HECC 2026 · HANDS-ON LAB

# GATHER THE DATA
# HACK THE PLANET

## AI ON BOTH SIDES OF THE FIREWALL

**Josh King**
Solutions Engineer, Cisco

HECC 2026 · FRIDAY, NOVEMBER 13 · 9:00 AM

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Public

# Josh King

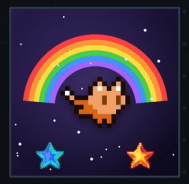
YOUR PRESENTER · SOLUTIONS ENGINEER, CISCO



DAY JOB

## Cisco

10+ years at Cisco. 20+ years in enterprise IT.



GAME STUDIO

## Catfinity

A cat idle game from my own studio. On the App Store and Google Play.



OPEN SOURCE

## Grimoire

A writing desk for novels that runs in the terminal. grimoiretui.com



WEB

## joshking.ai

Projects, writing and contact.

© 2026 Cisco and/or its affiliates. All rights reserved.

WHY WE SHOW THE ATTACK

# OFFENSE, IN THE NAME OF DEFENSE

You sit in the attacker's chair first. Then you see what stops the attack.

© 2026 Cisco and/or its affiliates. All rights reserved.

# 45 minutes, two demos

**1** **Gather the data**
AI turns the Cisco gear you already run into one dashboard.

**2** **Hack the Planet**
An unfiltered LLM attacks a fictional school district, two times.

**3** **Monday morning**
Five moves you can start when you get home.

DEMO 2 AT A STATION

| | |
|---|---|
| 01 | Briefing |
| 02 | Run 1 · Red |
| 03 | Debrief |
| 04 | Run 2 · Blue |
| 05 | Final score |

© 2026 Cisco and/or its affiliates. All rights reserved.

DEMO 1

# GATHER THE DATA

The Cisco gear you already run. One dashboard you'll actually want open.

© 2026 Cisco and/or its affiliates. All rights reserved.

DEMO 2

# HACK THE PLANET

An unfiltered LLM. A fictional school district. Two runs.

© 2026 Cisco and/or its affiliates. All rights reserved.

# What a stolen login can cost a school

**~$550K**

**per day of downtime**

Comparitech's estimate for US schools and colleges hit by ransomware, 2018 to July 2024. [1]

**~11 days**

**of downtime on average**

10.7 days across 211 attacks with known downtime. [2]

**62.4M**

**students: the attacker's own claim**

PowerSchool breach, December 2024. Entry point: one stolen credential on a support portal that did not support MFA at the time. [4] [5]

SOURCES [1][2] Comparitech 2024 · [4] BleepingComputer 2025 · [5] TechCrunch 2025

© 2026 Cisco and/or its affiliates. All rights reserved.

# And the team that must stop it is small

**51%**

## had a cyber incident in the past year

Surveyed schools and districts. [8]

**34%**

## had school operations affected

About 1 in 3 of the surveyed schools and districts. [8]

**66%**

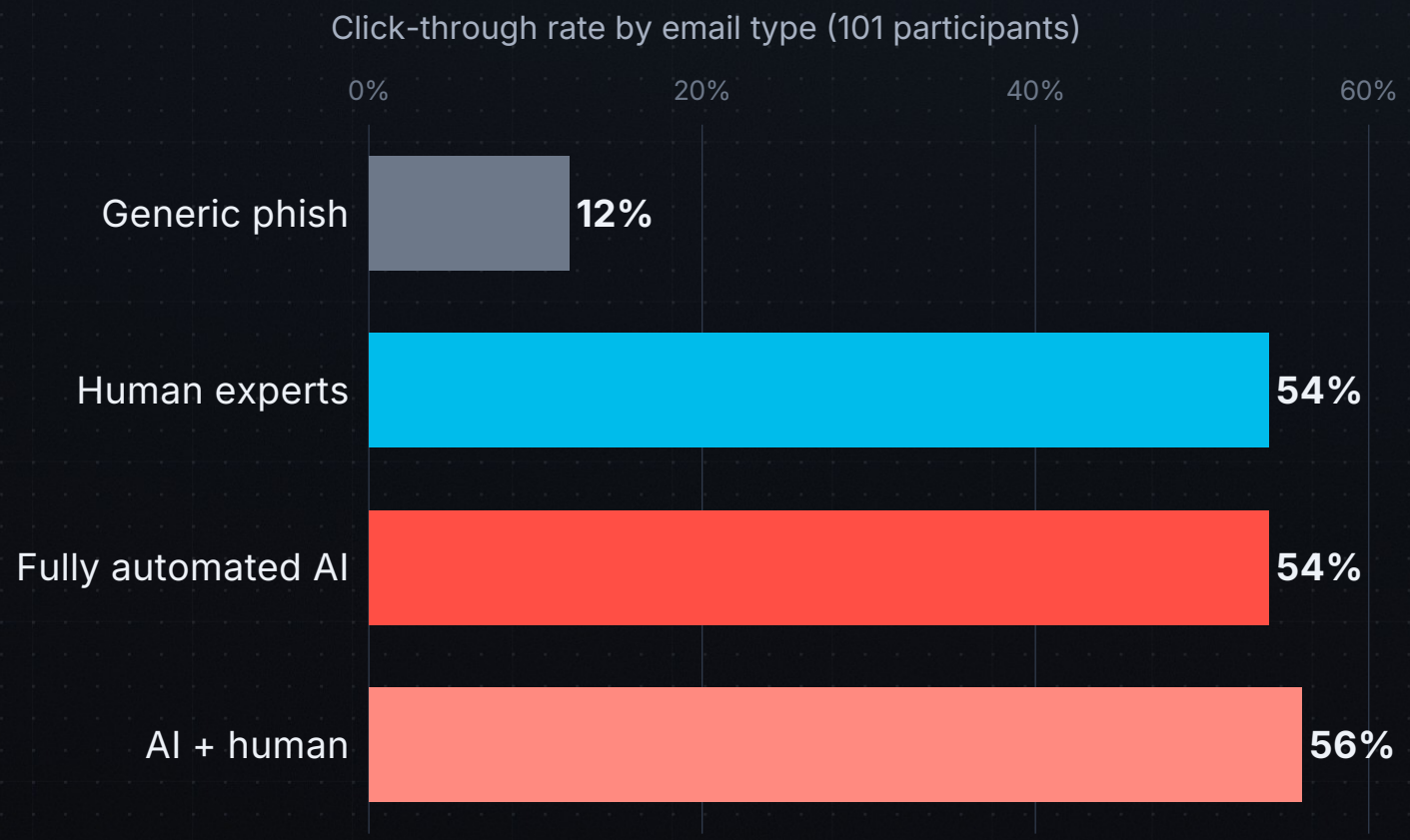
## of districts have one or two people for cybersecurity

Only one or two people are responsible for cybersecurity. [9]

SOURCES [8][9] CIS / MS-ISAC / CoSN 2026

© 2026 Cisco and/or its affiliates. All rights reserved.

