to create***
  - Attack/Defend (Red/Blue)
- ❑ Hosted by:
  - Teachers and professors
  - College CTF teams
  - Companies looking for talent
  - DoD and other government agencies

VIRGINIA CYBER RANGE

Why CTFs?

- Good way to spark interest in cybersecurity topics
  - Very popular among high school and college clubs
  - Can be used by teachers to reinforce classroom concepts
  - Gamifies the learning process
- A well-designed CTF . . .
  - Caters to wide range of ability levels
  - Encourages independent learning
  - Exercises real-world skills
- Can be used for . . .
  - Teambuilding events
  - Skills assessment
  - Teaching basic skills and problem-solving

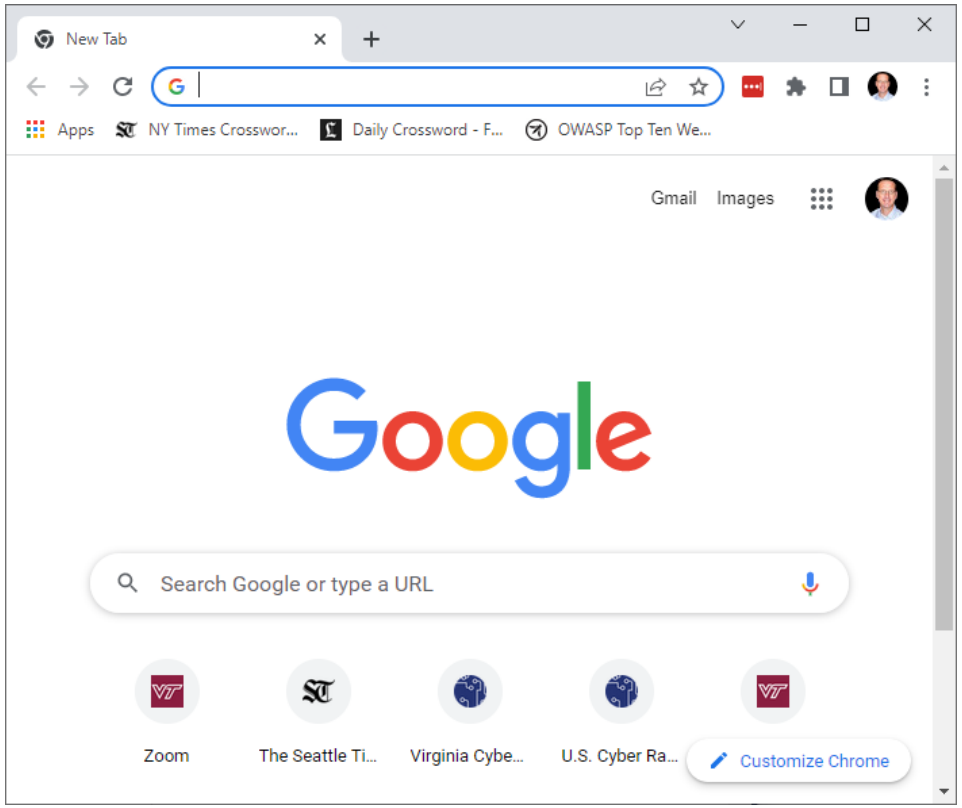
VIRGINIA CYBER RANGE

Common Challenge Types: Overview

- Trivia (various category names)
  - Category name might be targeted to specific topic areas
- Cryptography
  - Related to computer encodings, simple ciphers, or modern cryptography algorithms
- Web
  - Find flag hidden on a web page or in web traffic; or exploit vulnerable web application
- Reconnaissance
  - Follow a trail of hints to find a flag
- Networking
  - Find a flag by analyzing captured network traffic

Approaching Challenges: General Tips

- Look at point values
  - Indicates difficulty level
- Challenge name is almost always a hint
  - Google category along with challenge name
- Read the challenge description carefully
  - Google category along with keywords
- Is there a file? Filename might be a hint
  - The file extension might be wrong
  - Open the file and see if you can interpret contents
- Any people's names mentioned?
  - Is the name meaningful?



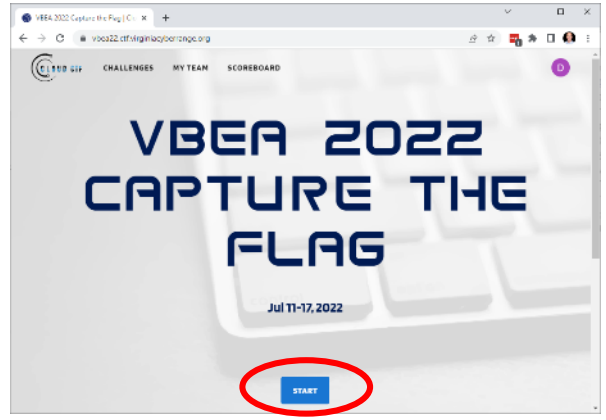
Google is the most useful CTF resource!

VIRGINIA CYBER RANGE

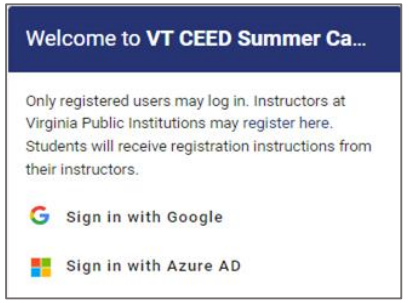
Play a CTF Today!

