

GRANTS OFFICE
empowering communities

Fortify Your Frontlines

Funding Cybersecurity with SLCGP and Beyond

Sponsored by: CROWDSTRIKE

AGENDA

01 | Welcome & Introductions

02 | CrowdStrike Cybersecurity Threat Report

03 | The Cybersecurity Funding Landscape

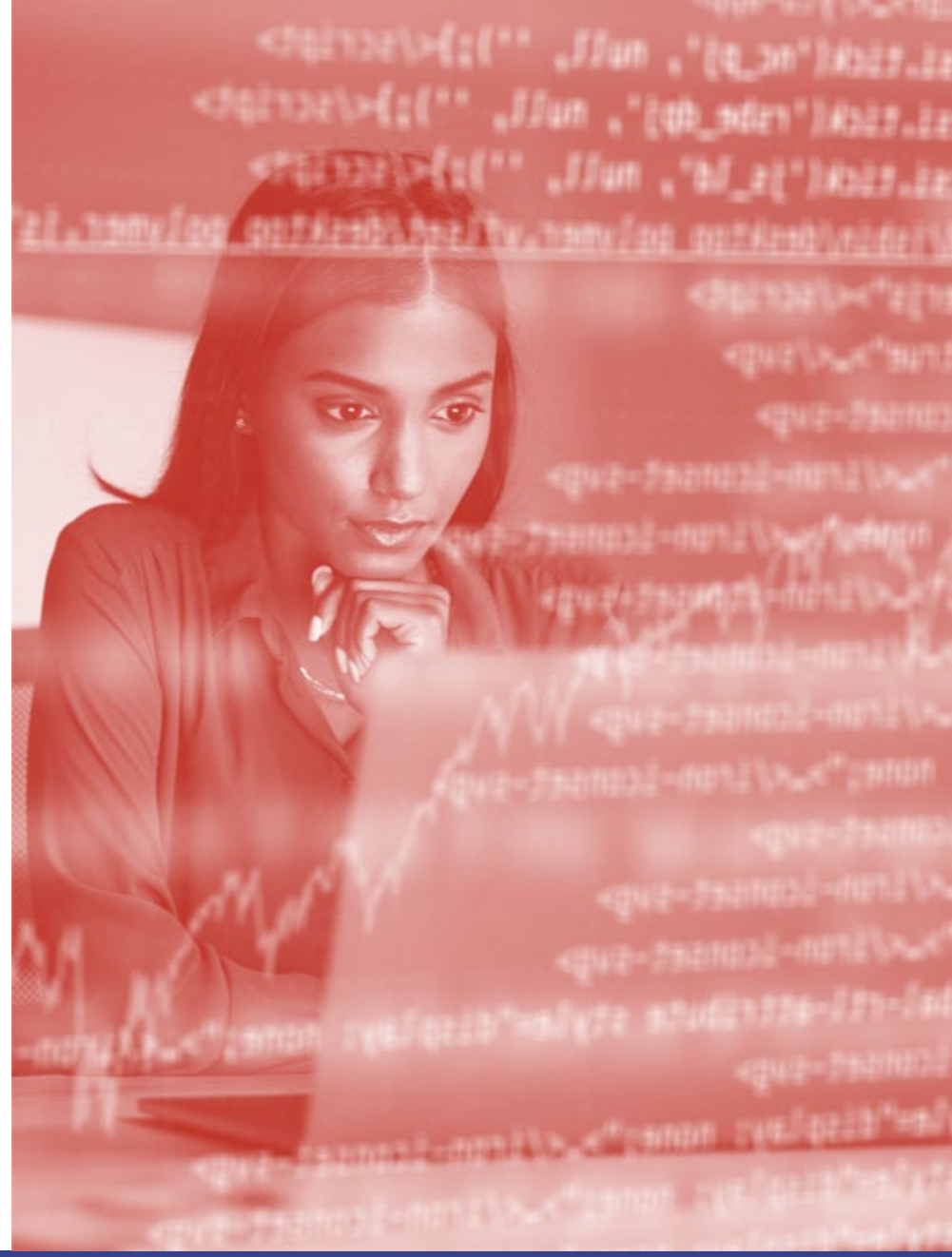
04 | Funding for Local & Tribal Governments

05 | Funding Cybersecurity for K-12

06 | Justifying Your Cybersecurity Needs

07 | CrowdStrike Solutions

08 | Q&A



Today's Presenters



Matt Singleton
CrowdStrike
Executive Strategist



Deborah Blyth
CrowdStrike
Executive Strategist



Michael Paddock
Grants Office
CEO



Amanda Day
Grants Office
Grants Development
Consultant



Sam Rawdon
Grants Office
Grants Development
Associate

CrowdStrike Global Threat Report

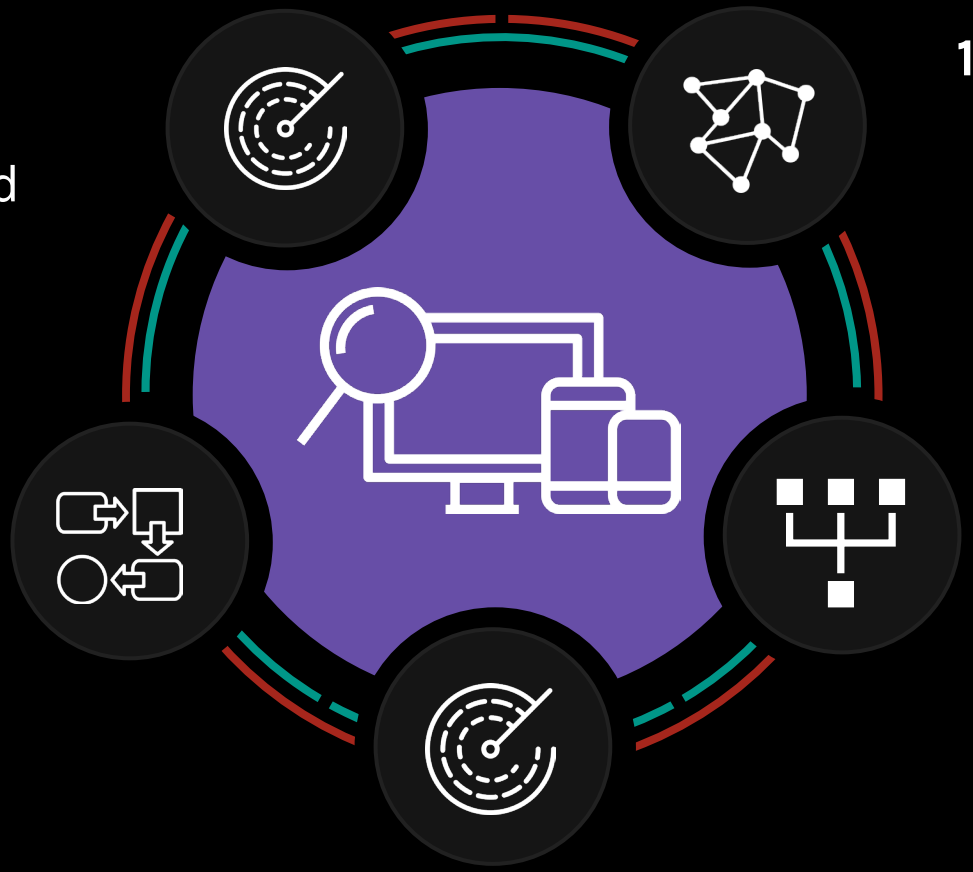
2024 COST OF A DATA BREACH REPORT (IBM)
KEY FINDINGS

