# Local Power, Global Defense

## Turning Your Mac or GPU into a Cyber Force Multiplier with Foundation-Sec-8B and other Open-Weight Models



SOVEREIGN AND SECURE

CANADA

Jason Maynard
Field CTO, Cybersecurity – Canada · Cisco

CCIE, CC[N|I|D]P, SFCE, C|EH, RCSS, GICSP, GRID, GPEN, GDAT, GCPN, AWS Cloud Practitioner, AWS Solutions Architect, AWS Security, Azure Fundamentals, Azure Security Engineer
MITRE ATT&CK: CTI, SOC Assessments, Threat Hunting Detection Engineering, Adversary Emulation Methodology, Purple Teaming Methodology
ATTACKIQ: Purple Team, Mitre Att&ck, Breach Attack Simulation
Splunk Power User, Splunk Administrator

Cisco Confidential





# VISS

# 2ND ANNUAL VANCOUVER INTERNATIONAL SECURITY SUMMIT

Addressing Foreign Threats and Ensuring Economic & Political Resiliency

**OCTOBER 16 - 17, 2025**

**COAST COAL HARBOUR HOTEL | VANCOUVER, BC, CANADA**

- We will never achieve 100% immunity
- The adversary will never be 100% correct
- The defender never needs to be 100% correct
- Time is a power move for defenders
- Intial access is inevitable




THREAT OVERVIEW
ACTIVE INCIDENT
PHP2SHELL WEBSHELL
SEVERITY: CRITICAL
LATERAL MOVEMENT DETECTED
AFFECTED ASSETS
7 SERVERS
3 CONTAINERS
DATA EXFILTRATION
OUTBOUND CONNECTIONS
2.4 GB
ATTACK PATH ANALYSIS
PIVOT POINT
php2shell → www-data
MOVEMENT PATHS
7 ACTIVE
php
PHP2Shell
PHP WEBSHELL ACCESS
php2shell@compromised:~# whoami
www-data
php2shell@compromised:~# ls /
bin boot dev etc home lib lib64
proc root sys tmp usr var
php2shell@compromised:~# cat
/etc/passwd | grep -v nologin
php2shell@compromised:~#
WEBSHELL EXECUTION DETECTED
COMPROMISED WORKLOAD
COMPROMISED WORKLOAD
COMPROMISED WORKLOAD
COMPROMISED WORKLOAD
CONTAINER WORKLOAD
runtime: containerd
COMPROMISED

# HOST-BASED WORKLOAD PROTECTION

Prescriptive Controls Delivered. Risk Contained.

## POLICY DELIVERY STREAM

POLICY ENGINE → LEAST-PRIVILEGE RULES → PROCESS CONTROLS → RUNTIME PROTECTIONS

Pushed directly to each host agent

## EXPLOIT ATTEMPT DETECTED & BLOCKED

SOURCE

10.10.45.23:51244

PHP2Shell Exploit

PAYLOAD DETECTED

PHP webshell / reverse shell code

INTENT

Command execution • Reverse shell

Persistence

ACTION: BLOCKED & CONTAINED

Exploit prevented. No execution.

No lateral movement.




## LOCAL WORKLOAD CONTROLS

**LEAST-PRIVILEGE RULES**
User: www-data (minimal)
Filesystem: read-only where possible
Network: deny all except allowed endpoints

**PROCESS CONTROLS**
Allowlisted binaries only
Fork / exec prevention
Memory protection enabled

**RUNTIME PROTECTIONS**
File integrity monitoring
System call filtering
Behavioral anomaly detection

**CONTAINMENT**
Namespace isolation
Resource limits
No pivot or breakout

**MONITORING & RESPONSE**
Local telemetry
Real-time blocking
Event reporting

PROTECTED AT THE HOST. RISK CONTAINED.

## PROTECTION STATUS

ALL CONTROLS ACTIVE

Least-Privilege • Process Isolation • Runtime Defense

| POLICIES ENFORCED | PROCESSES MONITORED | BLOCKED ACTIONS | CONTAINMENT EVENTS |
|---|---|---|---|
| 128 | 1,243 | 7 | 1 (ACTIVE) |

# We keep sending the case file to a brilliant stranger.

Every API call is a consultant who never signs your NDA.
The answer is often excellent, but the copy is no longer yours.