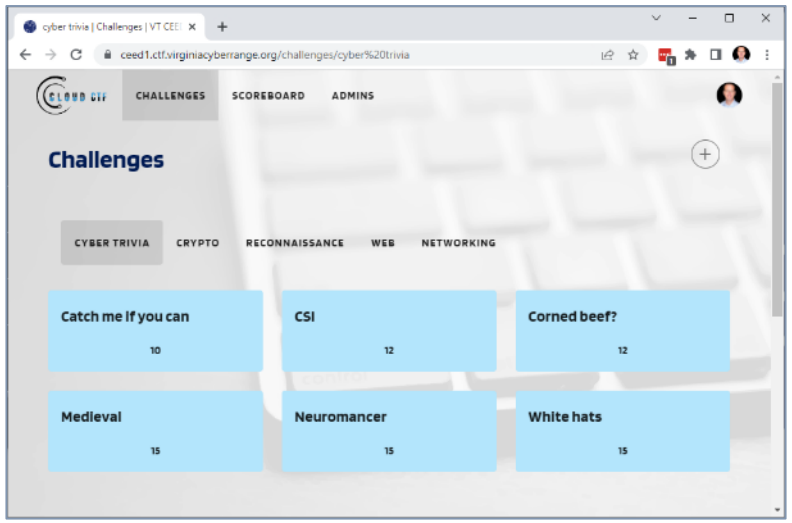
1. Browse to https://vacr.io/ctf and click “START”
2. Login with Google or Microsoft

1.



2.





Playing the Game

1. Select a Category
2. Click on a Challenge
3. Find and enter the flag

* Google is a great tool for finding resources to solve challenges!

Questions?

raymondd@vt.edu

VIRGINIA CYBER RANGE

Making Virginia a national resource for cybersecurity education.

CONNECT WITH US

@VaCyberRange

virginiacyberrange.org

Understanding Today's Modern Attack and the Power of a Platform to Empower Zero Trust

Patrick Doherty, VP Identity Protection Sales

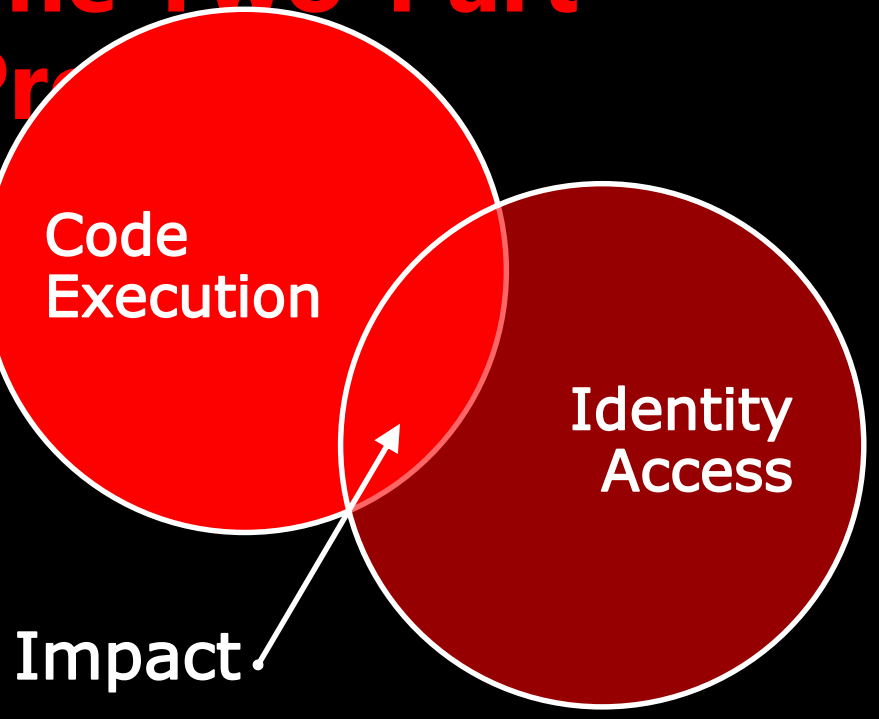
AGENDA

- Modern Attack Breakdown
- Platform Approach
- Bringing Simplicity to Zero Trust
- Q&A

CROWDSTRIKE

Modern Attack Breakdown

Modern Attacks: The Two-Part Pr



Modern attacks like ransomware, Log4j, noPac consist of two parts:

- Code execution
- Identity access

Adversary executes code on a single system (foothold)

Adversary leverages valid credentials to look normal and move laterally (LOTL)

