
DAFITC 2026 · MONTGOMERY, AL · 24–26 AUG
SESS-236
Weaponizing Infrastructure: OT Risks & Threats
Daryl Haegley
TECHNICAL DIRECTOR · CYBER RESILIENCY OFFICE FOR CONTROL SYSTEMS
CROCS
Department of the Air Force

CROCS PRESENTS

FOUR LEVELS
NO SAVE POINT

You defend data. I defend water pressure, breaker position, runway lights.
Same adversary. Different physics. No undo button.

▶ INSERT COIN

CROCS
Department of the Air Force

LEVEL 0 · THE MAP IS ALREADY CONTESTED

AN INSTALLATION, LAST YEAR

0347	Runway lighting controller setpoint written. Valid credential. Native tool
0347	No alert. System did exactly what it was told
0512	Fuel transfer pump logic modified. Same credential
0600	A crew chief notices something looks wrong. Calls it in
0600	A human being is your intrusion detection system

There was no ticket. There was no log anyone read.

CROCS
Department of the Air Force

NOBODY GOT HACKED

NO DATA EXFILTRATED	NOTHING ENCRYPTED	NO RANSOM DEMANDED	NO MALWARE TO FIND

SOMEONE TURNED A KNOB

CROCS
Department of the Air Force

THREAT PICTURE

THEY ARE NOT STEALING
THEY ARE STAGING

METHOD

Native tools, valid credentials, no payload. Nothing for your EDR to catch

TARGET

Utility, water and power at installations home and abroad. Not data. Physics

INTENT

Asymmetric advantage. Knock out power, hamper readiness, never fire a shot

If they only wanted secrets, they would not be in a pump house

CROCS
Department of the Air Force

YOUR REFLEXES DON'T TRANSFER

IN IT, YOU…	IN OT, YOU CAN'T
Protect confidentiality first	**Safety first. Then availability. Secrecy is fourth**
Patch on Tuesday	**Patching voids your warranty. Vendor is out of business**
Reboot it and see	**You do not reboot a chiller during a sortie**
Refresh on a three-year cycle	**That controller is older than any Airman watching it**
Push an agent to every endpoint	**Endpoint has no room for an agent, no OS to host it**
Scan your network	**An active scan can trip whatever process it scans**

Same adversary. Same tradecraft. None of your tools.

CROCS
Department of the Air Force

WHO IS TALKING

ONE FRONT DOOR

Cyber Resiliency Office for Control Systems (CROCS). Stood up 2024. First and still only service office dedicated to OT cyber

PLAN

A 100-point DAF OT cyber plan. Tracked initiative by initiative, not shelved

PEOPLE

100+ OT experts convene every month. Mission assurance, intel, ops, logistics, CE