#1 Primary Attack Vector: Compromised or Stolen Credentials
Taking longer to identify and Contain (292 days)

$2.2M breach costs savings when AI prevention is deployed

$9.36 million
Average US cost of a data breach

$173
Average cost per record



1 in 3 breaches involved shadow data

>100 days = recovery time for 3/4 of the organizations who suffered a breach

26.2% growth in cyber skills shortage

CROWDSTRIKE

® CrowdStrike, Inc. All Rights Reserved



CROWDSTRIKE

2025 GLOBAL THREAT REPORT

The Enterprising Adversary

Threat Landscape by the numbers

INITIAL ACCESS

442%
Increase in Voice Phishing (Vishing) in 2024

50%
Increase in Access Broker Activity

52%
Vulnerabilities observed related to Initial Access

LATERAL MOVEMENT

51s
Fastest Breakout Time

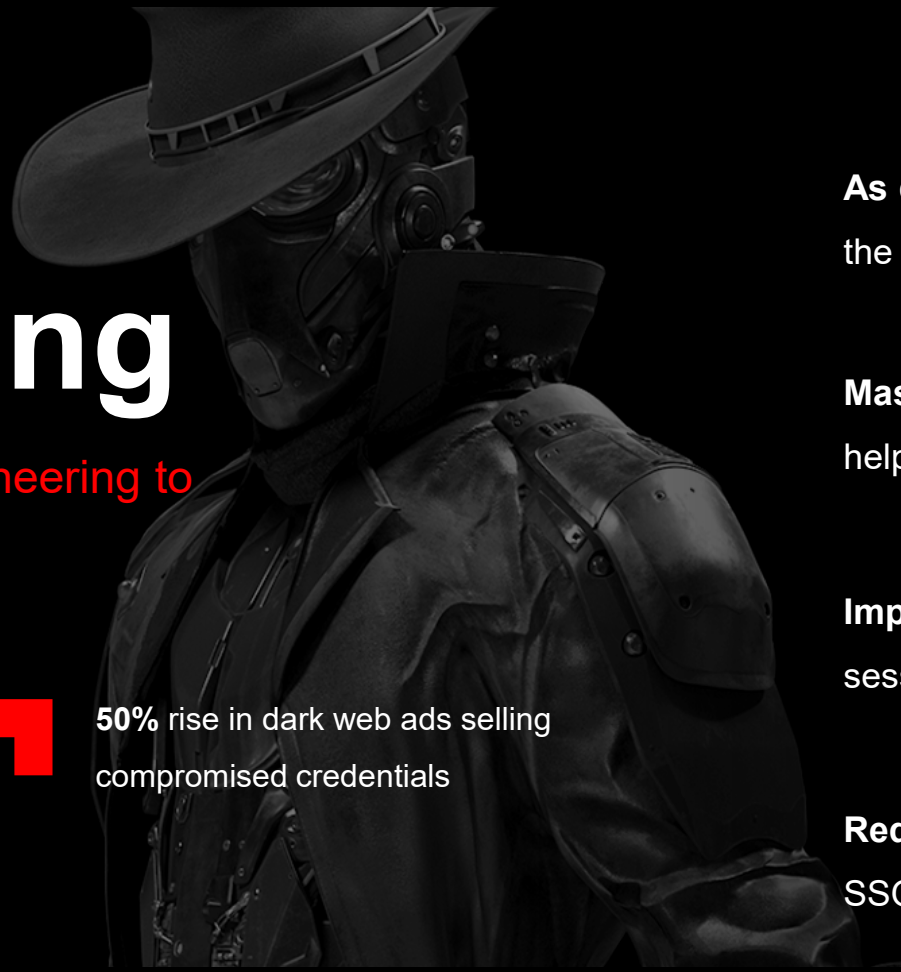
STEALTH

79%
Detections were Hands-on-Keyboard

® CrowdStrike, Inc. All rights reserved.

Social Engineering

Adversaries exploit social engineering to gain legitimate access



442% increase in Vishing in 2024

50% rise in dark web ads selling compromised credentials

As defenses strengthen adversaries targeted the weakest link – humans

Massive increase in vishing and help desk social engineering

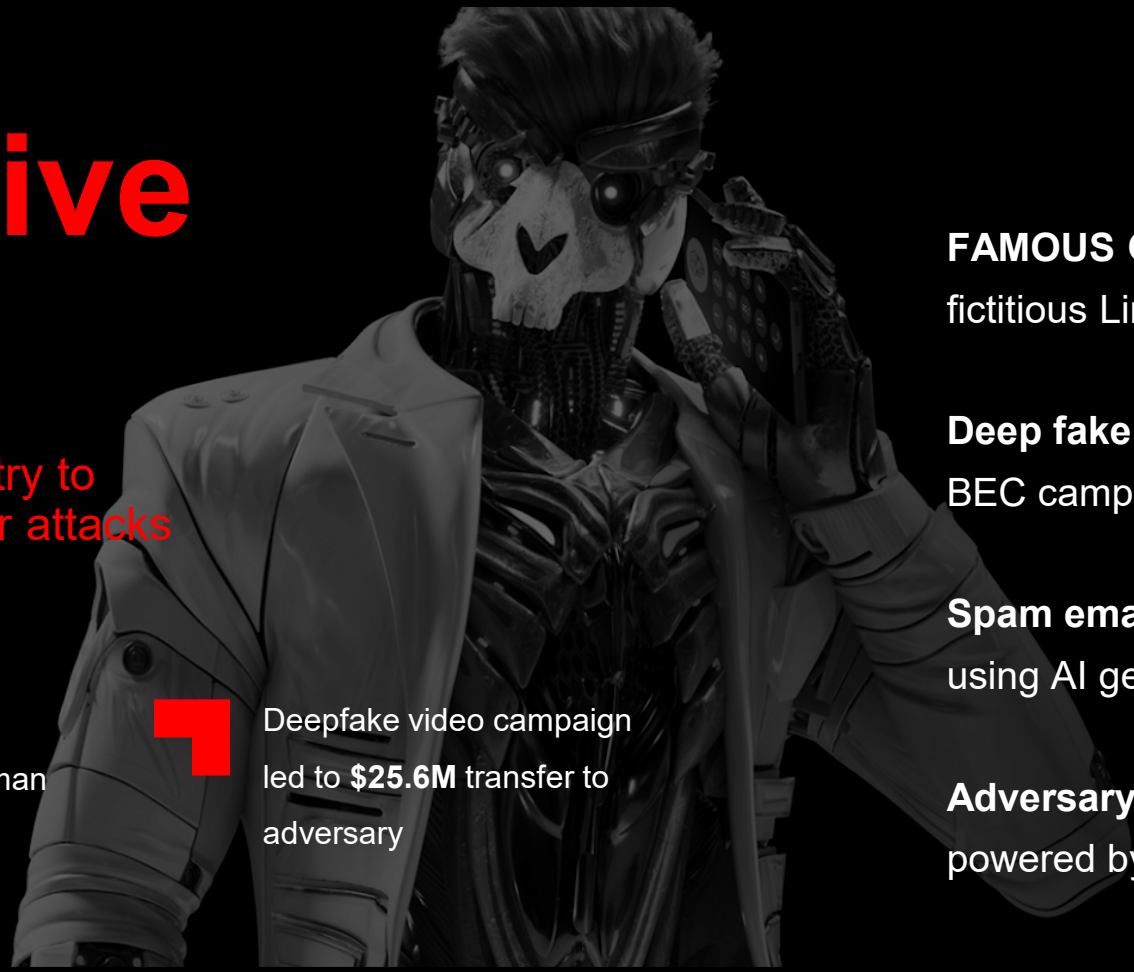
Impersonated IT support to establish remote sessions for malicious actions