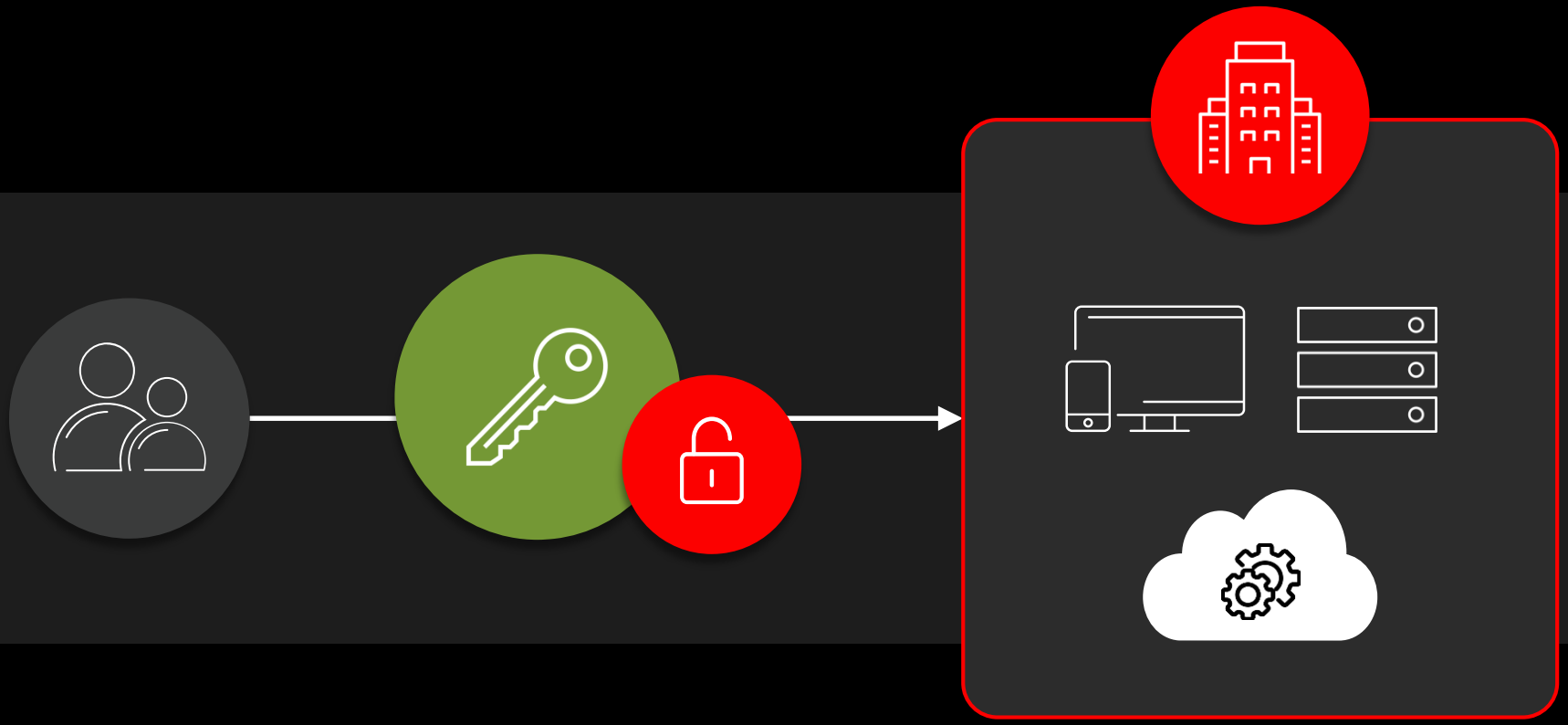
CROWDSTRIKE

80%+

OF BREACHES INCLUDE USE OF
VALID CREDENTIALS
(Active Directory, Azure AD, SSO)

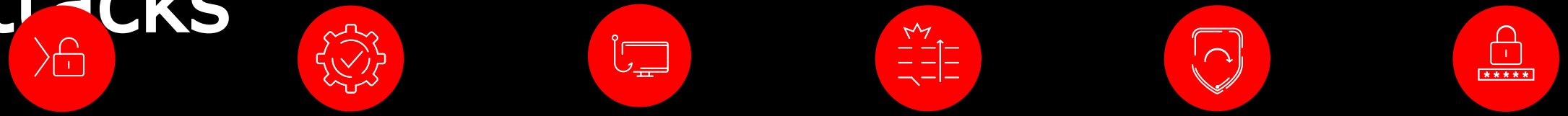
CROWDSTRIKE

Identity is the key to your enterprise



CROWDSTRIKE

And those keys are being stolen to execute hard to detect identity-based attacks



Initial Access

Technique	Sub-Technique
Valid Accounts	Domain Accounts
	Local Accounts
	Default Accounts
Exploit Public-Facing Application	
Phishing	Spearphishing Attatchment
	Spearphishing Link
	Spearphishing via Service

Execution

Technique	Sub-Technique
Command and Scripting Interpreter	Windows Command Shell
	PowerShell
	UnixShell
	Visual Basic
	Python
	Javascript
Windows Management Instrumentation	

Persistence

Technique	Sub-Technique
Valid Accounts	Domain Accounts
	Local Accounts
	Default Accounts
Scheduled Task/Job	Scheduled Task
	Cron
Create Account	Local Account
	Domain Account

Privilege Escalation

Technique	Sub-Technique
Valid Accounts	Domain Accounts
	Local Accounts
	Default Accounts
Scheduled Task/Job	Scheduled Task
	Cron
Create Account	Local Account
	Domain Account

Defense Evasion

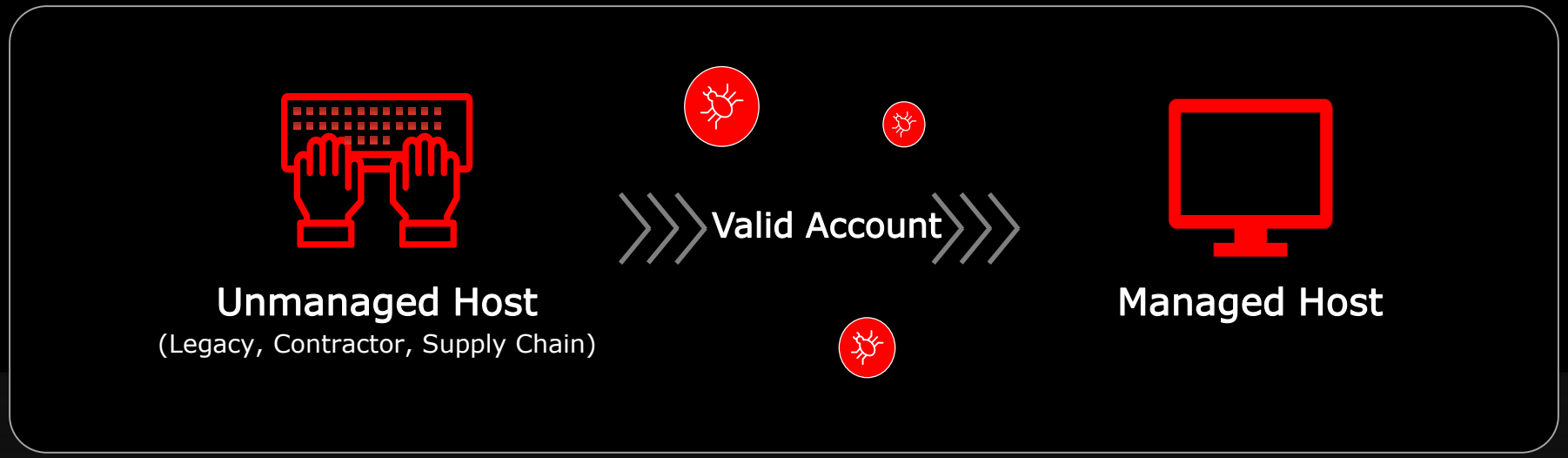
Technique	Sub-Technique
Valid Accounts	Domain Accounts
	Local Accounts
	Default Accounts
Masqueradin g	Match Legitimate Name or Location
	Masquerade Task or Service
	Rename System Utilities