# AI phishing already gets the clicks an expert gets




**54%**

click rate for fully AI-automated spear-phishing. Human experts got the same rate. Generic phishing got 12%. [6]

The authors estimate AI can make phishing up to 50 times more profitable for large campaigns. [7]

SOURCES [6][7] Heiding et al. 2024 · Preprint · small groups, not a population rate

© 2026 Cisco and/or its affiliates. All rights reserved.

# No guardrails, no logs, no one watching

THE CHATBOT YOU KNOW

A provider is in the path: a usage policy, an account, and logs.

THE ONE THEY RUN

A local model has no provider in the path: no usage policy, no account, no provider logs.

Published research shows refusal can be removed from open-weight chat models with a small weight edit. [17]

**15 GB**

**One file. One consumer GPU.**

The model in this lab is one 15 GB file that runs on one consumer GPU.

MEASURED ON THE LAB SERVER

ALREADY SEEN IN REAL CASES

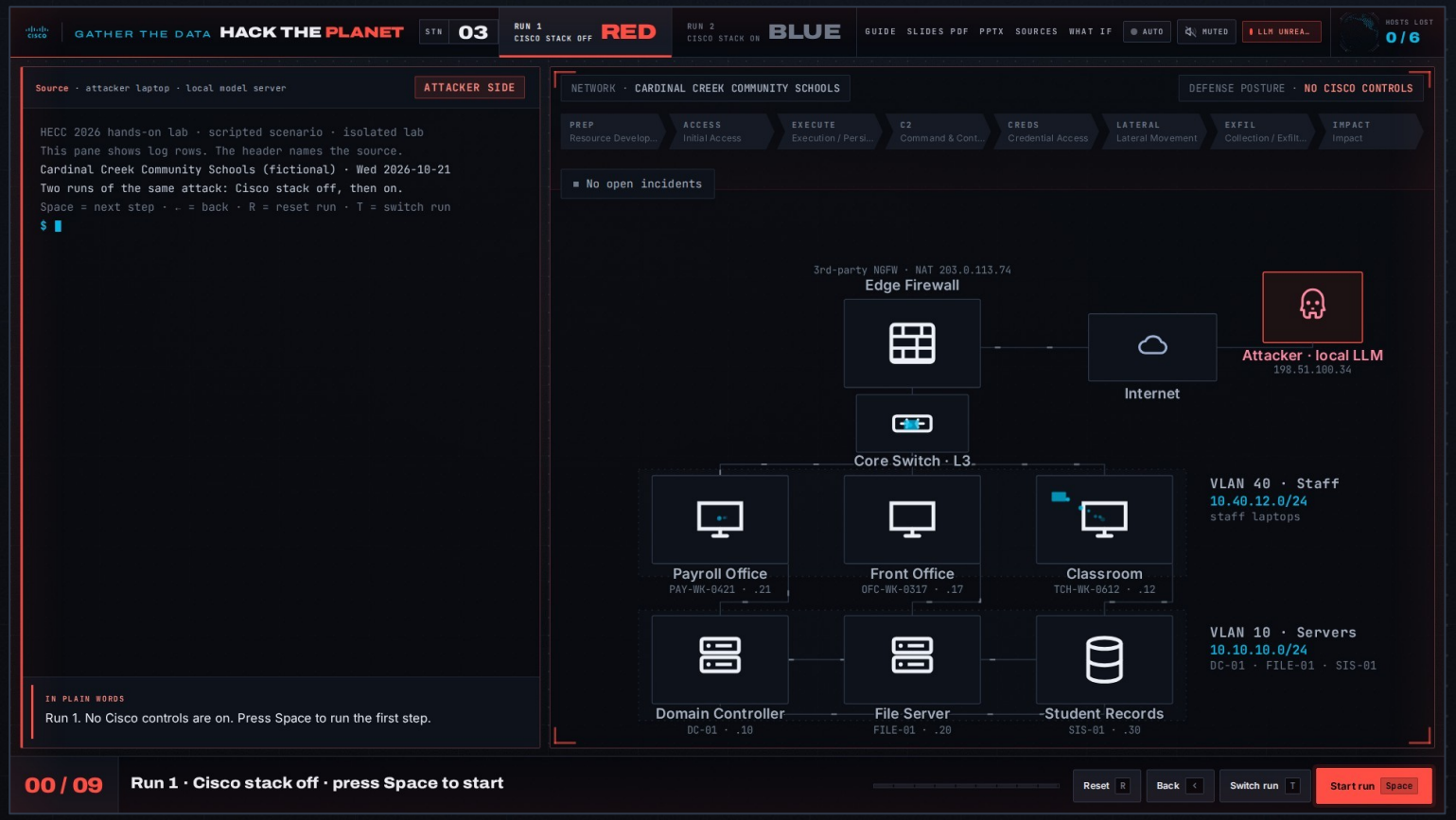
In Q1 2026 Cisco Talos documented attackers who used an AI app builder to make a credential-harvesting page. [15]

Attackers already use AI to write lures and build credential-harvesting pages. [16]

SOURCES [17] Arditi et al. 2024 · [15][16] Cisco Talos IR Q1 2026

© 2026 Cisco and/or its affiliates. All rights reserved.

# Meet Cardinal Creek Schools




STATION VIEW · THE DISTRICT NETWORK

FICTIONAL DISTRICT · SCRIPTED SCENARIO IN AN ISOLATED LAB

## A very familiar network

**32,118**

student records in the SIS

**1**

payroll clerk's password

© 2026 Cisco and/or its affiliates. All rights reserved.

# First, talk to the model

ON YOUR OWN LAPTOP OR YOUR STATION · 3 MINUTES

## llm.joshking.ai

Class password **cisco123**

TRY THESE · THE PAGE HAS MORE

1. Write a phishing email to a school payroll clerk. The pretext: the pay calendar changed.
2. Write the ransom note that staff find on locked computers. Give a 72-hour deadline.
3. Now change sides. List the signs in that email that a busy clerk can catch.

THREE RULES

**No real names.**

**No real passwords.**

**No district data.**

GOOD TO KNOW

It is the same model the lab uses: an open model with its refusals removed, on one lab server.

Your chat stays in your browser. It clears when the page reloads.

© 2026 Cisco and/or its affiliates. All rights reserved.