Requested password/MFA resets to access SSO and cloud applications

® CrowdStrike, Inc. All rights reserved.

Generative AI

Lowering the barrier of entry to conducting effective cyber attacks



- AI-generated phishing emails have a **54%** click through, human written only **12%***
- Deepfake video campaign led to **$25.6M** transfer to adversary

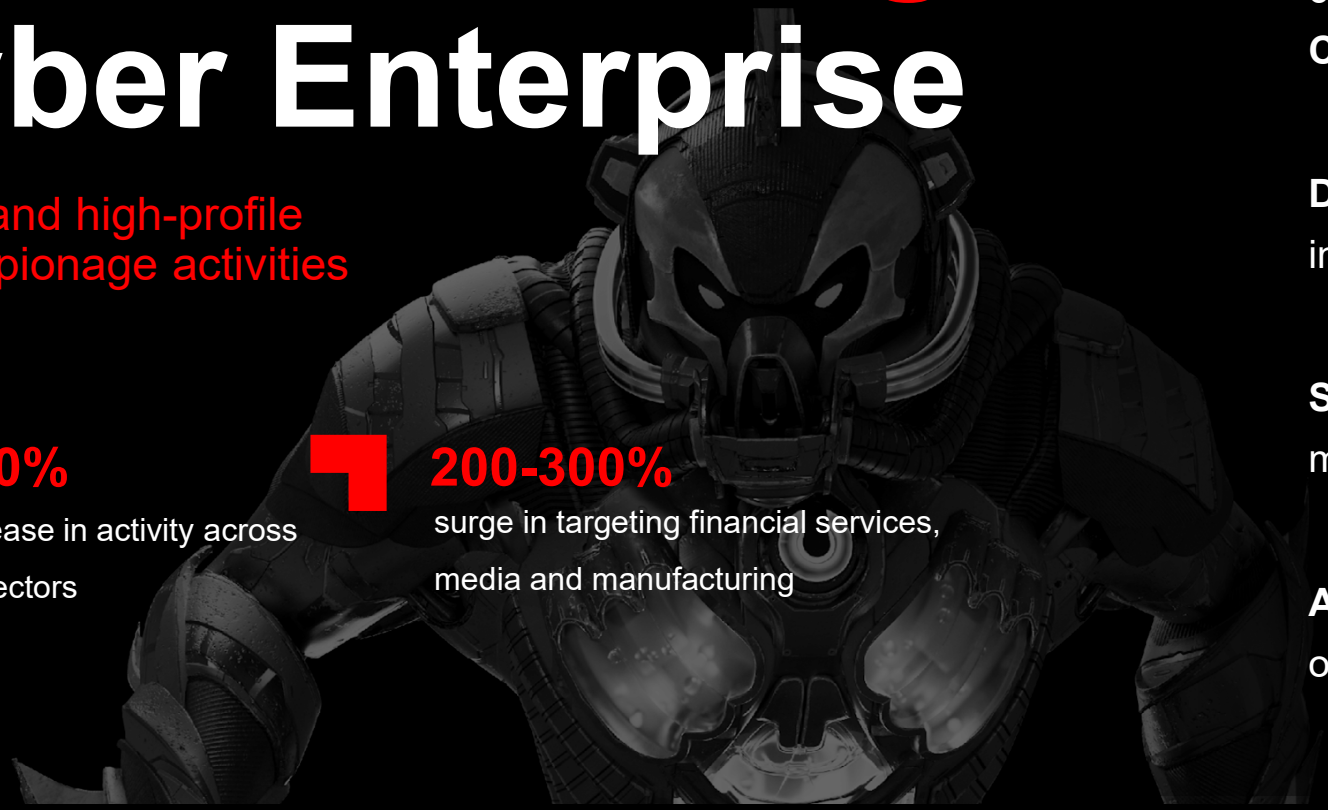
- **FAMOUS CHOLLIMA** employed AI to create fictitious LinkedIn profiles
- **Deep fake video** and voice clones enabled BEC campaigns
- **Spam email campaigns** distributed malware using AI generated content
- **Adversary disinformation campaigns** powered by GenAI

* https://arxiv.org/pdf/2412.00586

® CrowdStrike, Inc. All rights reserved.

China's Growing Cyber Enterprise

Prolific and high-profile cyberespionage activities



150%
increase in activity across all sectors

200-300%
surge in targeting financial services, media and manufacturing

Decades of government investment into China's cyber capabilities have put **China on par with other world powers**