Credential Access

Technique	Sub-Technique
OS Credential Dumping	LSASS Memory
	Security Account Manager
	NTDS
	/etc/passwd and/etc/shadow
	LSA Secrets
	Cached Domain Credentials

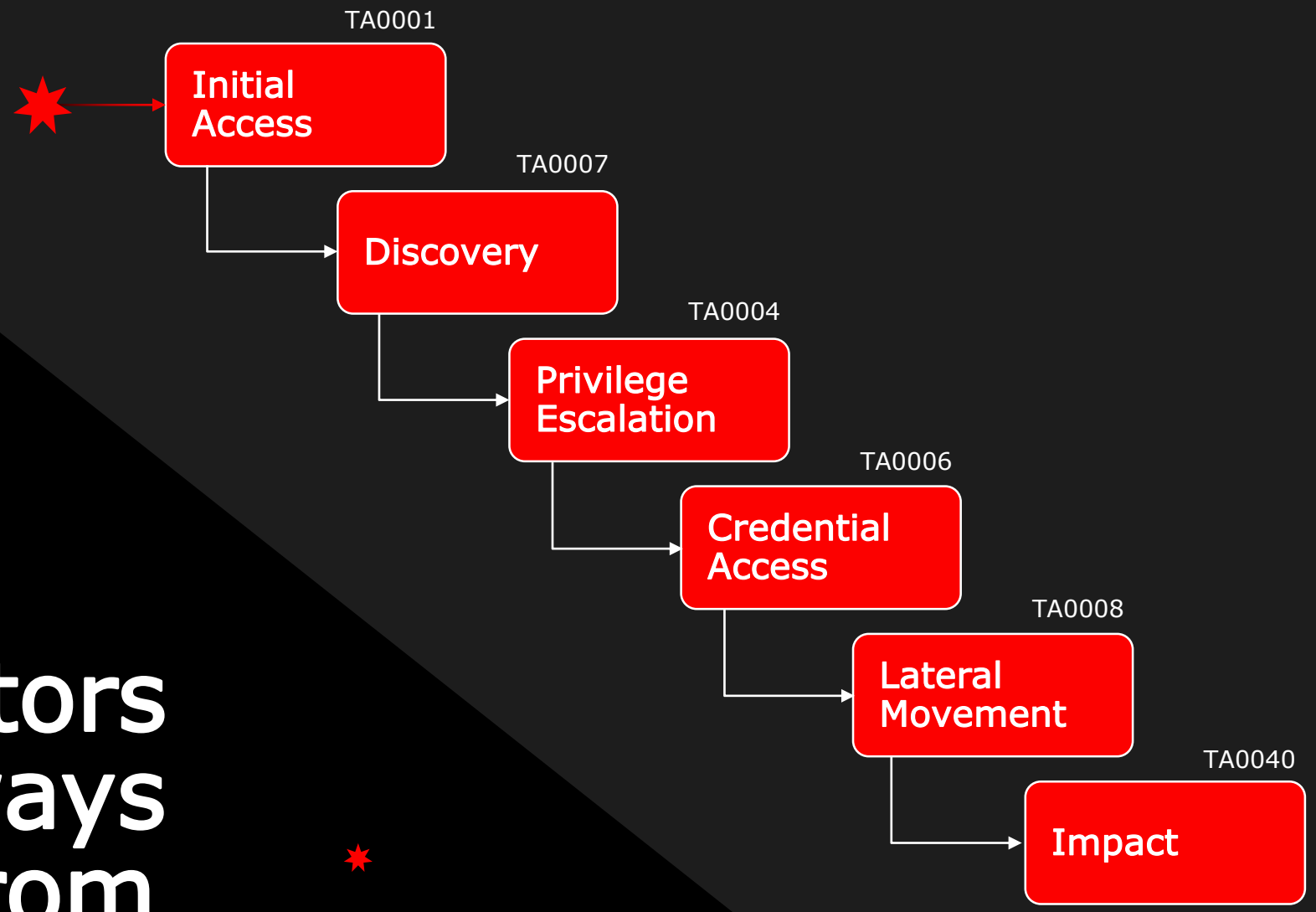