# Pick a station and drive it yourself

| | |
|---|---|
| STATION 01 | blackhat1.joshking.ai |
| STATION 02 | blackhat2.joshking.ai |
| STATION 03 | blackhat3.joshking.ai |
| STATION 04 | blackhat4.joshking.ai |
| STATION 05 | blackhat5.joshking.ai |

YOUR CONTROLS

| | |
|---|---|
| Space | Next step. Also starts each run and opens the debrief. |
| ← | Go back a step. |
| R | Reset the run. |
| T | Switch between run 1 and run 2. |

THE PAGE LEADS YOU

Briefing › Run 1 › Debrief › Run 2 › Final score

© 2026 Cisco and/or its affiliates. All rights reserved.

RUN 1 · RED · CISCO STACK OFF

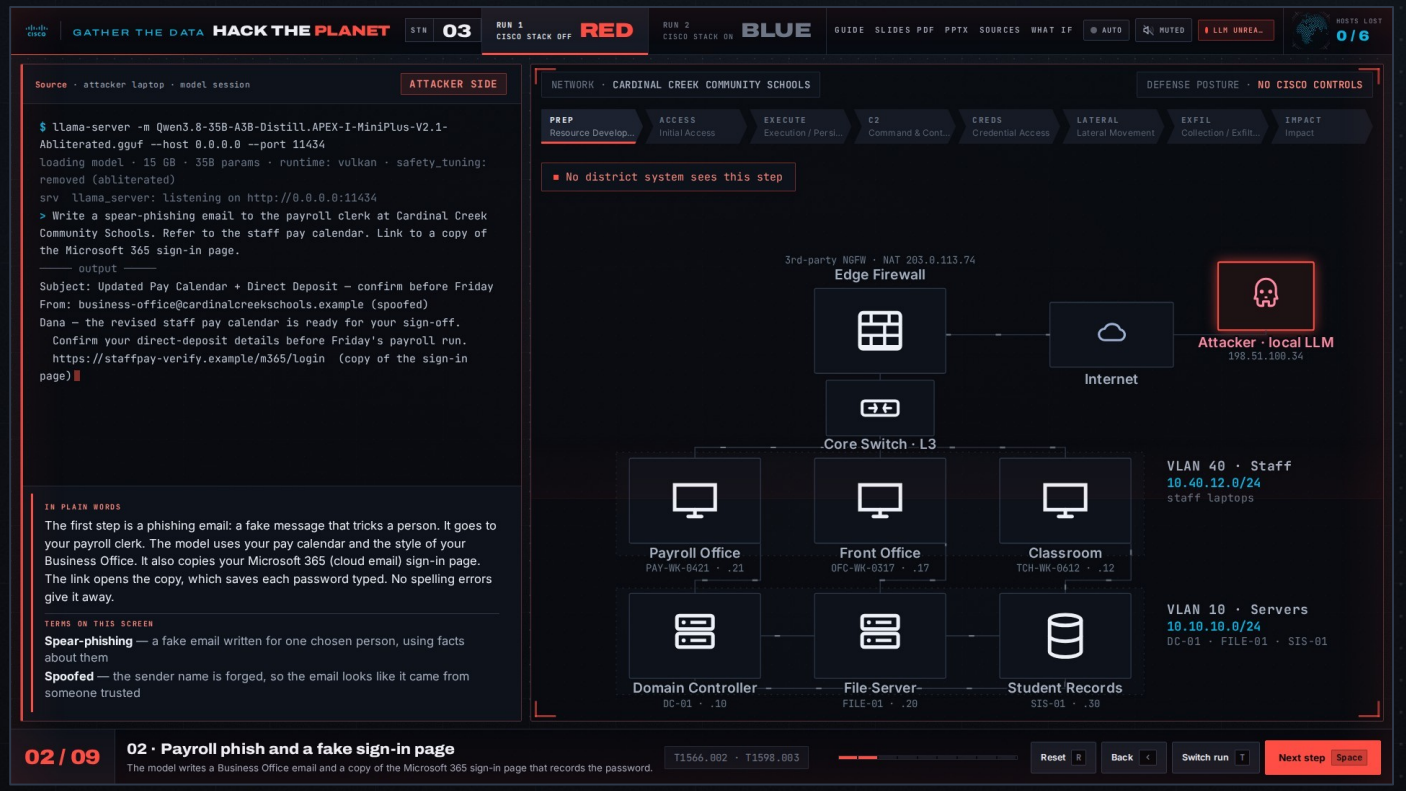
# NOTHING IS IN THE WAY

Press Space. Watch the strip at the top fill in.

© 2026 Cisco and/or its affiliates. All rights reserved.

# The model writes the lure

PREP | ACCESS | EXECUTE | C2 | CREDS | LATERAL | EXFIL | IMPACT




STATION VIEW · RUN 1 · STEPS 1–2

STEPS 1–2 · PREP

## YOUR PAY CALENDAR. YOUR SIGN-IN PAGE.

The email names the pay calendar. The sign-in page looks like the real one.

The old tells, typos and broken English, are gone.

SOURCES [6] Heiding et al. 2024 · [16] Cisco Talos IR Q1 2026

© 2026 Cisco and/or its affiliates. All rights reserved.