MONEY

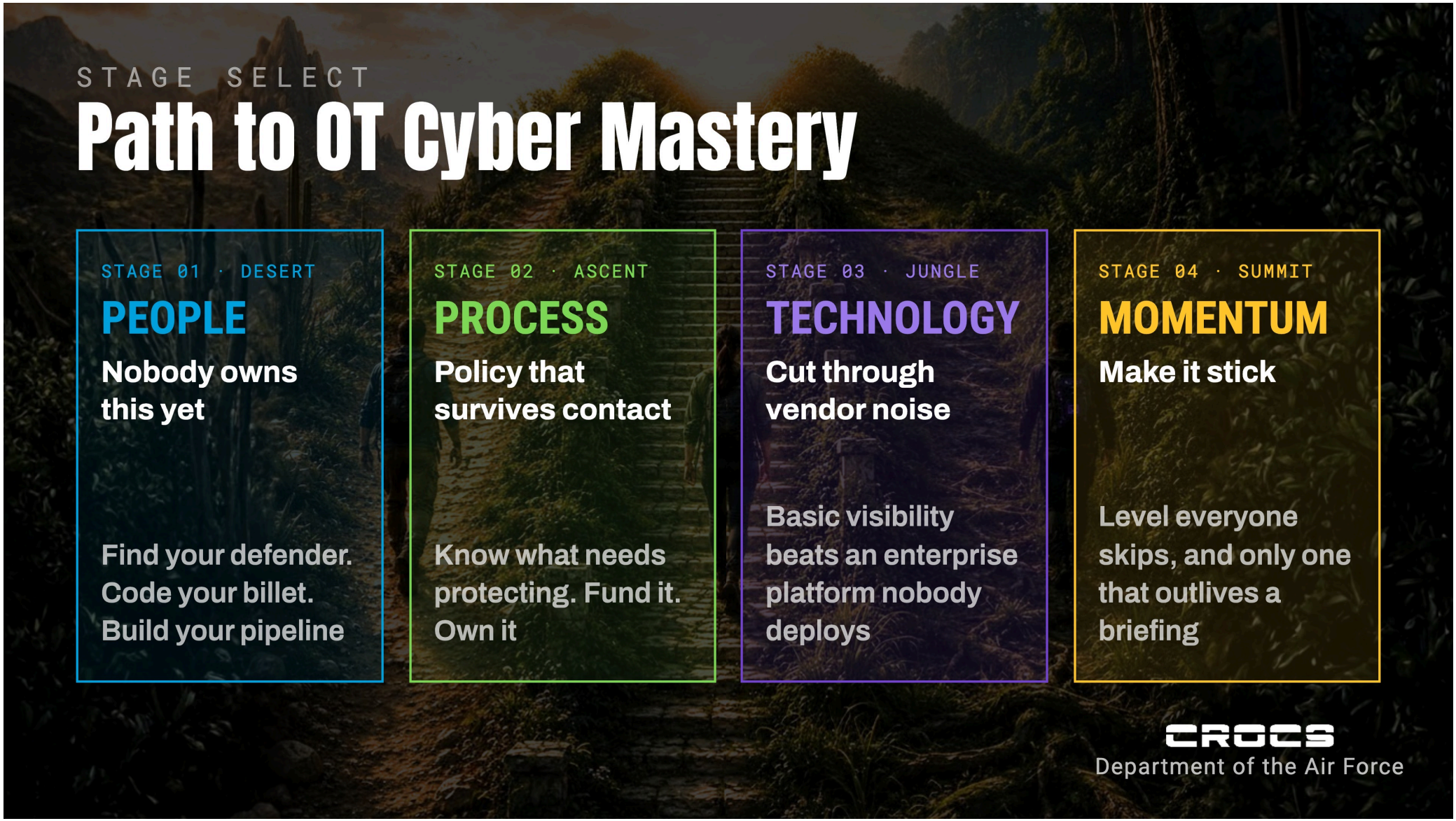
OT cyber is in POM. Assessment, mitigation and training now budget inside a program of record

SCOPE

Air Force and Space Force. Installations, infrastructure, ranges, launch

MODELED ON CROWS (WEAPON SYSTEMS, 2017)
TWO YEARS TO PROVE IT WAS NEEDED

CROCS
Department of the Air Force


STAGE SELECT
Path to OT Cyber Mastery
STAGE 01 · DESERT
PEOPLE
Nobody owns this yet
Find your defender. Code your billet. Build your pipeline
STAGE 02 · ASCENT
PROCESS
Policy that survives contact
Know what needs protecting. Fund it. Own it
STAGE 03 · JUNGLE
TECHNOLOGY
Cut through vendor noise
Basic visibility beats an enterprise platform nobody deploys
STAGE 04 · SUMMIT
MOMENTUM
Make it stick
Level everyone skips, and only one that outlives a briefing
CROCS
Department of the Air Force

PEOPLE



TERRAIN: DESERT

CHALLENGE:

Nobody owns this yet

BEGIN PATH

CROCS

Department of the Air Force


STAGE 01 · PEOPLE
HUMAN IN THE LOOP
Someone has to read terrain when an alert comes
One defender who knows what they are looking at
CROCS
Department of the Air Force


STAGE 01 · PEOPLE
KNOW
YOUR OT WORKFORCE
They understand these systems
They are part of your team whether they know it or not
CROCS
Department of the Air Force


STAGE 01 · PEOPLE
WR 462
Only designated OT cyber role in federal workforce framework
CROCS
Department of the Air Force

STAGE 01 · PEOPLE

DCWF 462 · NICE CI-WRL-001

CONTROL SYSTEMS SECURITY SPECIALIST

"Device, equipment, and system-level cybersecurity configuration and day-to-day security operations of control systems, including security monitoring and maintenance along with stakeholder coordination to ensure the system and its interconnections are secure in support of mission operations."