CROWDSTRIKE

Defense Evasion



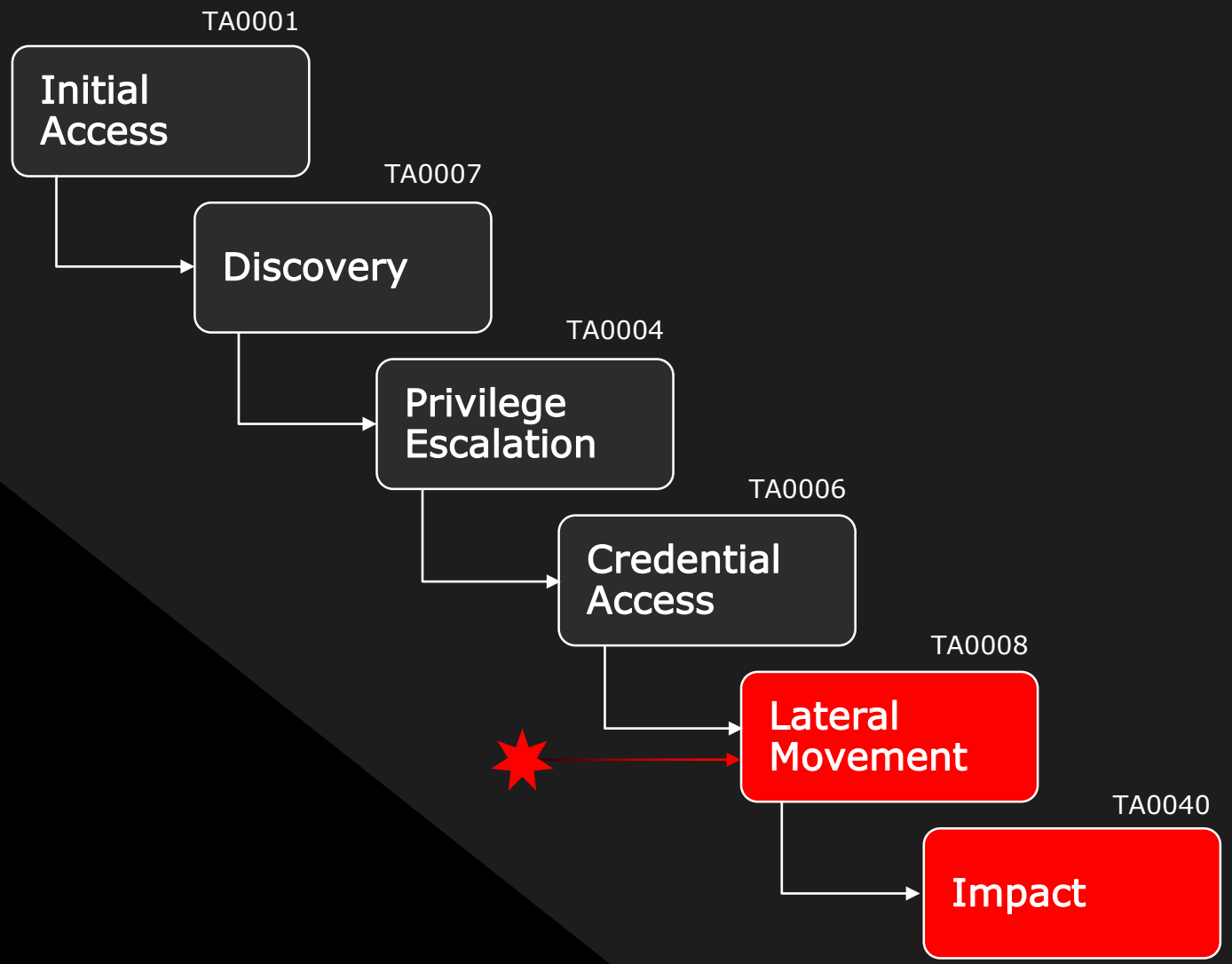
25% of attacks originated from unmanaged hosts

CROWDSTRIKE



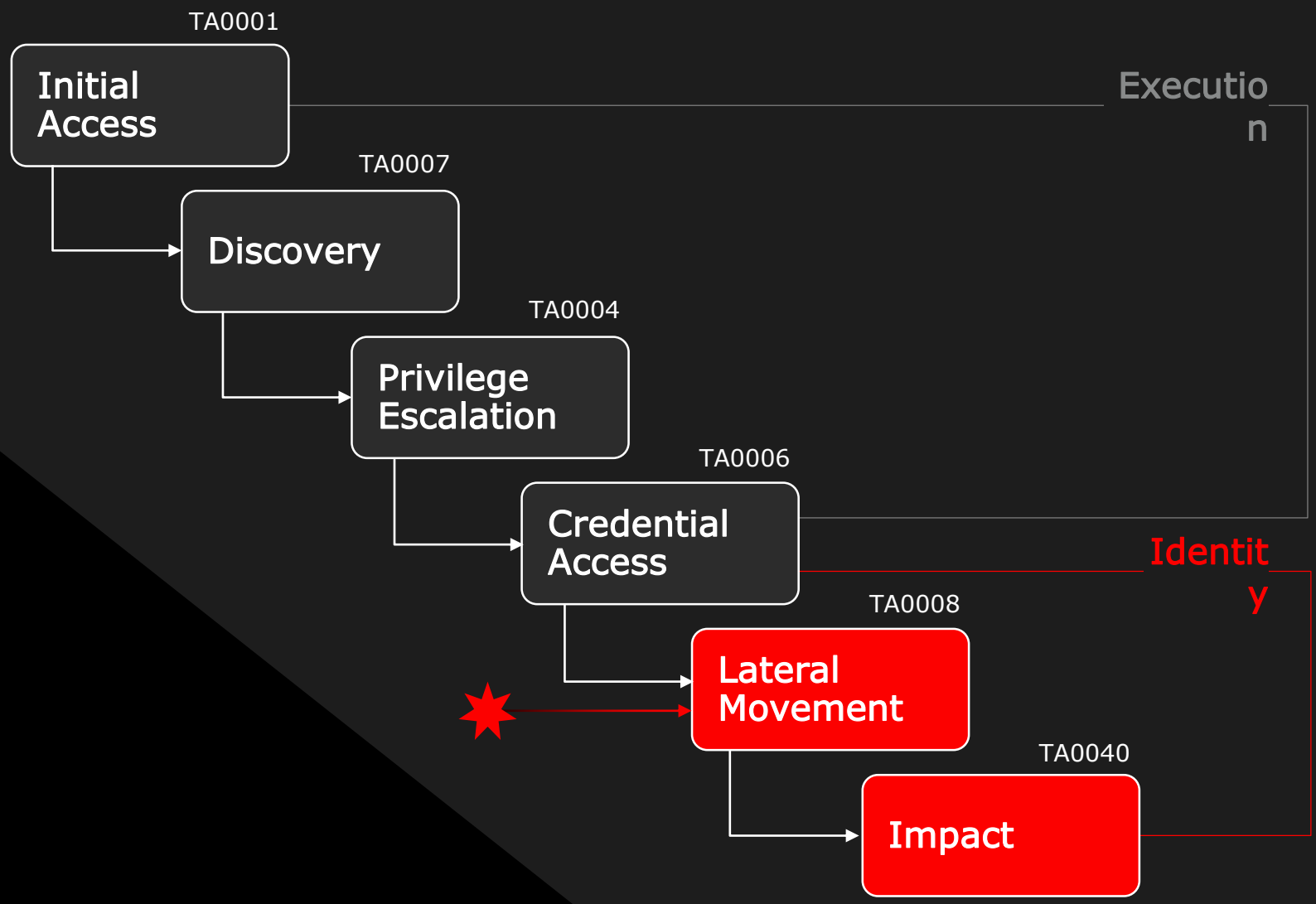
Threat actors aren't always starting from here