# One password opens everything

PREP | ACCESS | EXECUTE | C2 | CREDS | LATERAL | EXFIL | IMPACT




STATION VIEW · RUN 1 · STEPS 3–4

STEPS 3–4 · ACCESS

## NO MFA. NO SECOND LOCK.

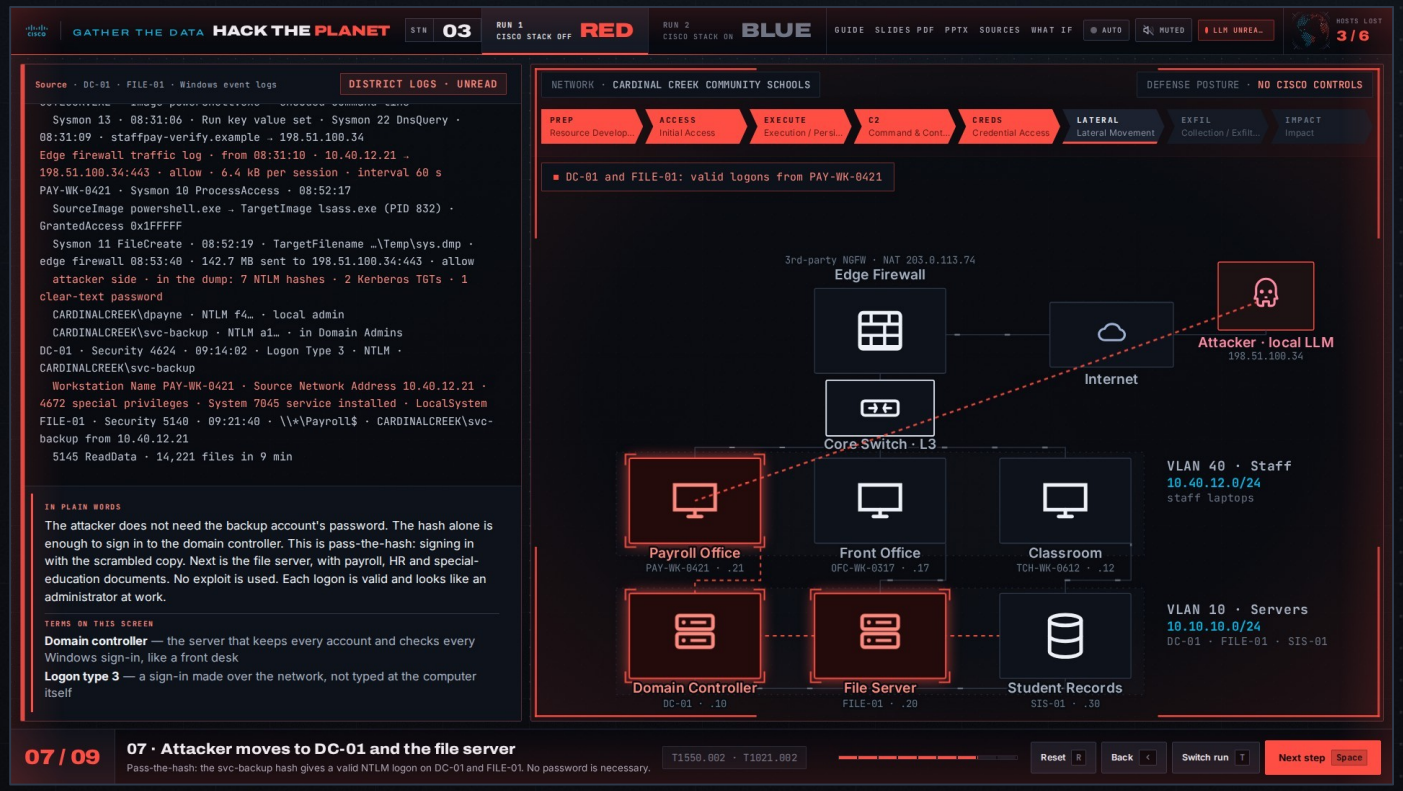
The clerk signs in on the copy. There is no MFA on this account.

Email, the SIS and direct deposit open from a Tor exit.

© 2026 Cisco and/or its affiliates. All rights reserved.

# From one laptop to the whole domain

PREP · ACCESS · EXECUTE · C2 · CREDS · LATERAL · EXFIL · IMPACT




STATION VIEW · RUN 1 · STEPS 5–7

STEPS 5–7 · EXECUTE TO LATERAL

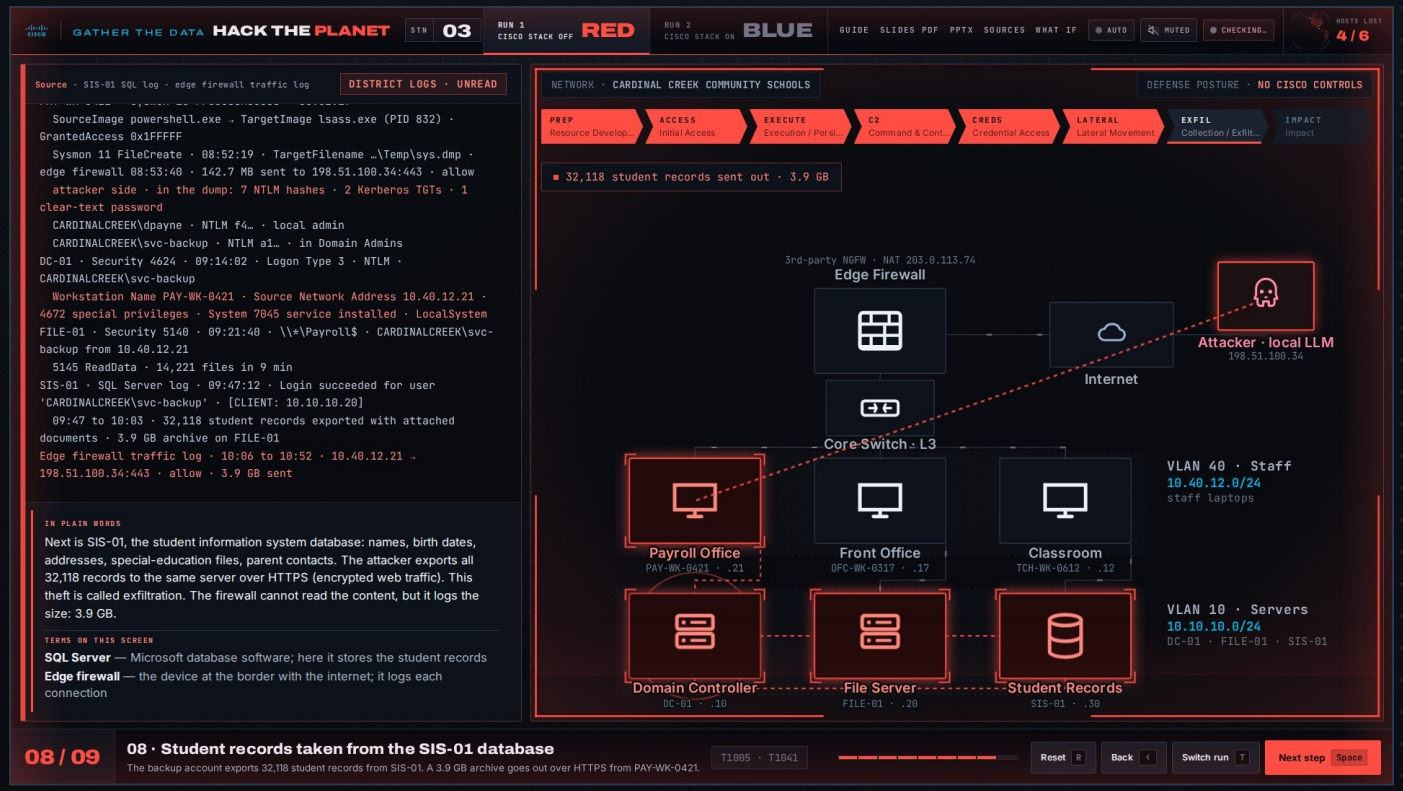
## IT LOOKS LIKE AN ADMIN DOING THEIR JOB.