NOT THIS

Cyber engineer who designs a system

NOT THIS

Facility engineer who keeps it running

THIS

Defender who watches it, and knows what a bad day looks like

Naming this role is what creates a career path

CROCS

Department of the Air Force

STAGE 01 · PEOPLE

HOW A PERSON ACTUALLY BECOMES A 462

01
CODE YOUR BILLET
Position gets 462 as its primary work role code. Nothing downstream works until this happens

02
FOUNDATIONAL QUAL
Education, training, *or* certification. One lane, not all three. 8140 gives you options

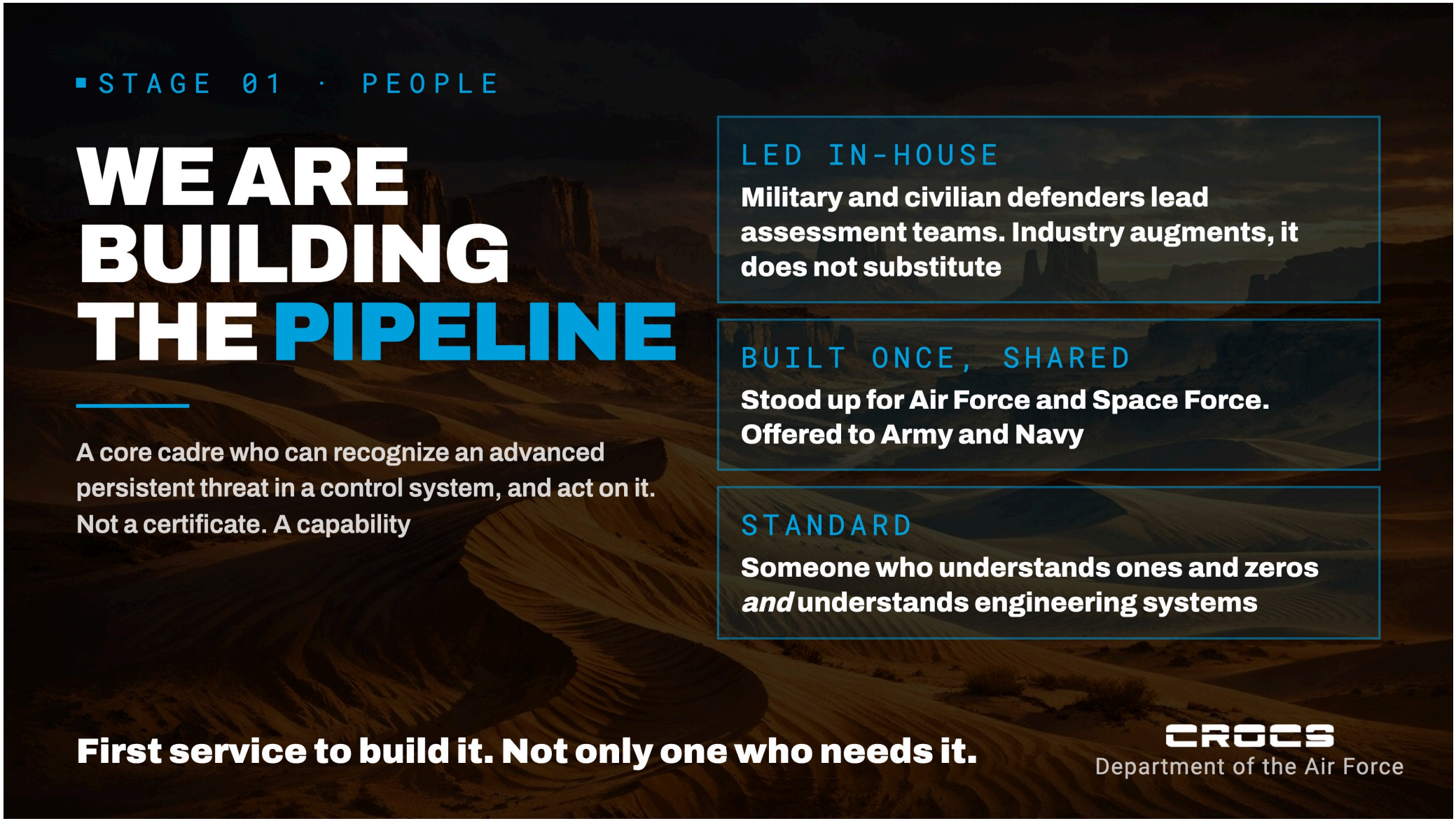
03
RESIDENTIAL QUAL
On-the-job, on a live plant. You cannot certify your way to knowing your own installation