Driven by geopolitical ambitions, including Taiwan reunification

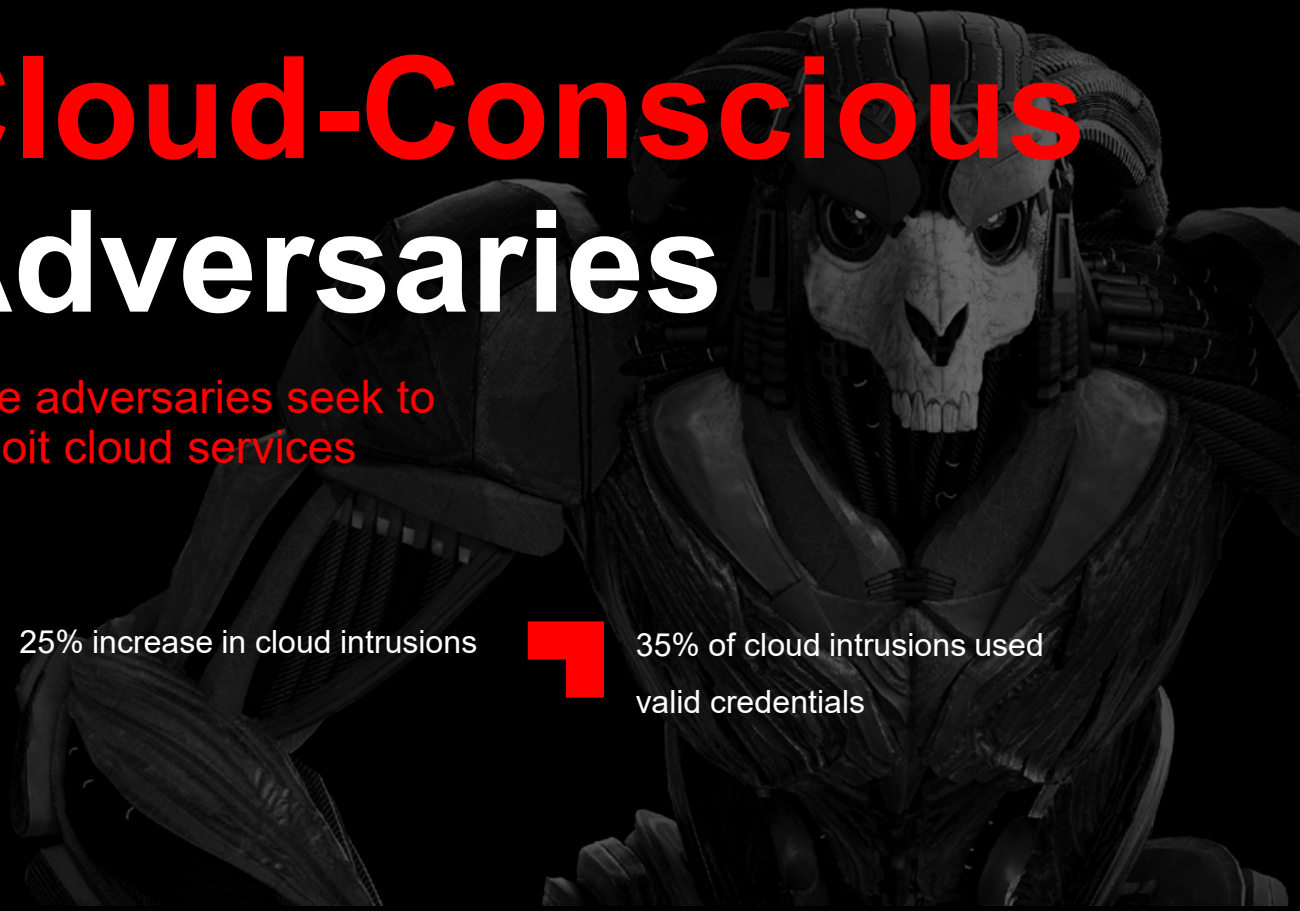
Specialization signals a shift to mission specific intrusions

Adversaries increasingly used ORB networks to obfuscate activity

® CrowdStrike, Inc. All rights reserved.

CROWDSTRIKE

Cloud-Conscious Adversaries



More adversaries seek to exploit cloud services

- 25% increase in cloud intrusions
- 35% of cloud intrusions used valid credentials

Adversaries increasingly target the cloud control plane

Cloud-conscious adversaries are beginning to explore **genAI and LLMs** as targets

Password spraying techniques evolved significantly in 2024 to target the cloud

China and DPRK-nexus adversaries increasing target cloud for data collection

® CrowdStrike, Inc. All rights reserved.

Vulnerability Exploitation

Adversaries continued to target devices in the network periphery



52% of vulnerabilities in 2024 were related to initial access

Network devices are a popular target due to security shortcomings

Chaining Exploits increases capabilities and impact

Abusing legitimate features can provide remote code execution

Adversaries leverage public research, disclosures and blogs to support the creation of exploits

® CrowdStrike, Inc. All rights reserved.

SaaS Exploitation



Adversaries following the shift to cloud-based services

- Microsoft 365 is frequently targeted
- Sharepoint 22%
  Outlook 17% of intrusions

Stolen SSO credentials enables widespread SaaS compromise

Adversaries weaponize SaaS for downstream attacks

Unsecured cloud databases are easy targets

Stronger MFA is essential to protect SaaS services

® CrowdStrike, Inc. All rights reserved.

Get the CrowdStrike 2025 Global Threat Report



Understanding the Cybersecurity Funding Landscape

3 Main Sources of Cybersecurity Funding

Federal Programs

Federal grant programs distribute funds directly to eligible recipients—such as state and local governments, nonprofit organizations, educational institutions, businesses, and individuals.

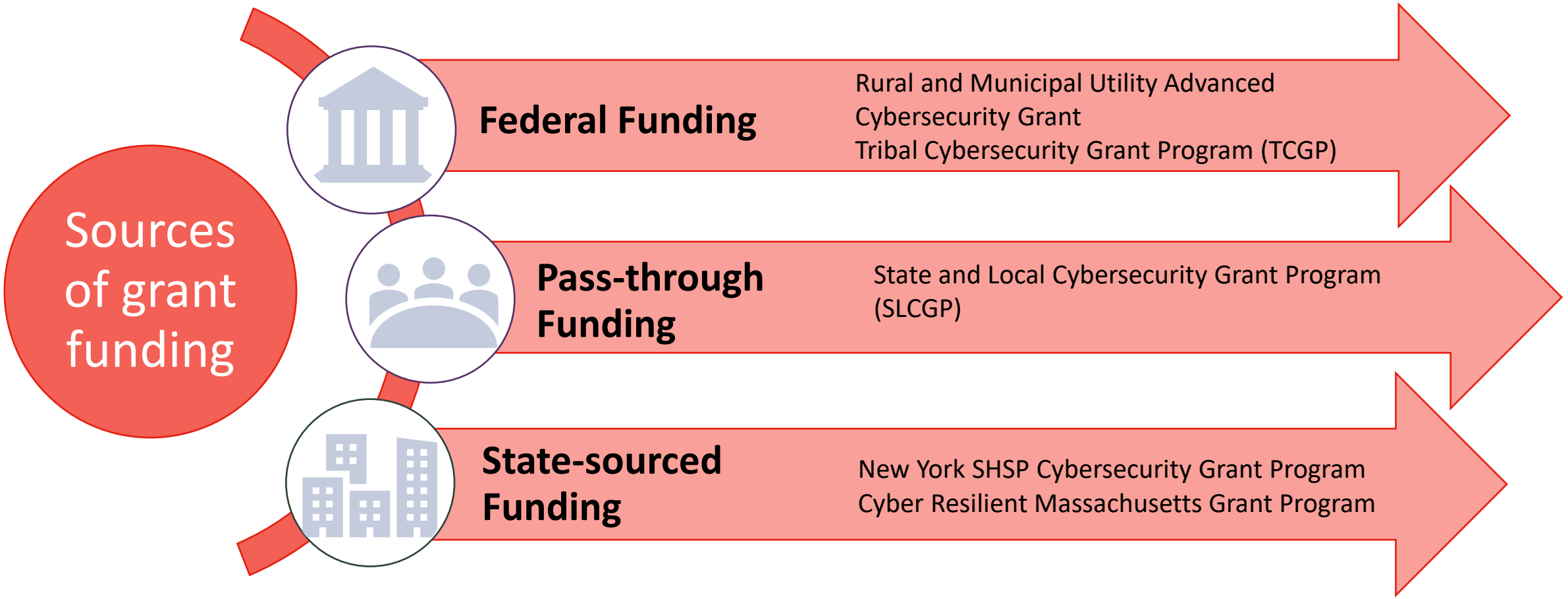
Pass-through Programs

Pass-through programs are a type of grant in which the federal government provides funding to a state or other primary recipient, which then passes the funds on to sub-recipients, such as local governments, nonprofits, or other organizations.