CROWDSTRIKE



Often, they are starting here

CROWDSTRIKE



Often, they are starting here

CROWDSTRIKE

CROWDSTRIKE

Platform Approach

Power of the Security Cloud

180+
Adversaries Tracked

1+ Trillion
Events/Day

135+ Million
IOA Decisions/Min

1.5+ Billion
Containers Protected/Day

Asset Graph
IT Asset Context

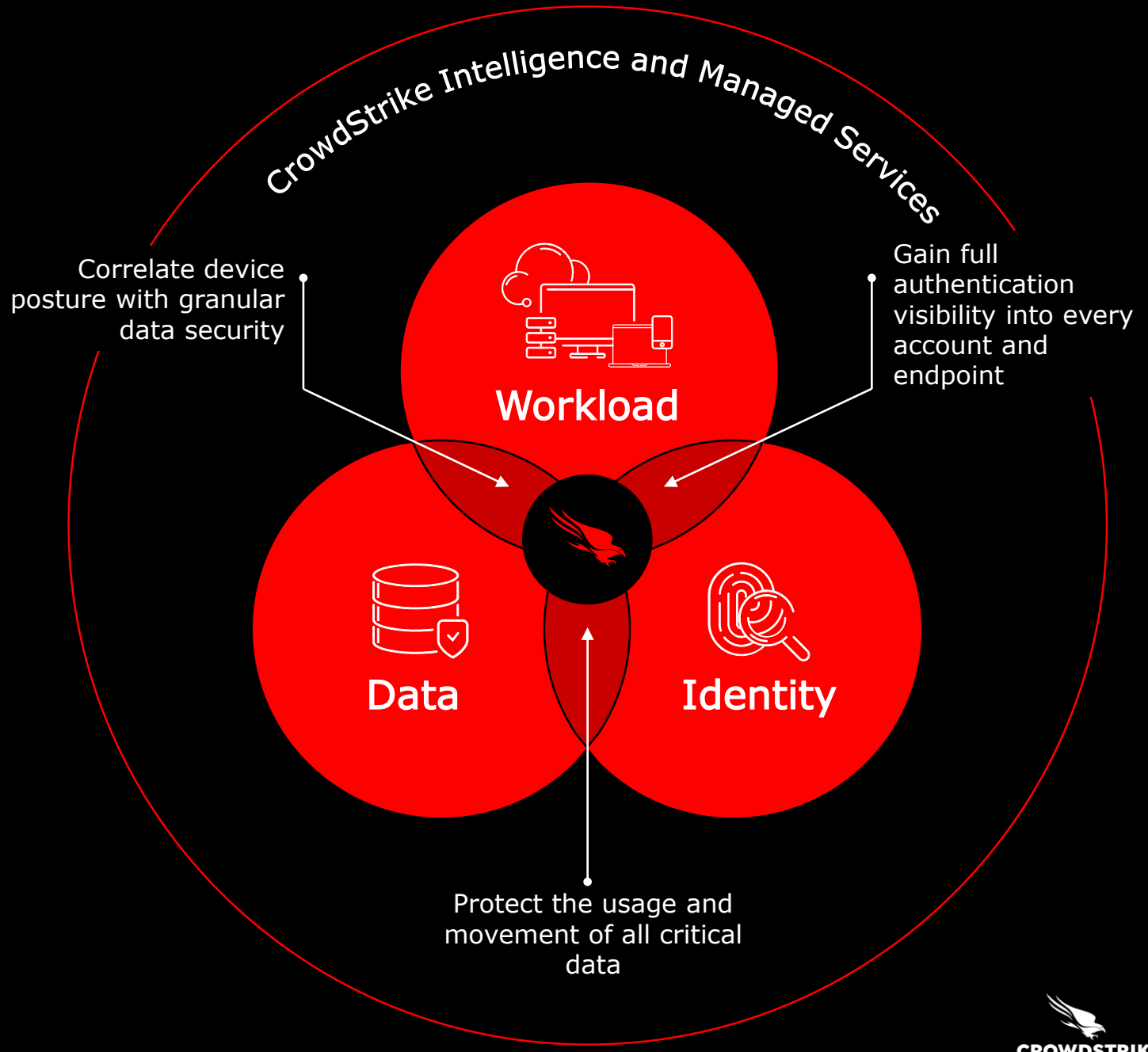
Threat Graph
Threat Intelligence

Intel Graph
Adversary Data

CROWDSTRIKE

CrowdStrike Platform

Protection at every layer.