04
SUSTAIN
Continuous professional development, reported on an annual cycle. Threat doesn't hold still

If a billet isn't coded, training doesn't get funded

DoDD 8140.01 · DoDM 8140.03

CROCS
Department of the Air Force


STAGE 01 · PEOPLE
WE ARE BUILDING THE PIPELINE
A core cadre who can recognize an advanced persistent threat in a control system, and act on it. Not a certificate. A capability
LED IN-HOUSE
Military and civilian defenders lead assessment teams. Industry augments, it does not substitute
BUILT ONCE, SHARED
Stood up for Air Force and Space Force. Offered to Army and Navy
STANDARD
Someone who understands ones and zeros *and* understands engineering systems
First service to build it. Not only one who needs it.
CROCS
Department of the Air Force

STAGE 01 · DESERT

PEOPLE CLEARED

★ ★ ★	★ ★ ★	★ ★ ★
FIND THEM	**CODE THEM**	**TRAIN THEM**
They already work for you	462, primary work role	Send them down your pipeline

▶ NEXT STAGE

CROCS
Department of the Air Force

PROCESS



TERRAIN: ASCENT

CHALLENGE:

Policy that survives contact

▶ **BEGIN PATH**

CROCS

Department of the Air Force


STAGE 02 · PROCESS
INCENTIVE
OVER
MANDATE
Funding is available for organizations
that put right technology in place
Adding cybersecurity as an unfunded requirement to an overstretched engineering shop does not work. It never has
CROCS
Department of the Air Force


STAGE 02 · PROCESS
KNOW WHAT NEEDS PROTECTING
Failure of these systems grounds a mission
You will never inventory every device on an installation. You can name five that stop a flying schedule
FUEL
WATER
POWER
LIFE SAFETY
RUNWAY LIGHTING
CROCS
Department of the Air Force


STAGE 02 · PROCESS
GOVERNANCE THAT CAN'T BE EXECUTED
DEAD END
CROCS
Department of the Air Force