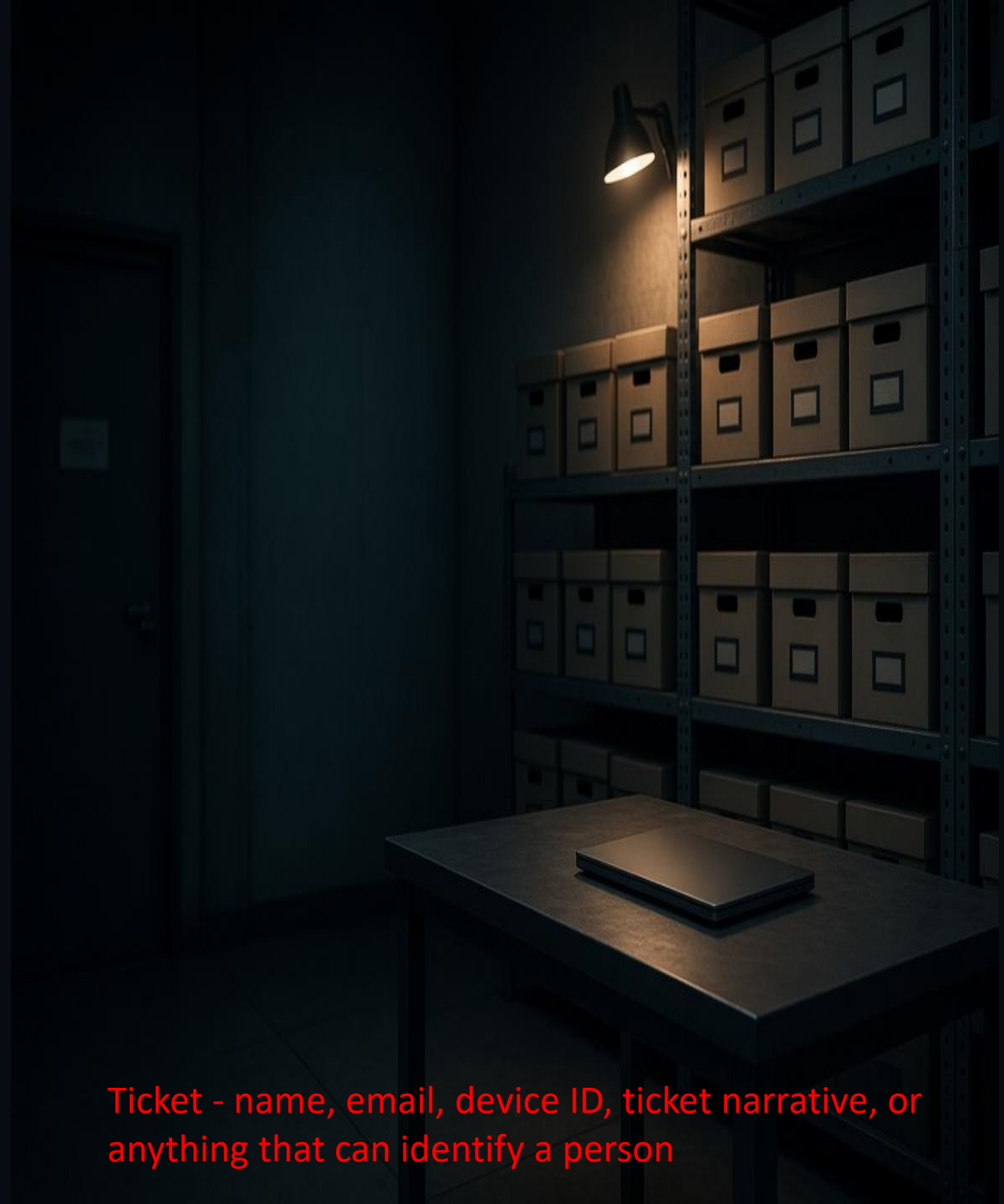
# Incident data is personal information wearing a ticket number.