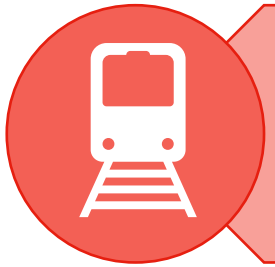
State-level Programs

A state-level grant program is a funding initiative administered by a state government to support specific projects or services within that state. These grants may be funded using state revenues.

Cybersecurity-Focused Grants Based on Type of Grant Source

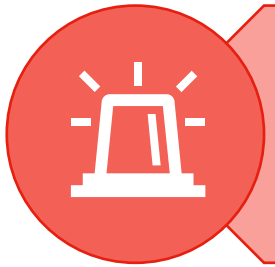


Top Cybersecurity Grant Funding Agencies



Department of Transportation

Total Funding Potential: $13,979,687,000



Federal Emergency Management Agency

Total Funding Potential: $2,550,568,484



Bureau of Justice Assistance

Total Funding Potential: $1,772,875,309

Cybersecurity Project Examples

Homeland Security Projects

- Anti-terrorism initiatives
- Emergency preparedness projects
- Election security projects

Law Enforcement Projects

- Updating/replacing a 911 center
- Body-worn camera implementation
- Rugged laptop programs

Water and Sewer Projects

- Replacing/upgrading SCADA systems
- Pumping station replacement
- Physical security upgrades (surveillance, etc.)

Public Healthcare Projects

- Protecting patient and staff data
- Combating ransomware attacks
- Protecting critical infrastructure

The State and Local Cybersecurity Grant Program: Progress and Outlook

State and Local Cybersecurity Grant Program (SLCGP)



Description

Administered by the **Department of Homeland Security (DHS)** and the **Federal Emergency Management Agency (FEMA)**, grant funds will be used to improve the nation's cybersecurity posture and protect critical infrastructure from malware, ransomware, and other threats.

States may choose to subgrant funds directly to eligible local entities to purchase necessary cybersecurity solutions and other eligible expenses, or they may purchase cybersecurity solutions and other eligible expenses at the state level on behalf of all local governments.

Funding Amount

$1 billion to 56 U. S. states and territories from FY22 through FY25.

Deadlines

States applied for FY23 funds in October 2023.

States applied for FY24 funds in September 2024.

Local deadlines will vary by state.

Eligibility

States, counties, municipalities, the District of Columbia, tribal governments, and five US territories are eligible.

Tribal Cybersecurity Grant Program (TCGP)



Description

The **Tribal Cybersecurity** Grant is a federal initiative designed to help tribal governments improve their cybersecurity capabilities and training. Guidelines are much the same as the **SLCGP**.

Applicants may apply to the **SLCGP** for funding, or they may choose to apply for the **TCGP**. Tribes can also apply for both grants, though they may not receive funding from both grants for the same project.

Funding Amount

For fiscal year 2022 and 2023, a total of $18.2 million in funding was provided by the State and Local Cybersecurity Grant Program (SLCGP). Future funding is TBA.

Deadline

FY24 deadline is to be announced.

Eligibility

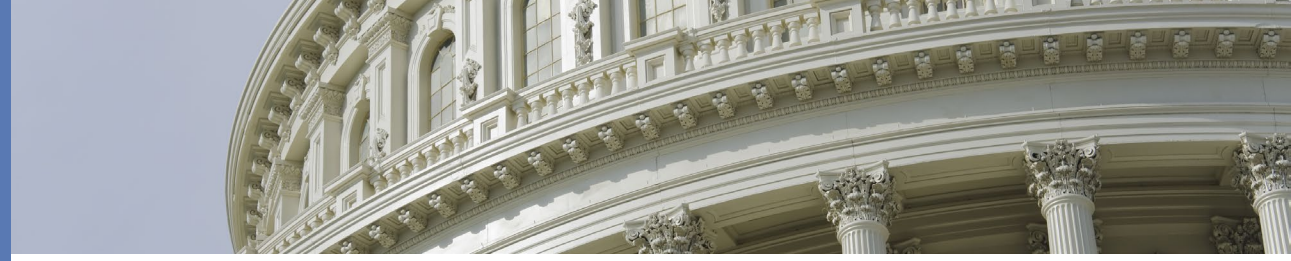
Eligible applicants are any recognized governing body of an Indian or Alaska Native Tribe.

US House Subcommittee reviews State and Local Cybersecurity Grant Program

Committee:
U.S. House Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection

Date:
April 1, 2025

Subject:
Reauthorization review of the State and Local Cybersecurity Grant Program (SLCGP), managed by the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Emergency Management Agency (FEMA).



Subcommittee chairman, Andrew Garbarino stated that cybersecurity is a whole-of-society challenge that the federal government must continue to support.

Cybersecurity experts from state governments and the private sector testified about the program and suggested several modifications that could greatly enhance the program in future years.

> "We can no longer be complacent when it comes to securing our critical infrastructure. We must take all steps necessary to ensure our nation's cyber preparedness and resilience. In doing so, it is essential that our state and local government partners are similarly well-situated to respond to these threats."
>
> *- Rep. Andrew Garbarino*

Meeting recording:
https://www.youtube.com/watch?v=80t-o4Sa5TM

Additional Cybersecurity Funding Opportunities

Homeland Security Grant Programs

Provides funding for the execution of the Prevention, Protection, Mitigation, Response, and Recovery mission areas and the realization of a secure and resilient Nation.

National priority areas include:

- Enhancing the protection of soft targets/crowded places
- Enhancing information and intelligence sharing and analysis
- Combating domestic violent extremism
- Enhancing cybersecurity
- Enhancing community preparedness and resilience
- Enhancing election security

Programs Include:

- State Homeland Security Program (SHSP)
- Tribal Homeland Security Program (THSGP)
- Urban Areas Security Initiative (UASI)
- Operation Stonegarden Grant Program (OPSG)
- Nonprofit Security Grant Program (NSGP)
- Transit Security Grant Program (TSGP)
- Port Security Grant Program (PSGP)

HAVA Election Security Funds

The **Help America Vote Act (HAVA)** grant program provides states with funds aimed at enhancing election technology and making election security improvements, including cybersecurity.