STAGE 02 · PROCESS

WHAT EXECUTABLE ACTUALLY LOOKS LIKE

TEST 01

A NAMED OWNER

A person you can call. Not an office symbol, not a working group

TEST 02

A FUNDED LINE

In POM, inside a program of record. Not a favor asked of your CE shop

TEST 03

A MEASURABLE STATE

You can show me a number this quarter, and that number moved

TEST 04

ONE FRONT DOOR

One place to call when you don't know. That is what this office is for

Fail any one of these and you have written a dead end

CROCS
Department of the Air Force

STAGE 02 · ASCENT

PROCESS CLEARED

★ ★ ★

PRIORITIZE

Five systems, not forty thousand

★ ★ ★

FUND IT

Incentive beats mandate

★ ★ ★

OWN IT

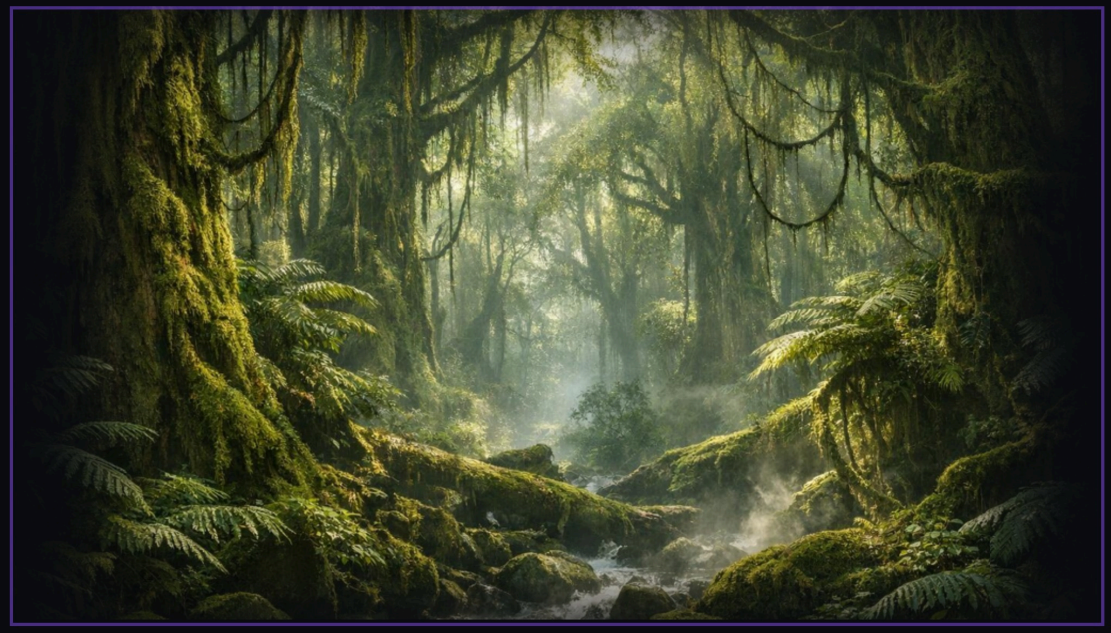
A name, not an office symbol

▶ NEXT STAGE

CROCS

Department of the Air Force

TECHNOLOGY



TERRAIN: JUNGLE

CHALLENGE:

Cut through vendor noise

BEGIN PATH

CROCS

Department of the Air Force

STAGE 03 · TECHNOLOGY

OT DATA IS NOT COMPLEX

SYSTEM READOUT	
WATER PRESSURE	42.7 PSI
TEMPERATURE	68.4 °F
VALVE POSITION	OPEN
SENSOR STATUS	NOMINAL
FLOW RATE	12.3 GPM

YOU DO NOT NEED ENTERPRISE-SCALE AI TO READ THIS

YOU DO NEED TO KNOW WHEN SOMETHING CHANGES

CROCS
Department of the Air Force

STAGE 03 · TECHNOLOGY

WHAT'S AVAILABLE



$$$$$

BUILT FOR ENTERPRISE IT

WHAT OT NEEDS



BASIC VISIBILITY
THREAT DETECTION

THIS TECHNOLOGY JUNGLE LOOKS LIKE IT NEEDS A MACHINE
MOST OF IT NEEDS A MACHETE

CROCS
Department of the Air Force

STAGE 03 · TECHNOLOGY

BASIC VISIBILITY

ZERO TRUST

In that order. You cannot zero-trust a network you have never seen

CROCS
Department of the Air Force

STAGE 03 · TECHNOLOGY

THIS ALREADY HAPPENED

WHERE ZERO TRUST GOT TESTED

COLONIAL PIPELINE · 2021

MISSING SEGMENTATION

A flat network let an IT-side ransomware hit force an OT shutdown. TSA now mandates an enforced boundary between the two

NORSK HYDRO · 2019

DENY BY DEFAULT

Rebuilt after ransomware into segmented zones that deny by default, not a perimeter you trust once you're inside

OLDSMAR, FL · 2021

VERIFY EVERY SESSION

One shared remote-access login, no MFA, gave an outsider the chemical dosing controls. Identity now gets checked per session, not once

Not a framework on a slide. The gap between an incident and an outage.