**Purpose** A PIA (privacy impact assessment) did not authorize 'paste into a public model.'

**Transfer** Prompts cross borders and sub processors appear. Ex: vendor A leverages vendor B. You inherit their custody story.

**Privilege** If the artifacts belong in an evidence room, it does not belong in someone else’s context window and training data.

**Retention** You can delete the ticket, but you cannot unsay the prompt.



Ticket - name, email, device ID, ticket narrative, or anything that can identify a person

# Time to assess and address

01

## Control

Frontier vs open-weight is not a religion. It is where the case file lives.



02

## Engine

Open weight models operate locally and does not cross-national boundaries.



03

## Harness

Playbook + tools + guardrails our intern becomes a teammate.



04

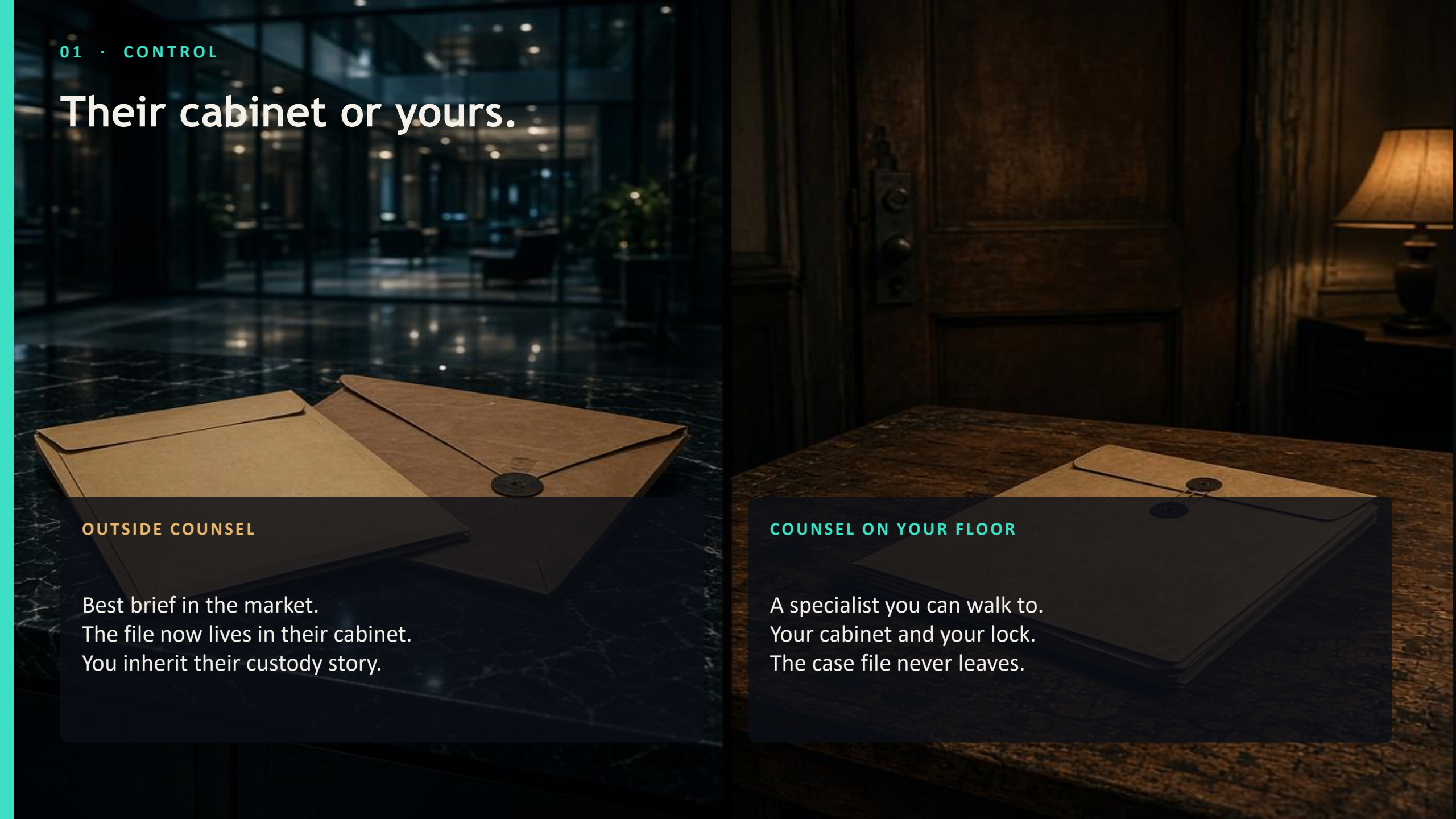
## Leash

When the model gets hands, we govern it like we govern people
nonhuman identities should be sponsored by humans.