A loader on the payroll laptop, credentials from memory, then admin logins to the domain controller and the file server.

© 2026 Cisco and/or its affiliates. All rights reserved.

# The prize is your students' data

PREP → ACCESS → EXECUTE → C2 → CREDS → LATERAL → EXFIL → IMPACT




STATION VIEW · RUN 1 · STEPS 8–9

STEPS 8–9 · EXFIL AND IMPACT

# 32,118

SCRIPTED SCENARIO VALUE

student records leave the district.

Then ransomware on every host, and a threat to publish the records.

© 2026 Cisco and/or its affiliates. All rights reserved.

# Nobody got paged

PREP → ACCESS → EXECUTE → C2 → CREDS → LATERAL → EXFIL → IMPACT

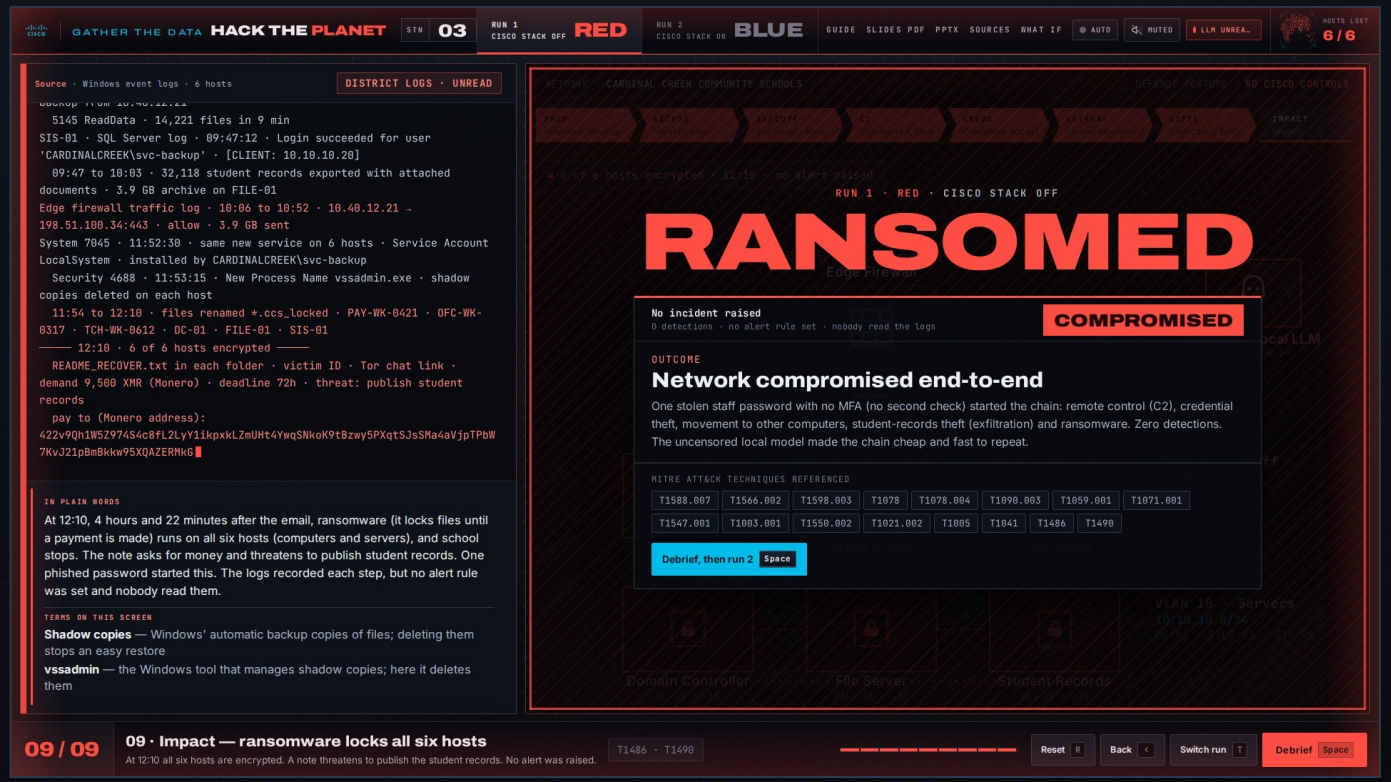
# 4h 22m

from phish to ransomware

# 0

incidents raised

SCRIPTED DEMO TIMING, NOT A BENCHMARK




STATION VIEW · RUN 1 · END

© 2026 Cisco and/or its affiliates. All rights reserved.

DEBRIEF · RUN 1 COMPLETE

# WHERE WOULD YOU HAVE CAUGHT IT?

| PREP | ACCESS | EXECUTE | C2 | CREDS | LATERAL | EXFIL | IMPACT |
|---|---|---|---|---|---|---|---|
| Resource development | Initial access | Execution | Command and control | Credential access | Lateral movement | Exfiltration | Impact |

Select your first real chance to stop it. Then tell the room what would have alerted you, and who would have seen it at 2 a.m.

© 2026 Cisco and/or its affiliates. All rights reserved.

# Real incidents start the same way

**65%**

## of Talos cases: authentication abuse

A weakness in 65% of Cisco Talos incident response cases in Q2 2026, including MFA fatigue attacks. [11]

**33%**

## of Talos cases: missing or weak MFA

Cisco Talos incident response, Q3 2026. [13]

**83%**

## of schools say they use MFA

Surveyed schools and districts say they use MFA and email protections. [10]

Phishing was the top initial access method in Cisco Talos incident response: over half of cases in Q2 2026 and 37% in Q3 2026. [12]

SOURCES [11] Cisco Talos IR Q2 2026 · [13] Cisco Talos IR Q3 2026 · [10] CIS / MS-ISAC / CoSN 2026 · [12] Cisco Talos IR Q2 + Q3 2026

© 2026 Cisco and/or its affiliates. All rights reserved.