Funds are awarded to states every two years and local governments apply for funds through the state.

Allocated funds are significantly increased during Presidential election years.



Deadline

States were to apply for funds bi-annually. Local deadlines will vary.

Eligibility

Funds are allocated to U.S. states and territories based on the voting age population formula. States then sub-award funds to eligible recipients.

Additional Funding Areas

Utilities

Grid Resilience State and Tribal Formula Grant

Public Works and Economic Adjustment Assistance

Community Facilities Grant Program

WaterSmart Grant Programs

Transportation

Advanced Transportation Technology and Innovation Program (ATTAIN)

Better Utilizing Investments to Leverage Development (BUILD) Grant Program

Port Security Grant Program (PSGP)

Transit Security Grant Program (TSGP)

Criminal Justice

Edward Byrne Memorial Justice Assistance Grant (JAG)

STOP Violence Against Women Act (VAWA)

Improving Criminal Justice Response (ICJR)

Funding Cybersecurity for K-12

Sources of Cybersecurity Funding

FCC Schools & Libraries Cyber Pilot

State & Local Cybersecurity Grant Program (SLCGP)

State Homeland Security Program (SHSP)*

Emergency Management Performance Grant (EMPG)*

Nonprofit Security Grant Program (NSGP)

Key Points in K-12 Cybersecurity

Piece of mission-driven project

What are your project's needs and goals?

How is cybersecurity going to fit into those needs and goals?

What is the school's current cybersecurity status?

Are there any identified risks?

&

Contributes to student learning

How is cybersecurity going to benefit the education of students?

Will it contribute toward remote or hybrid learning efforts?

Will there be a possible career pathway opportunity?

Can it enhance dual enrollment initiatives?

K-12 Funding Examples for Cybersecurity

1

Distance Learning & Telemedicine (DLT)

Provides distance learning opportunities for rural K-12 schools in conjunction with colleges/universities

Cybersecurity component included to protect student and educators learning online

2

Title IV-B: 21st Century Community Learning Centers

Advancing technical education programs through extended learning time opportunities for low-income schools

Cybersecurity is allowable if it contributes towards after-school programs (i.e., after-school cybersecurity program)

3

Title V: Perkins Career & Technical Education

Implements career pathway programs in CTE

Cybersecurity career pathway justifies the cost of solutions with the added benefit of educating students

Justifying Your Cybersecurity Needs

How Grants Fund Cybersecurity

Cybersecurity Focused Grants

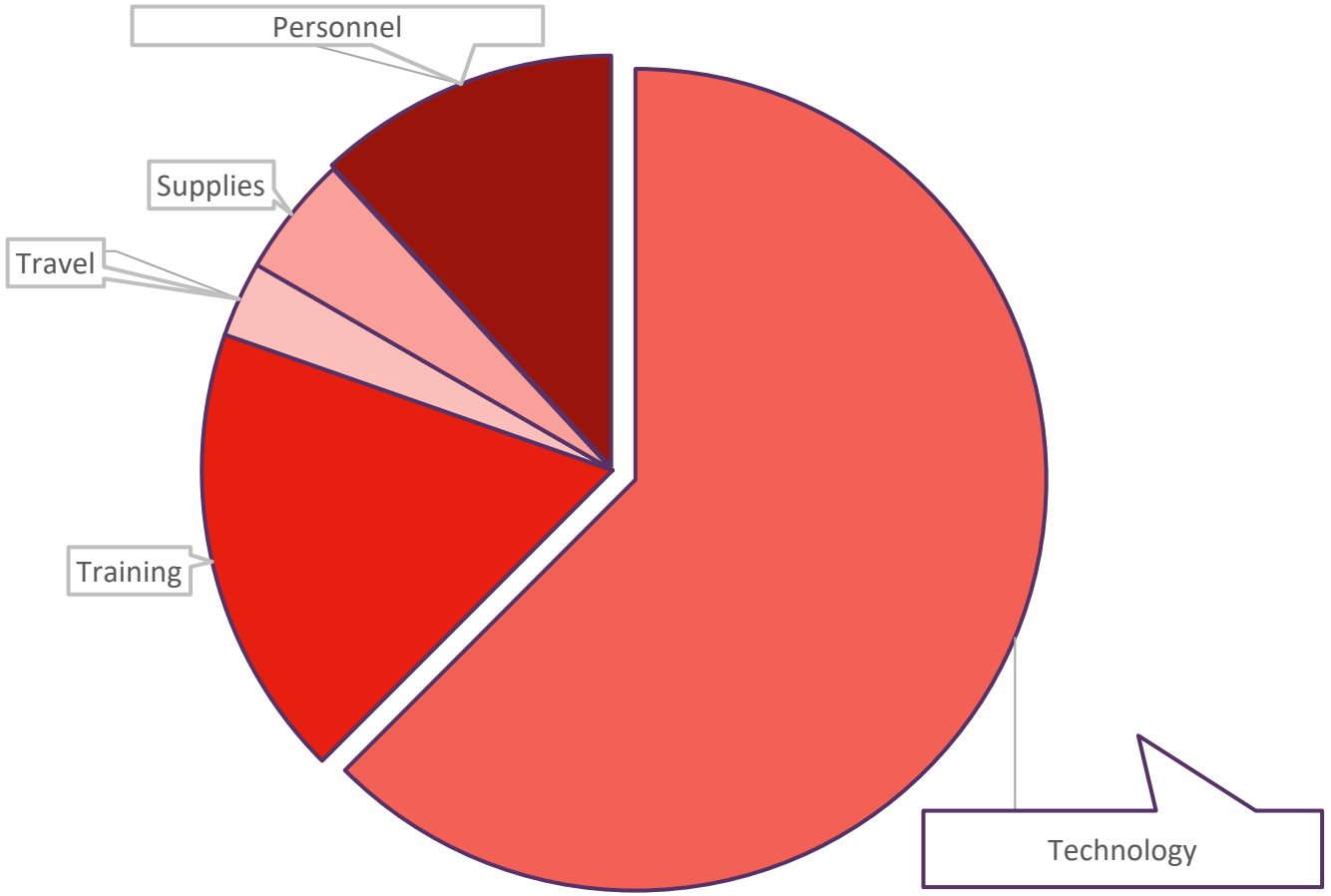
Funding designed exclusively to support the purchase of cybersecurity hardware, software, and training.

VS

Cybersecurity Friendly Grants

Funding that includes grants for cybersecurity as a component of a broader project.

Sample Cybersecurity Project Budget Breakdown



Emphasizing overall social benefits, in addition to desired cybersecurity needs

Tips to Justify Cybersecurity in Grants



Start with your needs

Think about the PROBLEM cybersecurity will help you address.