01 · CONTROL

# Their cabinet or yours.



## OUTSIDE COUNSEL

Best brief in the market.
The file now lives in their cabinet.
You inherit their custody story.

## COUNSEL ON YOUR FLOOR

A specialist you can walk to.
Your cabinet and your lock.
The case file never leaves.

# Local is a security control and a privacy control.

## Residency



The work runs on a box you can point to.

## Minimization



It only sees what you gave it.

## Not training their model



Your incident is not their training data.

## Air-gap



It still works when the network must stay off. Think sovereignty

## Comprehensive Audit



The question and the answer can also land in your SIEM.

## Onboarding



Onboard it to your playbooks and use local tools and skills.



Confidential

# What this is not.

01

## Not autopilot it’s an intelligent intern

It drafts the note, a person files it, and nobody isolates a host without a human in the loop.

02

## Not a replacement SIEM

It can read an alert, but the SIEM still owns the truth.

03

## Not a headcount cut

Blank-page time dies but judgment does not. We need humans in the loop

04

## Not a privacy impact free pass

Local is one control but you still classify the data, lock the box, and write the PIA (Privacy Impact Assessment).



Confidential

# You already own enough silicon.

**7-8B** The sweet spot. Foundation-Sec. Q5/Q8 on 16–24 GB.

**13-14B** Still local on a 24 GB Mac or mid GPU.

**30B+** Only if the harness cannot close the gap.



# A security specialist and just another chatbot in a costume.

| | |
|---|---|
| **8B** | Llama 3.1 backbone. Continued pre-training on ~5.1B cyber tokens. |
| **CTI** | Built on threat reports, vulns, incident docs, standards — defender language. |
| **A2.0** | Apache 2.0. Hugging Face: fdtn-ai/Foundation-Sec-8B and family. |
| **Jobs** | Triage, mapping, detection, advisory. Does not make coffee……yet. |



# The Foundation-Sec-8B specialist holds its own.

01

## On the intel

It maps a CVE (common vuln exposure) to a CWE (common weakness enumeration) and a report to an ATT&CK technique.



02

## On the investigation

The Reasoning line walks the path before it answers -> attack chain, residual risk, why. Not a one-shot guess.



03

## On the ticket

Alert notes, case handoff, vulnerabilities context. The work that must stay on the same box as the case file.





Confidential

# 3 Main Types of Language Models. Do not use a scalpel as a shovel.

BASE

## The clay



You do not chat with clay. You shape it — fine-tune, embed, research.

INSTRUCT

## The writer




The colleague who drafts the ticket, the brief, the summary.

REASONING

## The analyst




The colleague who shows the work, the attack paths, dual maps, and supports the why.


Confidential

# Let the giant draw the plans. Build them here.

Frontier models are extraordinary editors of playbooks, skills, and system prompts.

The specialized local model is the shop that runs those plans against data that must not leave.

That loop is the force multiplier. Not either-or.



# The Parts: Stand it up before lunch. Source it like a defender.

## Ollama

Serve. Pull, quantize, run.

## Known lineage

fdtn-ai. Model card. Apache 2.0.

## Open WebUI

Work. Chat, RAG, skills, tools.

## Read the scan

Hugging Face + enhanced ClamAV. Badges matter.

## Docker

Repeat. Same box next week.

## Pickle is code

Untrusted .pkl is untrusted execution.



Confidential

# The model is not the product. The harness is.



A smart intern and a blank screen.

The same person with a playbook, a map, and a badge.

# Four layers between raw weights and a teammate.

01



## Knowledge

*The library*

Curated RAG (Retrieval-Augmented Generation). Playbooks, intel, statutes. Small and clean beats huge and noisy.