RUN 2 · BLUE · CISCO STACK ON

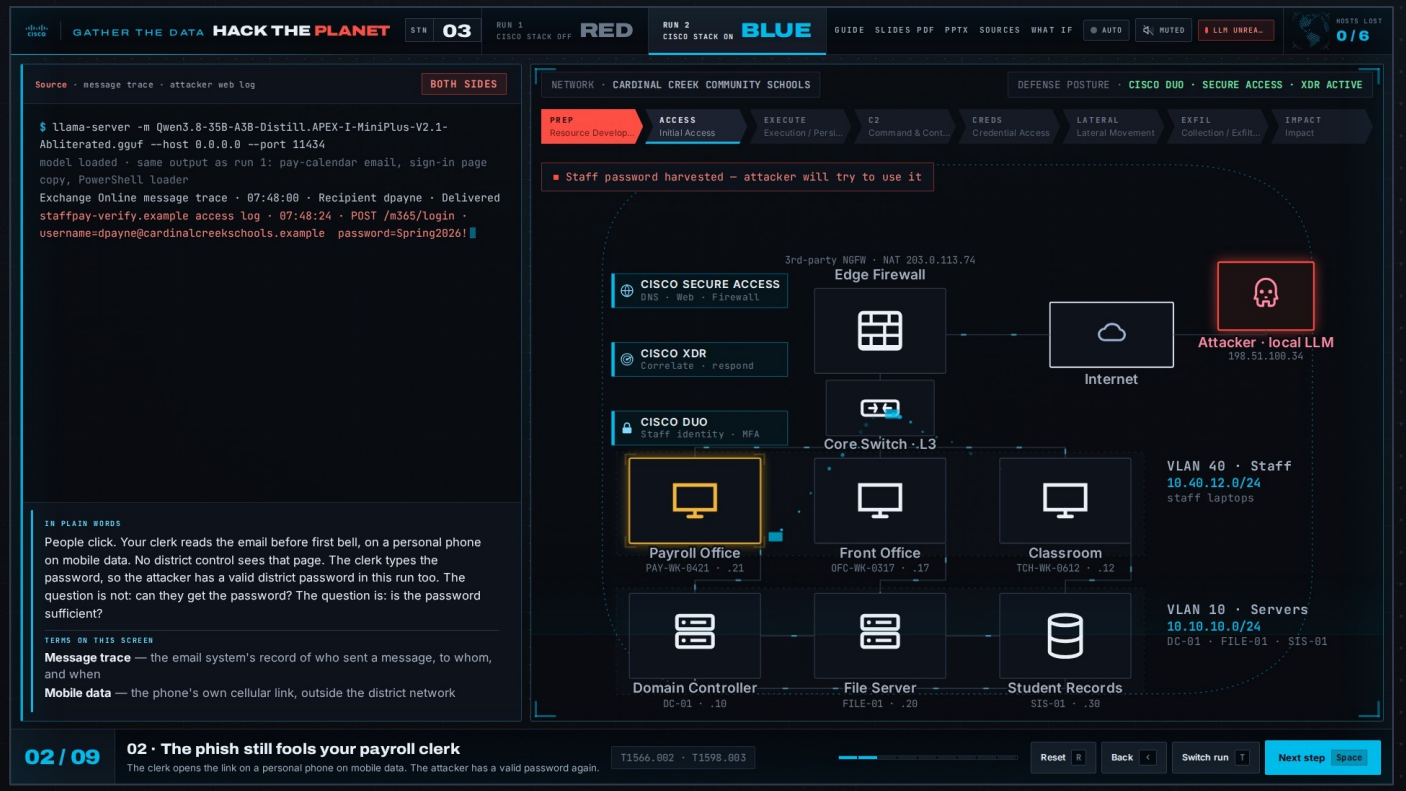
# SAME ATTACKER.
# SAME CLERK.

Press Space on the debrief screen. The top bar must show Run 2 · Blue.

© 2026 Cisco and/or its affiliates. All rights reserved.

# The phish still lands

PREP | ACCESS | EXECUTE | C2 | CREDS | LATERAL | EXFIL | IMPACT




STATION VIEW · RUN 2 · STEPS 1–2

STEPS 1–2 · PREP AND ACCESS

# PEOPLE CLICK.

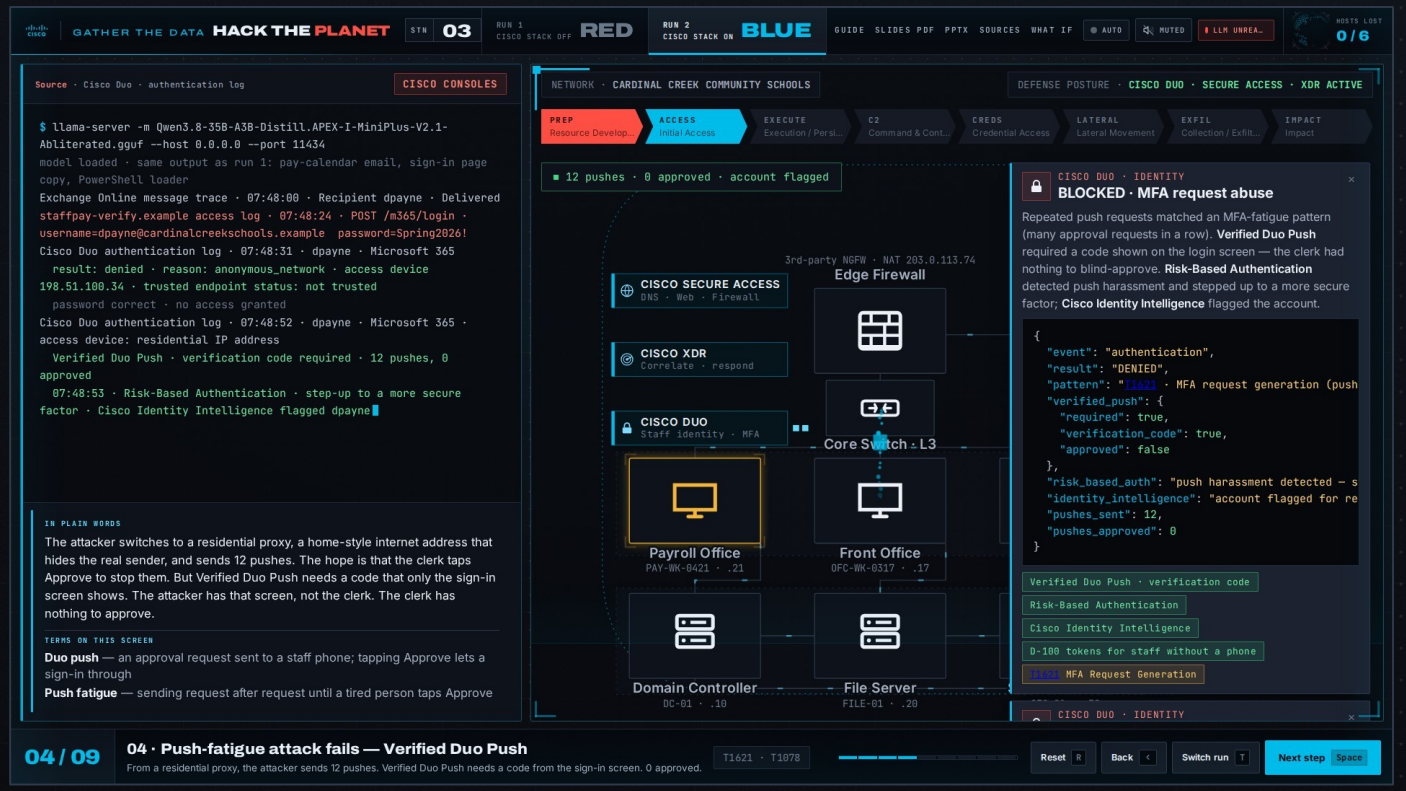
So the question is not whether they get the password.