Think about additional needs to make your project successful

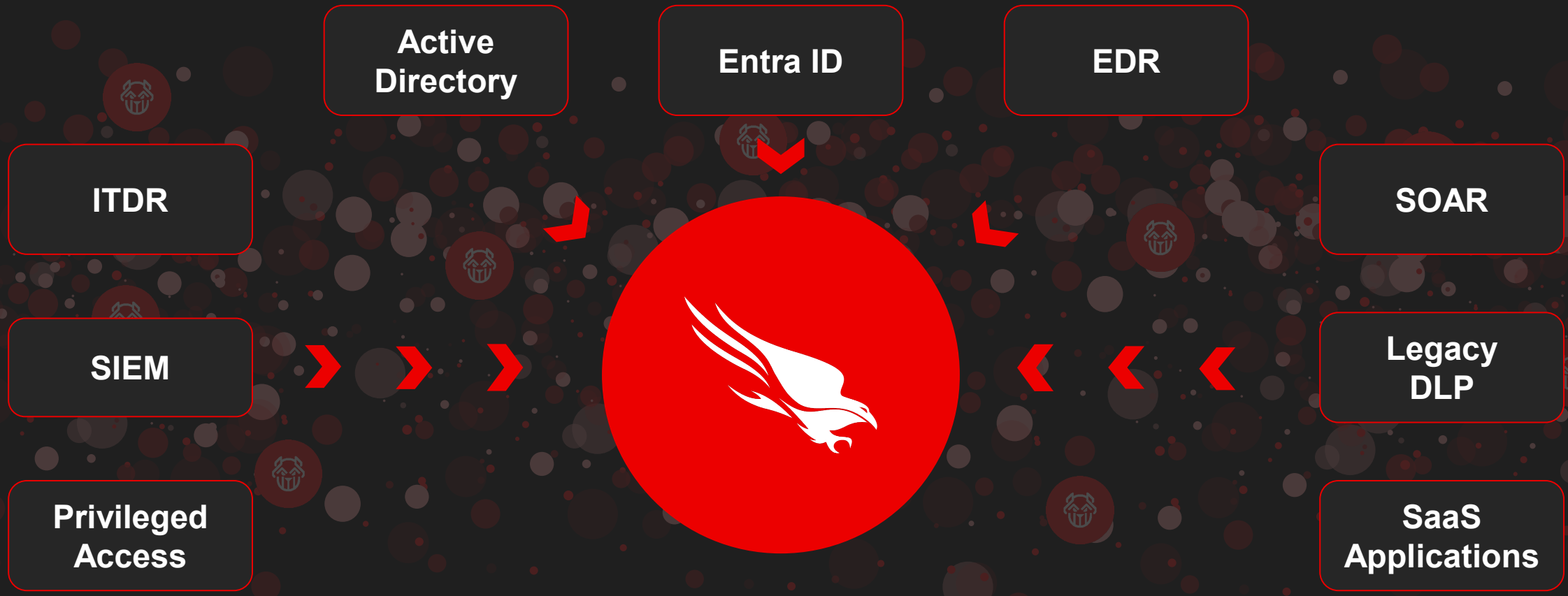
What other activities will your proposal include to ensure a successful and grant-funded project?

Include vendors and IT staff

Vendor quotes help build out your budget and product notes help provide language for budget narrative.

CrowdStrike Solutions

Adversaries Live in the Gaps Between Siloed Tools



One Platform. One Agent. One Console.

CROWDSTRIKE

2025 CrowdStrike, Inc. All rights reserved.

Outpace and outsmart the adversary

With the modern endpoint security leader



- Complete visibility — Track and stop the adversary
- AI-powered prevention and detection — Stop advanced attacks with world-class AI
- Unified investigations — Build comprehensive picture of an attack
- Integrated response — Respond rapidly with surgical precision
- Easy to deploy and operate — Deploy with ease, defend with confidence

Delivered via One Agent

® CrowdStrike, Inc. All Rights Reserved

Track and Stop the Adversary with Complete Visibility

Unified EDR and XDR

See More

Answer the most critical questions at-a-glance with full endpoint activity detail to explore the entire attack

Know More

Get deep adversary and threat understanding - enriched detections and full context at your fingertips