02



## Skills

*The laminated runbook*

Markdown files. How we triage. How we map. Lazy-loaded. Almost no blast radius.

03



## Tools

*The badge (access)*

Search, enrich, query. This is where power and privacy risk arrive together.

04



## Guardrails

*The standing order*

Persona, output contract, 'never invent a T-code,' Enterprise ATT&CK only.



Confidential

# Same incident with two jobs.

THE INPUT




Image is just an example

## INSTRUCT · THE WRITER

Ticket-ready note.
Timeline, IOCs, & Severity.

Next containment steps.
Language a SOC can file without rewriting the page.

## REASONING · THE ANALYST

ATT&CK map with receipts, detection ideas + telemetry.
Bypass paths and blind spots discovered.

A language an engineer and an auditor can use.



Confidential

# Same incident with two jobs.

THE INPUT




Image is just an example

INSTRUCT · THE WRITER

Triage this multi-source incident and produce a ticket-ready summary with timeline, IOCs, Enterprise ATT&CK mapping, severity, and next containment steps:

[EDR] 14:12:03 host=WS-FIN-042 user=jsmith process=powershell.exe parent=outlook.exe encoded command present
[Firewall] 14:12:18 src=10.20.15.42 dst=185.234.72.19:443 action=allow bytes=48210
[Proxy] 14:12:19 user=jsmith url=https://cdn-update-static[.]com/payload.ps1 category=uncategorized
[EDR] 14:12:45 host=WS-FIN-042 process=cmd.exe cmdline="whoami & net group Domain Admins /domain"


Confidential

# Same incident with two jobs.

THE INPUT




Image is just an example

REASONING · THE ANALYST

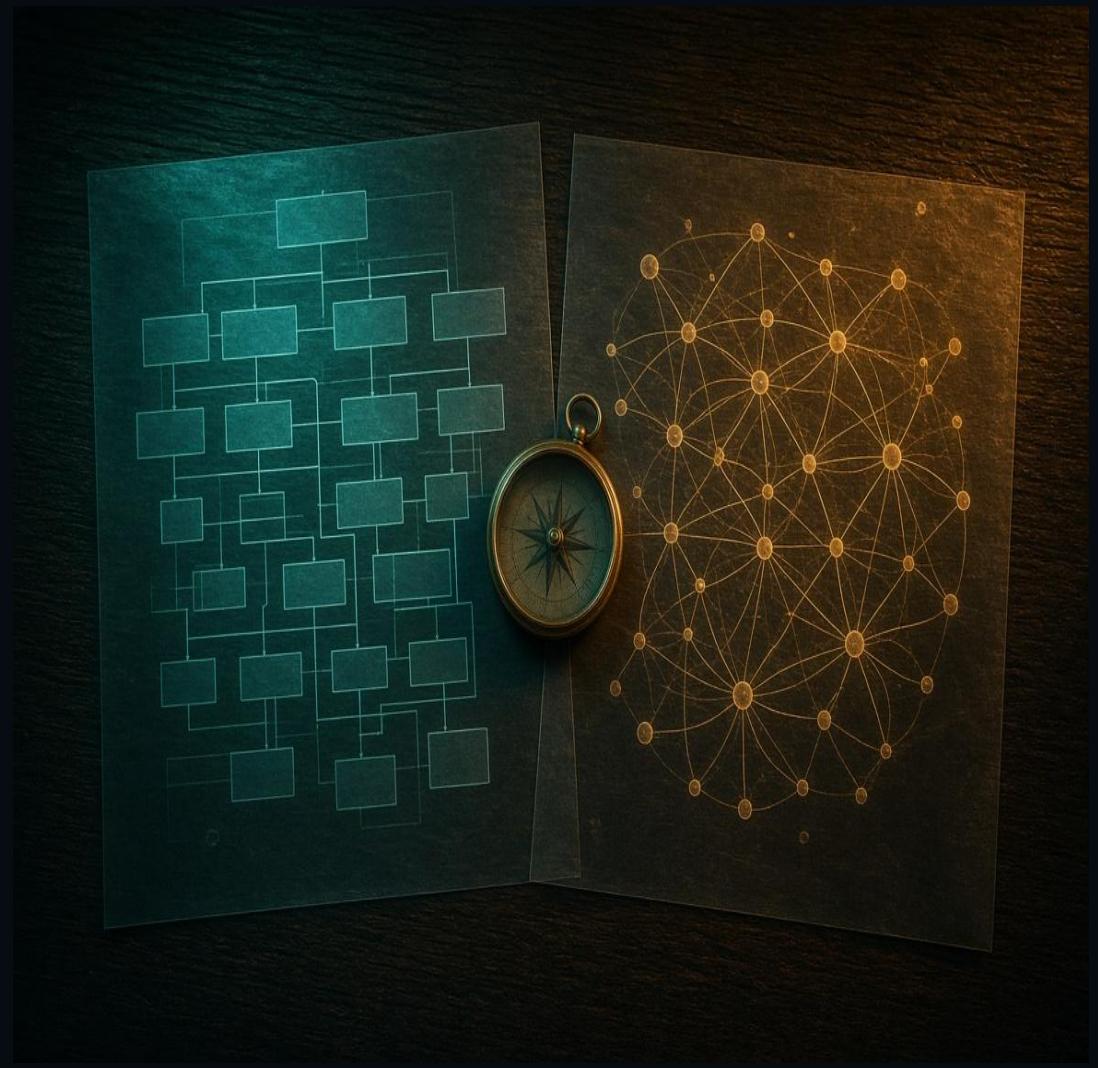
Map this behavior to Enterprise ATT&CK and propose detections. Include required telemetry, high-signal ideas, false-positive notes, and coverage gaps. Enterprise ATT&CK only. Never invent IDs.