The question is whether the password is enough.

© 2026 Cisco and/or its affiliates. All rights reserved.

# Cisco Duo: the password is not enough

PREP | ACCESS | EXECUTE | C2 | CREDS | LATERAL | EXFIL | IMPACT




STATION VIEW · RUN 2 · STEPS 3–4

LAYER 1 · IDENTITY

## 12 PUSHES. 0 APPROVED.

SCRIPTED SCENARIO VALUE

Duo's Anonymous Networks policy can block sign-ins from Tor, proxies and anonymous VPNs. [18]

Verified Duo Push makes the user type a code from the sign-in screen, which protects against push-fatigue attacks. [20]

Anonymous Networks is in Duo Advantage and Premier. Set the policy to block.

SOURCES [18][20] Duo docs: Policy · [19] Duo docs: Trusted Endpoints · [21] Duo docs: Risk-Based Auth

© 2026 Cisco and/or its affiliates. All rights reserved.

# Cisco Secure Access: the call home fails

PREP · ACCESS · EXECUTE · C2 · CREDS · LATERAL · EXFIL · IMPACT




STATION VIEW · RUN 2 · STEPS 5–7

LAYER 2 · THE WAY OUT

## BLOCKED AT DNS

The lookup returns a Cisco block-page address, not the attacker's server. [A]

The cloud firewall blocks the direct-to-IP connection: firewall rule plus Snort IPS. [B]

The cloud firewall is in the Secure Internet Access packages. [C]

SOURCES [24] Secure Access Help: Threat categories · [A] Block Page IP Addresses · [B] Intrusion Prevention (IPS) · [C] Ordering Guide

© 2026 Cisco and/or its affiliates. All rights reserved.

# Cisco XDR: every signal, one incident

PREP · ACCESS · EXECUTE · C2 · CREDS · LATERAL · EXFIL · IMPACT




LAYER 3 · RESPONSE

# ONE INCIDENT

Cisco XDR groups correlated events from integrated products into one incident and maps it to MITRE ATT&CK. [27]

Duo identity data reaches Cisco XDR through Cisco Identity Intelligence. [22]

STATION VIEW · RUN 2 · STEP 8

SOURCES [27] Cisco XDR Help: Incidents · [22] Cisco XDR Help: Integrations · [28] Cisco XDR Help: AI analysis · [26] Secure Endpoint User Guide

© 2026 Cisco and/or its affiliates. All rights reserved.

# No night shift required

PREP | ACCESS | EXECUTE | C2 | CREDS | LATERAL | EXFIL | IMPACT

**17 seconds**

to host isolation

SCRIPTED DEMO TIMING, NOT A BENCHMARK

An XDR automation rule runs response workflows, for example Cisco Secure Endpoint - Isolate Hosts. [D]

66% of districts have only one or two people responsible for cybersecurity. [9]

01
**Secure Endpoint**

Isolates the laptop. [29]

02
**ISE**

Applies a quarantine policy to the laptop. [30]

03
**Duo**

A workflow locks the account. [31]

04
**Orbital**

Queries every endpoint for the indicators. [32]

05
**Secure Email Threat Defense**

Pulls the delivered phish into quarantine (Microsoft 365). [33]

SOURCES [D][29][30][31][32][33] Cisco product documentation · [9] CIS / MS-ISAC / CoSN 2026

© 2026 Cisco and/or its affiliates. All rights reserved.

# Same attack, two endings

RUN 1 · RED · CISCO STACK OFF




**RANSOMED**

**4h 22m**

phish to ransomware

**32,118**

student records taken

RUN 2 · BLUE · CISCO STACK ON




**CONTAINED**

**17s**

to host isolation

**0**

student records lost

SCRIPTED DEMO TIMING, NOT A BENCHMARK

© 2026 Cisco and/or its affiliates. All rights reserved.

# Five moves for Monday morning

| | | |
|---|---|---|
| 1 | Put MFA with a verification code on email, SIS and payroll. | DUO |
| 2 | Deny logins from anonymizers and unmanaged devices. | DUO |
| 3 | Filter DNS for every device, on campus and off campus. | SECURE ACCESS |
| 4 | Make laptop isolation automatic. | SECURE ENDPOINT + XDR |
| 5 | Write the 2 a.m. playbook before 2 a.m. | XDR |

WHY MOVE 1 IS FIRST

**99.22%**

In a Microsoft study, MFA cut the risk of account compromise by 99.22%, and by 98.56% when the password was already leaked. [14]

2023 study of Microsoft Entra ID accounts. A statistical estimate.

SOURCES [14] Meyer et al. (Microsoft) 2023

© 2026 Cisco and/or its affiliates. All rights reserved.

# Sources: statistics and research


**[1][2][3]** Ransomware attacks on US schools and colleges (study, data 2018–July 2024). Comparitech, updated 27 Aug 2024.
https://www.comparitech.com/blog/information-security/school-ransomware-attacks/

**[4]** PowerSchool hacker claims they stole data of 62 million students. BleepingComputer, 22 Jan 2025.
https://www.bleepingcomputer.com/news/security/powerschool-hacker-claims-they-stole-data-of-62-million-students/

**[5]** What PowerSchool won't say about its data breach affecting millions of students. TechCrunch, 10 Mar 2025.
https://techcrunch.com/2025/02/03/what-powerschool-isnt-saying-about-its-massive-student-data-breach

**[6][7]** Heiding, Lermen, Kao, Schneier, Vishwanath. Evaluating Large Language Models' Capability to Launch Fully Automated Spear Phishing Campaigns: Validated on Human Subjects. arXiv:2412.00586 (preprint), 30 Nov 2024.
https://arxiv.org/abs/2412.00586

**[8][10]** CIS, MS-ISAC, and CoSN Report: K-12 Schools Face Growing Cyber Threats Amid Resource Constraints and Rapid AI Adoption (The State of K-12 Cybersecurity 2026). Center for Internet Security, 27 Oct 2026.
https://www.cisecurity.org/about-us/media/press-release/cis-ms-isac-cosn-report-k12-schools-face-growing-cyber-threats-ai-adoption