CROCS

Department of the Air Force

STAGE 03 · TECHNOLOGY

TO VENDORS IN THIS ROOM

WHAT WE WILL ACTUALLY BUY

01 **PASSIVE FIRST**
If it can trip a process, it does not come on base

02 **SPEAKS YOUR LANGUAGE**
Modbus, DNP3, BACnet, LonWorks. Not just TCP and syslog

03 **NO AGENT REQUIRED**
Endpoint is a controller from two decades ago. It has no room for you

04 **WORKS DISCONNECTED**
Contested means no cloud, no phone-home, no licence check

05 **PRICED FOR AN INSTALLATION**
Not for an enterprise. We have a lot of installations

06 **TELLS ME WHAT CHANGED**
That is your whole product. Everything else is packaging

Don't bring us an IT platform wearing an OT skin

CROCS
Department of the Air Force

STAGE 03 · JUNGLE

TECHNOLOGY CLEARED

★ ★ ★

SEE IT

Basic visibility, passively

★ ★ ★

SEGMENT IT

Keep your plant off your enterprise

★ ★ ★

TRUST NOTHING

But only after you can see

CROCS

Department of the Air Force

MOMENTUM



TERRAIN: SUMMIT

CHALLENGE:

Make it stick

▶ FINAL ASCENT

CROCS

Department of the Air Force

STAGE 04 · MOMENTUM

ROAD FROM HERE

NOW

SCAFFOLDING EXISTS

Office is standing. Role is in a framework. Plan is tracked point by point. OT cyber has a line in POM

NEXT

PIPELINE PRODUCES

Defenders coming off a line. Assessment teams led in uniform. Sister services plugging into what DAF built

AFTER

IT STOPS BEING SPECIAL

OT cyber is a line item in every program of record, same as structural loads and fire code. Nobody asks permission

Measure us by how soon you stop needing us

CROCS
Department of the Air Force

STAGE 04 · MOMENTUM

TAKE A PICTURE OF THIS ONE

MONDAY MORNING

- [ ] 01 List five systems that ground your mission if they fail
- [ ] 02 Find out who is watching them right now. Write that name down
- [ ] 03 Pull your billets. Count how many are coded 462
- [ ] 04 Ask your control-system vendor one question: what changed last night?
- [ ] 05 Call CROCS before you buy, build, or connect anything

None of this needs a budget. All of it needs a decision.

CROCS
Department of the Air Force

LEVEL COMPLETE

OT CYBER MASTERY · ALL STAGES CLEARED

★ ★ ★	★ ★ ★	★ ★ ★
VIGILANT	**VICIOUS**	**VICTORIOUS**
visibility into critical systems	willingness to act on what you find	OT security as warfighting priority

MISSION RANK S · SCORE 1500 / 1500

► PRESS START TO CONTINUE

CROCS
Department of the Air Force

PICK YOUR ROW

ASK

INSTALLATION LEADERSHIP	**Fund visibility. You cannot defend what you have never seen**
CYBER & IT	**Go meet your OT workforce this month. They are already on your team**
MANPOWER & FORCE DEV	**Code your billets 462. Then send those people down a pipeline**
PROGRAM OFFICES	**Call us before design review, not after a finding**
INDUSTRY	**Build for a pump house, not a data center**

One front door. Use it.

CROCS
Department of the Air Force


SESS-236
Weaponizing Infrastructure:
OT Risks & Threats
Daryl Haegley
TECHNICAL DIRECTOR · CYBER RESILIENCY OFFICE FOR CONTROL SYSTEMS
DAFITC 2026 · MONTGOMERY, AL
CROCS
Department of the Air Force