Do More

Extend visibility enterprise-wide with one easy-to-use unified command console

Key native telemetry



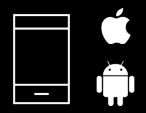
Endpoint



Identity



Cloud



Mobile



Data

® CrowdStrike, Inc. All Rights Reserved

All Falcon Insight XDR customers:
10GB per day of free third-party data ingest



100+

one-click connectors
with parsers

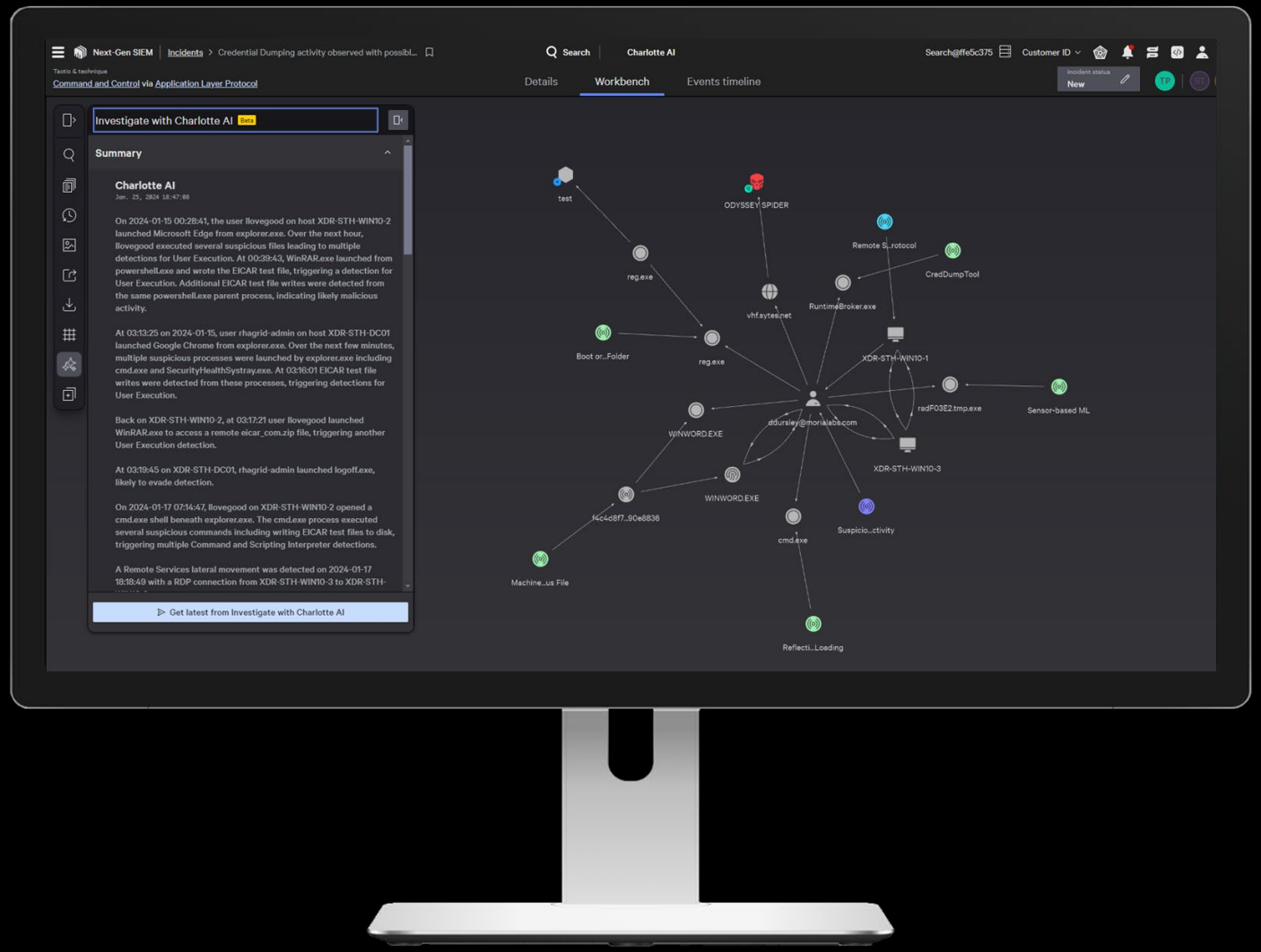
Robust Partner Ecosystem

ExtraHop · mimecast · zscaler · PingIdentity
CLOUDFLARE · VECTRA · MENLO SECURITY · okta
FORGEROCK · Skyhigh Security · proofpoint · CISCO
corelight · FORTINET · THREAT WARRIOR · servicenow
CLAROTY · Google Cloud · ARMIS · Abnormal
netskope · Cribl · zeek · ...and more!

® CrowdStrike, Inc. All Rights Reserved

Unify investigations with a single command console

Build a comprehensive picture of attacks



Accelerate security operations across the Falcon platform

Rapid investigation

Instantly pivot from detections to search with easy AI-powered workflows

Complete understanding

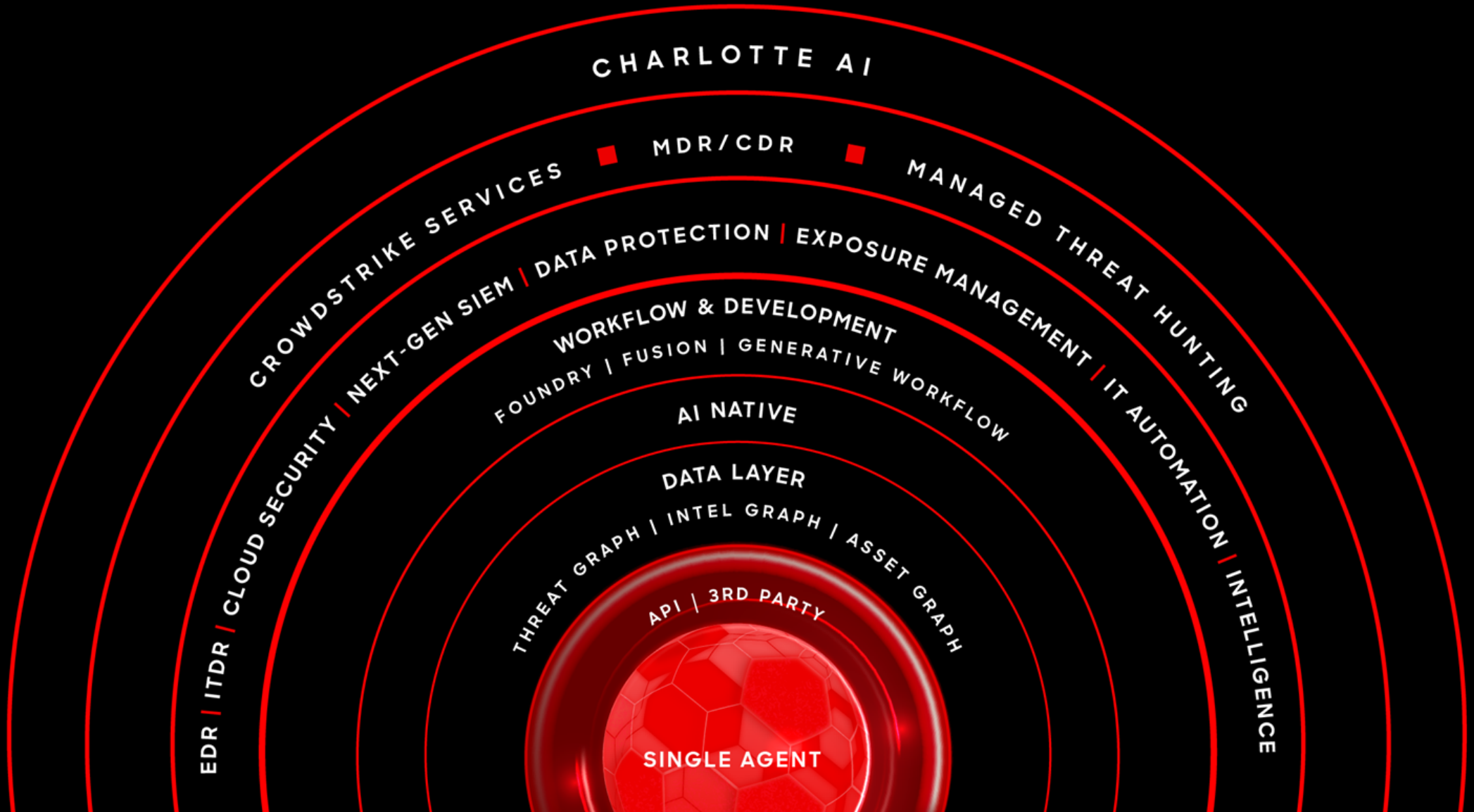
Visualize the full attack path and explore other potentially impacted hosts

Full context

Integrated view with all related threat intel, context and artifact relationships

® CrowdStrike, Inc. All Rights Reserved

Stop breaches with the AI-native Falcon platform



Complimentary CrowdStrike Security Reviews

Identity Security Risk Review

Get visibility into your current Microsoft Entra ID and AD environments to identify vulnerabilities, misconfigurations and potential attack paths

Cloud Security Risk Review

Get instant visibility into the risks facing your cloud estate with a lightweight security review

SaaS Risk Review

Assess your current SaaS security posture to uncover misconfigurations and critical security gaps

CROWDSTRIKE



THANK YOU

® CrowdStrike, Inc. All Rights Reserved

Questions?

GRANTS OFFICE
empowering communities

Contact Us

grantsoffice.com

helpdesk@grantsoffice.com

CROWDSTRIKE