CROWDSTRIKE

One Agent
Full Visibility

Falcon Agent

Prevent • Predict • Detect • Respond

Endpoints

Workstations

Mobile

Servers

IOT

Clouds

Data Centers

Workloads

Containers

Identities

Active Directory

User Accounts

3rd Parties

CROWDSTRIKE

Top Adversary ATT&CK
Tactics in 2022… Thus far

Actor Class	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
eCrime	Valid Accounts	Command and Scripting	Valid Accounts	Valid Accounts	Valid Accounts	OS Credential Dumping	System Owner/ User Discovery	Remote Services	Archive Collected Data	Ingress Tool Transver	Exfiltration Over Alternative Protocol	Service Stop
Targeted	Valid Accounts	Command and Scripting	Valid Accounts	Valid Accounts	Valid Accounts	OS Credential Dumping	System Owner/ User Discovery	Remote Services	Archive Collected Data	Ingress Tool Transver	Exfiltration Over Alternative Protocol	Service Stop

CROWDSTRIKE

Endpoint Protection
Coverage of Tradecraft

Actor Class	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
eCrime		✓ Command and Scripting				✓ OS Credential Dumping	✓ System Owner/ User Discovery		✓ Archive Collected Data	✓ Ingress Tool Transver	✓ Exfiltration Over Alternative Protocol	✓ Service Stop
Targeted		✓ Command and Scripting				✓ OS Credential Dumping	✓ System Owner/ User Discovery		✓ Archive Collected Data	✓ Ingress Tool Transver	✓ Exfiltration Over Alternative Protocol	✓ Service Stop

CROWDSTRIKE

Identity Threat Protection

Coverage of Tradecraft

Actor Class	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
eCrime	Valid Accounts		Valid Accounts	Valid Accounts	Valid Accounts	OS Credential Dumping		Remote Services				
Targeted	Valid Accounts		Valid Accounts	Valid Accounts	Valid Accounts	OS Credential Dumping		Remote Services				

CROWDSTRIKE

Falcon Platform
Coverage of Tradecraft

Actor Class	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
eCrime	Valid Accounts	Command and Scripting	Valid Accounts	Valid Accounts	Valid Accounts	OS Credential Dumping	System Owner/ User Discovery	Remote Services	Archive Collected Data	Ingress Tool Transver	Exfiltration Over Alternative Protocol	Service Stop
Targeted	Valid Accounts	Command and Scripting	Valid Accounts	Valid Accounts	Valid Accounts	OS Credential Dumping	System Owner/ User Discovery	Remote Services	Archive Collected Data	Ingress Tool Transver	Exfiltration Over Alternative Protocol	Service Stop

CROWDSTRIKE

one PLATFORM

Protect

Reduce Identity Store Attack Surface

Visibility into AD/Azure AD, hybrid identity stores

Auto-classify all identities

Get identity store attack path visibility

Enable identity segmentation

Prevent

Detect AND Prevent ID Threats

Detect & respond to ID specific threats – hybrid directories, multi-vendor SSO

Create simple, dynamic policies that adapt to the attack path

Defend your AD/Azure AD from modern attacks

Enable

MFA Everywhere

Enable risk-based MFA and improve UX

Extend MFA protection to legacy apps/tools

Digest ZTA risk score to key in device risk posture

CROWDSTRIKE

CROWDSTRIKE

Zero Trust

Advancing Security Measures to Reduce Risks

Apps everywhere, work anywhere

Nation-state actors

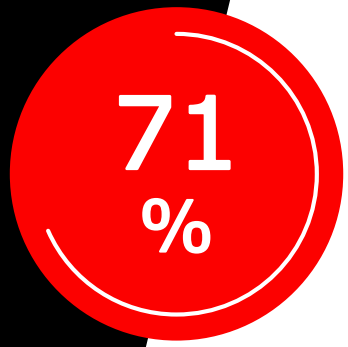
Ransomware, supply chain threats

Insider threats

CROWDSTRIKE

What Factors Play a Key Role in Choosing Your Zero Trust Solution? [1]

Ease of deployment



Ease of use (less friction for users)

