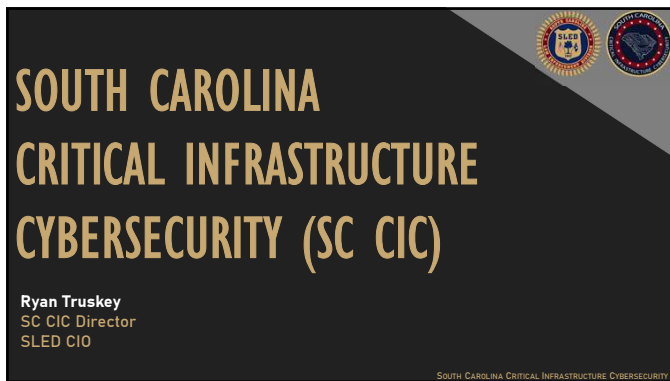
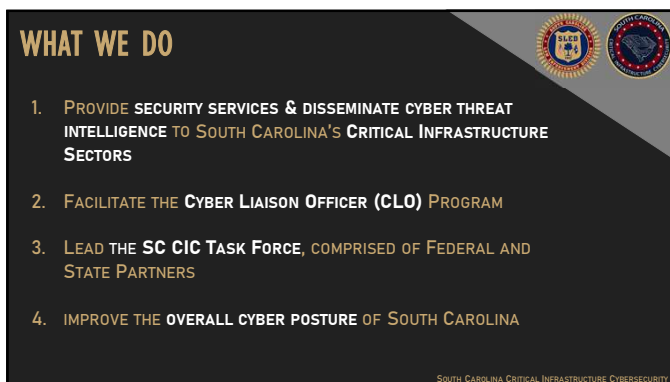


The information provided here is for informational and educational purposes and current as of the date of publication. The information is not a substitute for legal advice and does not necessarily reflect the opinion or policy position of the Municipal Association of South Carolina. Consult your attorney for advice concerning specific situations.









CYBER LIAISON OFFICER (CLO) PROGRAM

The CLO program has been critical in:

- Facilitating information sharing between SC CIC and private and public critical infrastructure organizations.
- Giving SC CIC Task Force partners the opportunity to leverage the CLO program to share intelligence bulletins and establish relationships.
- Creating networking and training opportunities for cybersecurity professionals across the state through conferences, workshops, and presentations.



SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY



STEP ONE: REPORT TO SC CIC



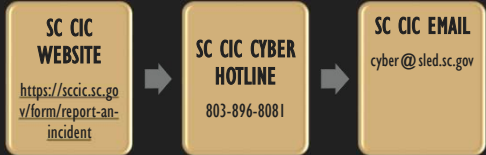
If you are a victim of a scam, cyberbullying, sextortion, identity theft, or experienced a financial loss as a result of a cyber-related scam or email,
PLEASE FILE A COMPLAINT AT IC3 AND WITH LOCAL LAW ENFORCEMENT.



If you're experiencing a cyber event, like malware, insider threat, account compromise, DoS/DDoS, ransomware, or anything similar, please contact SC CIC.

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

STEP ONE: REPORT TO SC CIC



SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

STEP TWO:

BE PREPARED TO ANSWER THE FOLLOWING QUESTIONS



- What happened?
- What is the impact to critical services?
- Have you been able to establish a timeline?
- What measures have you already taken to contain the incident?
- Do you have cyber insurance?
 - Have they been notified?
- Do you have an EDR?
 - What EDR do you use?
 - Are you willing to provide SC CIC a read-only account?
- Do you have any Indicators of Compromise (IoCs)?
- What kind of assistance are you requesting?
 - Law Enforcement
 - SC CIC guidance
 - On-site assistance
- Have you reported the incident to local law enforcement or IC3?

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

STEP THREE: PREPARE THE INCIDENT; IR WISHLIST

- ☒ **EDR / SIEM Telemetry**
What actually executed, and where it spread. Retention is often only 7-30 days.
- ☒ **Firewall, Syslog, and Flow Data**
What left the building, and where it went. Usually, the shortest retention you have.
- ☒ **Identity and Authentication Logs**
Whose account, from where, and whether that access is still live right now.
- ☒ **Backup and Configuration State**
What can be restored, and what was quietly tampered with before the encryption.
- ☒ **Software and Asset Inventory**
Helps the team understand what's normal vs abnormal.

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

STEP THREE: INTERNAL RESPONSE

Current Incidents Posts Shared Page 2026 Incident Tracker

Larkin, Timothy E 7/14 8:52 AM

Cyber Incident (14 July 2026)

had a problem at 0600.
provider let us know that all data and backup is gone.
IT has been working since 630.
Think it came in from SAN.
They are unplugged and completely off line.