Confidential


INCIDENT HELPER
Alert to Action Sidekick
SOC COMMAND CENTER
THREAT MAP
LIVE THREATS
1,248
ACTIVE INCIDENTS
37
NETWORK HEALTH
98%
AI AGENT NETWORK
Threat Intel Agent
Detection Agent
Response Agent
OpenWebUI
New Chat
Chats
Agents
Tools
Models
Settings
Incident Helper Assistant
AI Agent Network Online
Analyze recent threats and prioritize incidents
10:24 AM
Analysis complete. Top threats identified and prioritized.
View Dashboard
Generate Report
Ask CyberBuddy...
OLLAMA
Running locally
CISCO
Foundational Cyber Model
Neural Reasoning Engine
OpenClaw
Robotic Claw Agent
Autonomous Response
DefenseClaw
Armored Shield
Threat Containment Protection
SECURITY ORCHESTRATION
ENDPOINT DEFENSE
Protected
2,156 / 2,156
DATA INGESTION
2.4 Tb/s
THREAT INTELLIGENCE
Indicators of Compromise
87
INCIDENT HELPER

# The worked example: two maps, one compass.



CyberAlberta controls on one sheet. Enterprise ATT&CK on the other.

The Reasoning model dual-maps them: risk removed, techniques disrupted, how adversaries bypass, residual risk — plus PIPA context for a public-sector org.

That is not a party trick. That is a briefing a CISO and a privacy officer can both sit through.



Confidential

# CyberBuddy

## Frameworks & Cyber Research

Assess. Map. Score. Prioritize.

### CyberAlberta 35 Goals

Align to provincial cyber resilience outcomes.

### Residual ATT&CK TTPs

Track remaining adversary techniques & procedures.

### Foundation-Sec AI

AI-powered security research & control recommendations.

### Splunk SOC Dashboards

Real-time monitoring, hunting, and response.



Orhan Ergun - YouTube | Temp - OneDrive | Cisco Cloud Control | Frameworks | CyberAlberta

cyberalberta.ca/frameworks

Continue where you left off: Chrome can restore your tabs every time you restart. To turn this on, go to Settings.

**Scam Alert**

Fraudulent text messages are circulating that impersonate the Government of Alberta and promise an unclaimed energy rebate or similar benefit. These messages are scams designed to steal personal or banking information. **Do not click the link, reply, or provide any information**. Click here to view an example.



01

## GOVERN

Establish and maintain cybersecurity governance, risk management strategy, and supply chain oversight.

02

## IDENTIFY

Understand your assets, business environment, and risk posture to prioritize cybersecurity efforts.