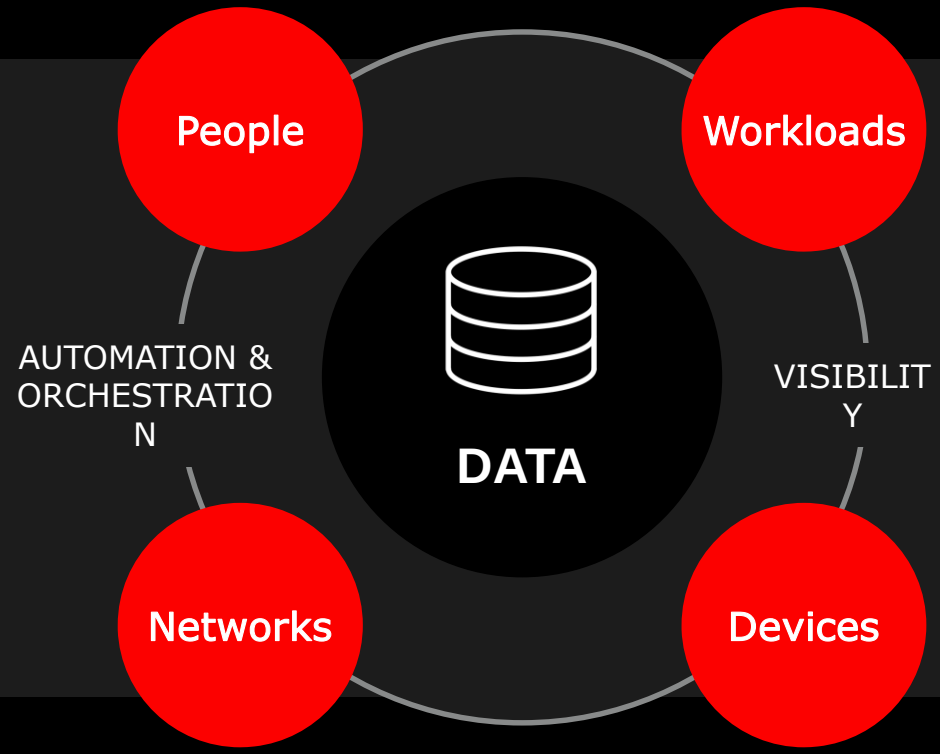
Security coverage

1July '21 CrowdStrike Survey

CROWDSTRIKE

Required Capabilities for Cloud First, Work Anywhere

Based on The NIST 800-207 Framework



Behavioral data

Segmentation & least access

Security automation {tied to context}

Continuous verification

CROWDSTRIKE

Cloud-Native, Single Agent Architecture

Easy Deployment

Security Cloud

Requestor

Endpoint
Identity
Workload

Data

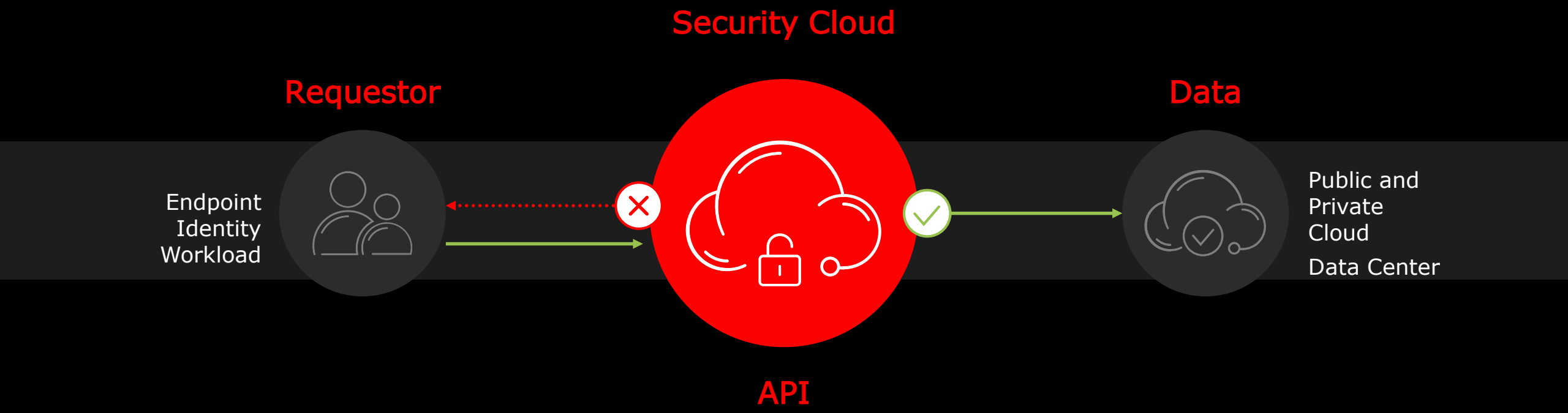
Public and
Private
Cloud

Data Center

CROWDSTRIKE

Continually Verify + Behavioral Data + Segmentation

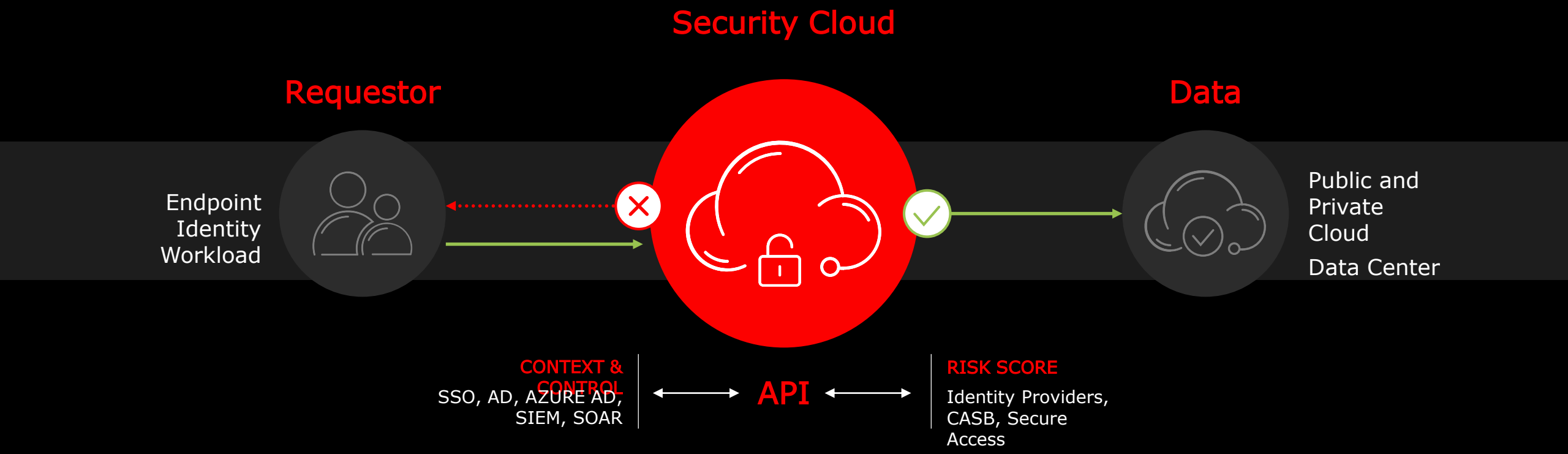
Frictionless User Experience



CROWDSTRIKE

Automate Context and Integrate with Existing Tools

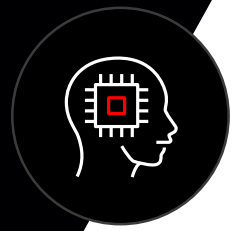
Increase Security Coverage/Save Cost



CROWDSTRIKE

Why CrowdStrike?

World's **largest** unified, threat-centric data fabric



World-class AI for **Hyper-accurate** detections & automated protection

Cloud-native for rapid deployment, scalability and **reduced complexity**

CROWDSTRIKE

CROWDSTRIKE

Q&A

UPCOMING EVENTS

ISOAG MEETING: DEC. 7

SPEAKERS:

TETOYA GIBSON – VERIZON

DAN HAN -VCU

BRYAN CARNAHAN - ASSURAINC

NEXT ISO ORIENTATION

DATE: DEC. 12

TIME: 1 – 3 P.M.

HOSTED BY – MARLON COLE

HTTPS://COVACONF.WEBEX.COM/COVACONF/ONSTAGE/G.PHP?MTID=E6299241BFEFDE9A4E45B6E1B8A81E7CB

VIRGINIA
IT AGENCY

MEETING ADJOURNED