His cell # is:
see more

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

STEP THREE: INTERNAL RESPONSE

Email subject: SC CIC - incident alert - call
Email Example:

SC CIC is requesting all task force participants call in at 10:15am on Friday, September 24, 2022, in reference to a cyber incident notification. Assistance is requested.

Phone number: 415-655-0001
Access code: *** ***
No participant ID

Thank you,
South Carolina Critical Infrastructure Cybersecurity (SC CIC)
cyber@scled.sc.gov



SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

STEP FOUR: SC CIC INITIATES RESPONSE



SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

STEP FOUR: SC CIC INITIATES RESPONSE



Goal #1:

Determine how the threat actor gained access



Goal #2:

Collect IOCs and artifacts for further analysis



Goal #3:

Stop the Bleeding



Goal #4:

Information Sharing with SC CIC Participants

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

INC Ransom

INCIDENT RESPONSE



SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

ANOTHER ONE

**BANKS: invalid configuration.
BANKS: invalid configuration.
No hypervisor found.**

South Carolina Critical Infrastructure Cybersecurity

YET ANOTHER VPN COMPROMISE

- Initial analysis showed **2 VPN accounts** used to access the environment
 - No Multi-factor Authentication (MFA)
 - No Brute Forcing
- More on this later...

ALRIGHT THEN, KEEP YOUR SECRETS

South Carolina Critical Infrastructure Cybersecurity

PUBLICLY EXPOSED MANAGEMENT INTERFACE

- It was also determined that the management interface for the **Fortinet firewall** was exposed to the internet

South Carolina Critical Infrastructure Cybersecurity

[illegible]

HOW DO WE STOP THIS?

1. Enroll in **SC CIC Threat Intelligence**
 - If in doubt, reach out
2. Install **Endpoint Detection and Response (EDR) tools**
 - SLCGP eligible – ask us about CrowdStrike and CheckPoint offerings available to you
3. Check your **public exposure**
4. Monitor for **suspicious logins**
 - Odd hours
 - VPN connections when there shouldn't be any
5. Use **password managers** to store credentials

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

SC CIC - INCIDENT RESPONSE BRIEFING

YOU DON'T RISE TO THE OCCASION.

YOU FALL TO YOUR LEVEL OF PREPARATION.

Making incident-response decisions faster — before the incident.

Ryan Truskey - Director, SC CIC

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

THE PROBLEM

AN INCIDENT IS NOT A KNOWLEDGE TEST. IT'S A DECISION TEST.

In the first hours of an incident, the damage is driven by **how long it takes to make each decision** not by how well you eventually make it.

Every minute of "who's allowed to decide this?" is a minute the attacker keeps working.

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

The eight decisions every incident forces

Preparedness is simply deciding as many of these as possible while it's calm.

1

Declare

Is this an incident — and who says so?

2

Disconnect

What comes offline, and who authorizes it?

3

Communicate

What do we say publicly, and who says it?

4

Engage

Insurer, breach counsel, IR firm, SC CIO?

5

Pay / Don't

What is our ransom position?

6

Continue

How do we keep services running?

7

Notify

Who must be told, and by when?

8

Recover

What comes back first?

South Carolina Critical Infrastructure Cybersecurity

THE SEVEN LEVERS

SEVEN THINGS TO PUT IN PLACE BEFORE 3:40PM ON A FRIDAY

Each one converts a decision you'd otherwise make in crisis into one you've already made.

South Carolina Critical Infrastructure Cybersecurity

LEVER 1 OF 7

⚡

Pre-decide authority

The single highest-value, lowest-cost thing you can do.

What to have in place

- A written delegation of authority: who can declare an incident, and who can order the network disconnected by name and by role.
- A clear line of succession when the top person is unreachable (soccer game, vacation, hospital).
- After-hours reachability that is actually tested not "we'd find them."
- A standing rule for the money question: who can approve emergency spend on a weekend.

South Carolina Critical Infrastructure Cybersecurity

LEVER 2 OF 7



Know your contacts cold

The moment you need the number is the moment you can't look it up.

What to have in place

- A one-page call list kept off the network on paper and on personal phones.
- SC CIC, your MSP's after-hours line, and your insurer's breach hotline at the top.
- The name of your breach coach and the IR firm your policy requires before you need them.
- Federal and state partners: FBI/IC3, CISA, and your water/wastewater primacy contact.



SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

Work Cell – 803-206-0096

Personal Cell – 973-919-0528



SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

LEVER 3 OF 7



Back up like you'll be attacked

Backups are only real if they're offline and you've restored from them.

What to have in place

- At least one copy that is offline or immutable and unreachable from the network the ransomware is on.
- A restore you have actually tested in the last 90 days, with the time-to-restore written down.
- Backups that a compromised admin account cannot reach or delete.
- Know your real recovery point: "how much data would we lose?" answered before, not during.



SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

LEVER 4 OF 7



Plan to run without systems

Continuity of operations is where towns are weakest.

What to have in place

- A ranked list of what cannot go dark (dispatch, water treatment, payroll) agreed by leadership, not just IT.
- A manual or paper fallback for payroll, utility billing, permitting, and court, written down somewhere reachable.
- A pre-set recovery-priority order so restoration isn't argued during the outage.
- An out-of-band way to communicate when you must assume email is being read.




SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

LEVER 5 OF 7



Have the words ready

How you communicate under pressure becomes a public record.

What to have in place

- A pre-approved holding statement the mayor could read to a reporter tonight, written calmly not at 9 p.m under pressure.
- One designated spokesperson (PIO) and a rule that everyone else routes to them.
- FOIA awareness: assume your incident emails and documents may be released.
- A simple internal update rhythm so staff and council aren't filling the silence with rumor.




SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

LEVER 6 OF 7



Know your policy before you need it

Cyber insurance can help you — or trip you — in the first hour.

What to have in place

- Read the incident-response requirements now: many policies require you use panel counsel and a panel IR firm.
- Know your notice deadline late notice can jeopardize coverage.
- Confirm in advance how SC CIC support coexists with insurer-led response they are not mutually exclusive.
- Keep the policy's IR section with your call list, not buried in a shared drive that's now encrypted.




SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

LEVER 1 OF 1



Exercise it — on a cadence

A plan you've never run is a document, not a capability.

What to have in place

- Run a tabletop at least annually rotate the scenario (ransomware, BEC, OT, insider).
- Put new officials through the decision-authority worksheet when they take office.
- Use the SC CIC to run exercises between internal ones.
- Track your own metric: time-to-first-decision. Watch it drop each time you practice.



SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

BEFORE YOU LEAVE · 1 OF 3



The readiness check

If you can't answer "yes" to these today, you've found your action items. Start with authority and contacts.

☐ Right now, who can order our network disconnected after hours?

Lever 1

☐ If our top official is unreachable, who is next in line to decide?

Lever 1

☐ When did we last test that we can reach every decision-maker after hours?

Lever 1

☐ Right now, can I reach my insurance breach coach without searching my inbox?

Lever 2 & 6

☐ Is our call list on paper and on personal phones, off the network?

Lever 2

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

BEFORE YOU LEAVE · 2 OF 3



The readiness check

Backups and continuity: can we recover, and can we keep serving residents while we do?

☐ Right now, do we have a tested, offline backup from the last 90 days?

Lever 3

☐ Could a compromised admin account reach or delete our backups?

Lever 3

☐ How much data would we lose restoring from our last good backup?

Lever 3

☐ Right now, could we make payroll next week with every system down?

Lever 4

☐ Has leadership, not just IT, agreed which services come back first?

Lever 4

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

BEFORE YOU LEAVE · 3 OF 3



The readiness check

Communications, insurance and practice: the decisions that play out in public.

☐ Right now, is there a holding statement the mayor could read tonight?

Lever 5

☐ Does every staff member know to route press calls to one spokesperson?

Lever 5

☐ Do we know our policy's notice deadline and its required panel firms?

Lever 6

☐ When did we last run a tabletop, and which scenario did it test?

Lever 7

☐ Have newly elected officials walked through the decision-authority worksheet?

Lever 7

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

THE TAKEAWAY



SPEED COMES FROM DECISIONS ALREADY MADE.

You can't predict the attack. You **can** pre-decide the response.

SC CIC is your no-cost partner for helping you build that list whether it's planning, exercises, or response.

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

SC CIC · MTASC BRIEFING



COVERAGE YOU CAN PROVE.

MONITORING CONFIGURATION DRIFT.

Verifying that security tools are deployed, monitored, and enforced.

Ryan Truskey · Director, SC CIC

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

THE PROBLEM

THE GAP WE KEEP FINDING

- › EDR licensed but agent missing after a rebuild
- › Log source dead six weeks, no alert
- › Blocking policy deployed but a group excluded since 2023
- › Gaps during the incident, not before

THE POINT: Unverified coverage is not coverage.