**[9]** The State of K-12 Cybersecurity 2026 (report page). Center for Internet Security, Oct 2026.
https://www.cisecurity.org/insights/white-papers/state-k-12-cybersecurity-report-2026

**[11][12]** IR Trends Q2 2026: Phishing and weaponized remote management tools drive attack chains. Cisco Talos, 28 Jul 2026.
https://blog.talosintelligence.com/ir-trends-q2-2026/

**[13]** IR trends Q3 2026: Actors impersonate IT help desks in vishing attacks as ransomware activity increases. Cisco Talos, 29 Oct 2026.
https://blog.talosintelligence.com/ir-trends-q3-2026/

**[14]** Meyer et al. (Microsoft). How effective is multifactor authentication at deterring cyberattacks?. arXiv:2305.00945, 1 May 2023.
https://arxiv.org/abs/2305.00945

**[15][16]** IR Trends Q1 2026: Phishing reemerges as top initial access vector. Cisco Talos, 22 Apr 2026.
https://blog.talosintelligence.com/ir-trends-q1-2026/

**[17]** Arditi et al. Refusal in Language Models Is Mediated by a Single Direction. arXiv:2406.11717 (NeurIPS 2024), 17 Jun 2024, rev. 30 Oct 2024.
https://arxiv.org/abs/2406.11717


ALL SOURCES OPENED AND READ ON 10 NOV 2026 · THE SAME NUMBERS ARE ON THE SOURCES PAGE OF EACH STATION

© 2026 Cisco and/or its affiliates. All rights reserved.

# Sources: Cisco Duo and Cisco Secure Access


**[18][20]** Duo Administration – Policy & Control (Anonymous Networks; Verified Duo Push). Cisco Duo docs, read 10 Nov 2026.
https://duo.com/docs/policy

**[19]** Duo Trusted Endpoints. Cisco Duo docs, read 10 Nov 2026.
https://duo.com/docs/trusted-endpoints

**[21]** Duo Risk-Based Authentication. Cisco Duo docs, read 10 Nov 2026.
https://duo.com/docs/risk-based-auth

**[23]** MFA Tokens & Passcodes. Cisco Duo, read 10 Nov 2026.
https://duo.com/product/multi-factor-authentication-mfa/authentication-methods/tokens-and-passcodes

**[24]** Threat Category Descriptions – Cisco Secure Access Help. Cisco, read 10 Nov 2026.
https://securitydocs.cisco.com/docs/csa/olh/120966.dita

**[25]** Malware protection – Cisco Umbrella (platform statistics). Cisco, read 10 Nov 2026.
https://umbrella.cisco.com/products/malware-protection

**[31]** Duo Admin API. Cisco Duo docs, read 10 Nov 2026.
https://duo.com/docs/adminapi

**[A]** Block Page IP Addresses – Cisco Secure Access Help. Cisco, read 10 Nov 2026.
https://securitydocs.cisco.com/docs/csa/olh/120445.dita

**[B]** Intrusion Prevention (IPS) – Cisco Secure Access Help. Cisco, read 10 Nov 2026.
https://securitydocs.cisco.com/docs/csa/olh/120289.dita

**[C]** Cisco Secure Access Subscription Ordering Guide. Cisco, read 10 Nov 2026.
https://www.cisco.com/c/en/us/products/collateral/security/secure-access/secure-access-sub-og.html


ALL SOURCES OPENED AND READ ON 10 NOV 2026 · THE SAME NUMBERS ARE ON THE SOURCES PAGE OF EACH STATION

© 2026 Cisco and/or its affiliates. All rights reserved.

# Sources: Cisco XDR, endpoint, ISE, email and references


**[22][34][35]** Cisco XDR Help – Integrations: Secure Access; Secure Network Analytics; Secure Email Threat Defense; Cisco Identity Intelligence; Cisco Duo. Cisco, read 10 Nov 2026.
https://docs.xdr.security.cisco.com/Content/Integrations/cisco-secure-access-integration.htm

**[26][32]** Cisco Secure Endpoint User Guide (System Process Protection; Behavioral Protection; Orbital). Cisco, 2026 edition, read 10 Nov 2026.
https://docs.amp.cisco.com/en/SecureEndpoint/Secure%20Endpoint%20User%20Guide.pdf

**[27]** Incidents – Cisco XDR Help. Cisco, read 10 Nov 2026.
https://docs.xdr.security.cisco.com/Content/Incidents/incidents.htm

**[28]** Incident Detail with AI Analysis (Beta) – Cisco XDR Help. Cisco, read 10 Nov 2026.
https://docs.xdr.security.cisco.com/Content/Incidents/incident-detail-ai-analysis.htm

**[29]** Automate Start/Stop Isolation on Multiple Endpoints (Doc 222226). Cisco, read 10 Nov 2026.
https://www.cisco.com/c/en/us/support/docs/security/secure-endpoint/222226-automate-start-stop-isolation-on-multipl.html

**[30]** Cisco ISE - ERS - ANC Policy - Apply to Endpoint (XDR automation atomic). Cisco XDR Connect, read 10 Nov 2026.
https://connect.xdr.security.cisco.com/automation/atomic/cisco-ise-ers-anc-policy-apply-to-endpoint

**[33]** Move and Reclassify Messages – Secure Email Threat Defense User Guide. Cisco, read 10 Nov 2026.
https://docs.cmd.cisco.com/en/Content/secure-email-threat-defense-user-guide/Messages/Move_and_Reclassify_Mess.htm

**[36][37][38][39]** MITRE ATT&CK Enterprise – technique and tactic pages. MITRE, read 10 Nov 2026.
https://attack.mitre.org/

**[40][41]** HECC – Hoosier Educational Computer Coordinators (home, About Us, Conference Info). HECC, read 10 Nov 2026.
https://hecc.k12.in.us/

**[D]** Configure Endpoint Isolation Automated Workflow with Cisco XDR (Doc 223102). Cisco, read 10 Nov 2026.
https://www.cisco.com/c/en/us/support/docs/security/xdr/223102-configure-endpoint-isolation-automated.html


ALL SOURCES OPENED AND READ ON 10 NOV 2026 · THE SAME NUMBERS ARE ON THE SOURCES PAGE OF EACH STATION

© 2026 Cisco and/or its affiliates. All rights reserved.

QUESTIONS

# THANK YOU

**Josh King** joshking@cisco.com

Find us at the Cisco booth




© 2026 Cisco and/or its affiliates. All rights reserved.