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

DEFINITION

WHAT CONFIGURATION DRIFT IS

- › Intended state: the control you designed and funded
- › Actual state: what is running right now
- › Drift is the gap between the two
- › It can happen quietly, with no alert

THE POINT: Drift is normal. Unmeasured drift is risk.

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

ROOT CAUSES

WHY DRIFT HAPPENS

- › Rebuilt and new assets skip deployment
- › Agents stall, licenses lapse, services stop
- › Temporary exceptions never expire
- › Cloud and SaaS grow outside the baseline

THE POINT: Nobody causes drift on purpose.

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

THE MODEL

DEPLOYED IS NOT MONITORED IS NOT ENFORCED

01
DEPLOYED
Is it on the asset?

› On every inventoried asset

› Inventory current

› Coverage as a percentage

FAILS AS: unknown assets

02
MONITORED
Is it still reporting?

› Checked in recently

› Telemetry reaching SIEM

› Someone owns the alert

FAILS AS: silent agents

03
ENFORCED
Does it actually act?

› Applied, not assigned

› Blocking, not audit

› Exclusions dated

FAILS AS: policy holes

THE POINT: All three, or it is not covered.

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

DEPLOYED

VERIFY COVERAGE, NOT PURCHASE

› Start from inventory, not the console

› Reconcile inventory, console, directory

› Report coverage per asset class

› 98% of 4,000 assets leaves 80 open

Device status

1,094
100%

Installed1071

Not Installed0

Failed10

Not Responding13

Not Application0

THE POINT: No inventory, no coverage metric.

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

MONITORED

PROVE THE TELEMETRY IS STILL FLOWING

› Track last check-in, not install count

› Alert when a log source goes quiet

Ingestion Rate

VendorsPANW

Traffic / Sec

586 KB/s

537 KB/s

488 KB/s

Sens 1.4

Sens 1.5

Sens 1.6

Sens 1.7

Sens 1.8

Sens 1.9

Sens 2.0

Sens 2.1

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

ENFORCED

CHECK THAT THE POLICY HAS A CONTROL

Applied, not just assigned

Blocking mode, not audit mode

Every exclusion has an expiration

Spot-check with a safe test

CA Policy - Authentication Context - Compliant Device

Assignments

Target resources

Networks

Conditions

Access controls

THE POINT: An unenforced policy is paperwork.

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

Compliance Before Connect

Every check a SLED employee must pass before Cisco Secure Client (AnyConnect) will open a VPN tunnel.

STEP 1

Employee signs in to a SLED laptop

Windows sign-in establishes the user's session with Microsoft Entra ID.

Device registered in Entra ID

Intrune reports ownership and compliance

STEP 2

Launches Cisco Secure Client

The VPN client hands authentication off to Microsoft Entra ID.

Single sign-on to Entra ID

Signals user, device, platform, location, method

STEP 3

Entra ID Conditional Access checks

1 Sign-in from within the US

2 Approved sign-in method

3 Supported operating system

4 SLED-owned device

5 In tune-compliant Windows device

6 Strong MFA (no SMS or voice)

If it fails

Blocked outside the US

Blocked non-US Logins

Blocked device code flow

Blocked Android, iOS, Linux

Blocked personal device

Blocked non-compliant

Blocked weak or no MFA

Device security

Minimum Baseline Compliance Policy for Windows Devices

BitLocker drive encryption

Secure Boot enabled

Code integrity enabled

TPM present

Firewall, antivirus & antiappware active

Operating system

Same baseline policy

Only supported, patched Windows 11 releases are allowed. Each release must be at or above its minimum build.

RELEASEMINIMUMBUILD

Windows 11 22H226200.7840

Windows 11 24H226100.7840

Windows 11 23H222631.6783

Windows 10, older Windows 11 releases, or missing patches fail

Required security tools

Minimum Baseline Policy for each tool - custom compliance scripts

Cortex XDR

Cisco Umbrella

Symantec

ScreenConnect

ThreatLocker

Tenable Nessus Agent

Cribl Agent

Each tool must be installed and its service running. Installed but stopped fails.

IF A DEVICE FALLS OUT

DAY 0

7-day grace period, then VPN access stops

DAY 1

User notified, IT security copied on tool alerts

DAY 2

Reminder to fix the missing tool

DAY 4

Final warning

DAY 7

Marked non-compliant. Secure Client sign-in blocked

16

BASELINE

WRITE DOWN THE INTENDED STATE

Control	Applies to	Proof of deployment	Proof of enforcement
Endpoint detection	Workstations, servers	Agent present, in inventory	Blocking, no stale exclusions
Log collection	Auth, DNS, firewall	Sending in last 24h	Parsed, mapped to detections
MFA / conditional access	Privileged accounts	Enrolled and registered	No legacy-auth bypass
Patch / config baseline	Managed OS builds	Scan result within 7 days	Remediated or accepted

THE POINT: No baseline, no drift detection.



SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

THE LOOP

MAKE DRIFT DETECTION A STANDING LOOP

STEP 1
INVENTORY

Enumerate every asset, account, and tenant

STEP 2
COMPARE

Actual against baseline

STEP 3
FLAG

Each delta gets an owner

STEP 4
REMEDiate

Fix it, or accept it with an expiry date

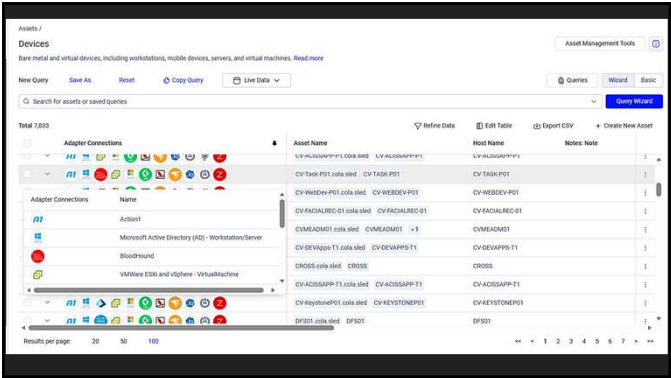
STEP 5
RE-VERIFY

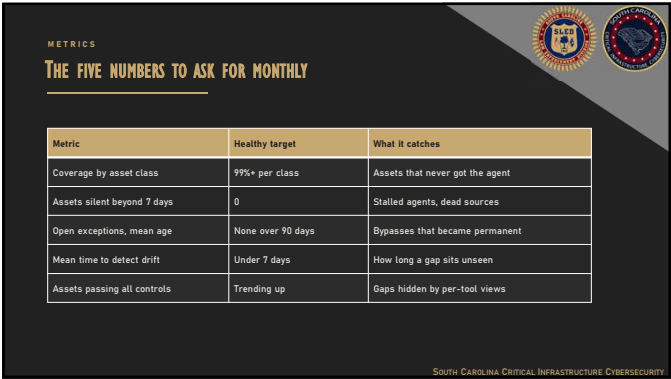
Confirm it holds next cycle

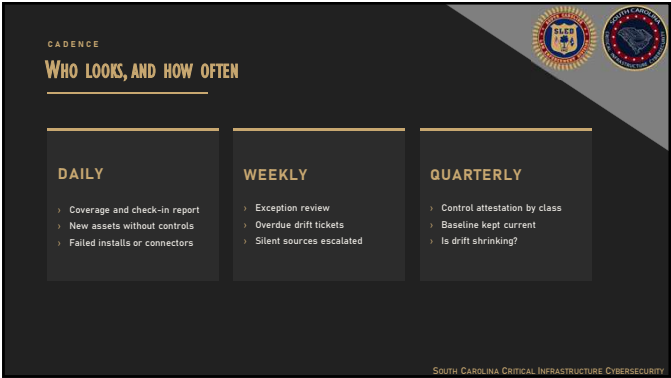


SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY









ACTION PLAN

THIRTY, SIXTY, NINETY DAYS

FIRST 30 DAYS

› Pick one control, one asset list

› Measure and publish coverage

› Name an owner per gap

BY 60 DAYS

› Automate the reports

› Inventory exceptions and set expiry dates

› Draft tickets in the work queue

BY 90 DAYS

› Extend to remaining controls

› Report the five metrics monthly

› Tabletop a coverage gap

THE POINT: Start with one control.

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

YOUR FRIENDLY NEIGHBORHOOD GHOSTBUSTERS

OCTOBER 1 at 10 AM

PARTNERS, PORTALS & PERIMETERS

THE FORTY-FOURTY PICK MONSTER MANUAL

OCTOBER 8 at 10 AM

OPERATION PALMETTO SHIELD-UPSTATE

OCTOBER 14th at 9AM

2026 SC CIC CYBERSECURITY AWARENESS MONTH SCHEDULE

OPERATION PALMETTO SHIELD-MIDLANDS

OCTOBER 21st at 9AM

ENTER THE MONSTER'S NETWORK: SURVIVE THE EXPLOIT, SAVE THE SYSTEM

OCTOBER 23 at 9 AM

FRANKENSTEIN'S NETWORK

Stitching IT and OT Together

OCTOBER 27 at 10 AM