03

## PROTECT

Implement safeguards for critical infrastructure, access control, data security, and training.

04

## DETECT

Deploy continuous monitoring, anomaly detection, and security event analysis capabilities.

05

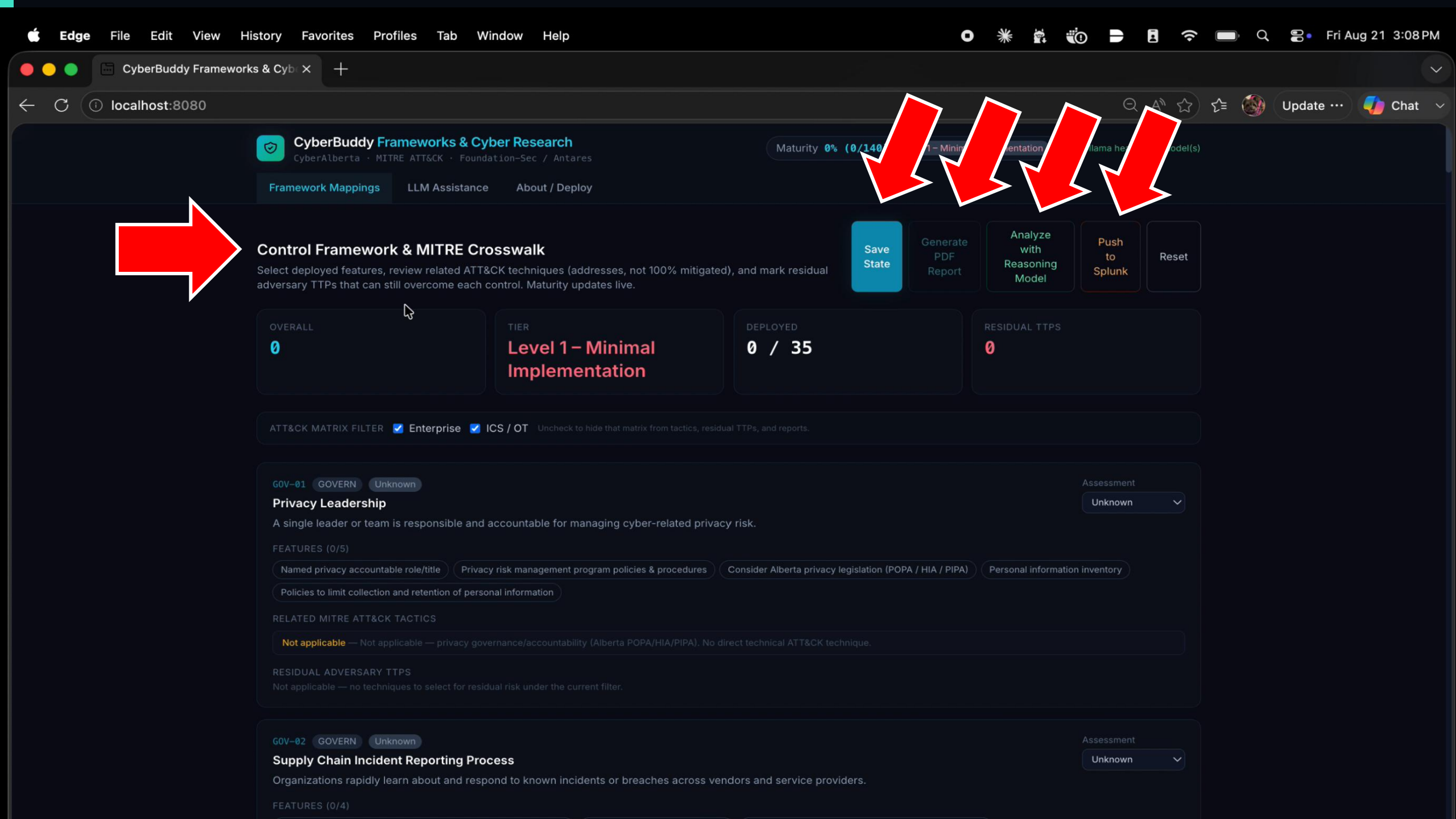
## RESPOND

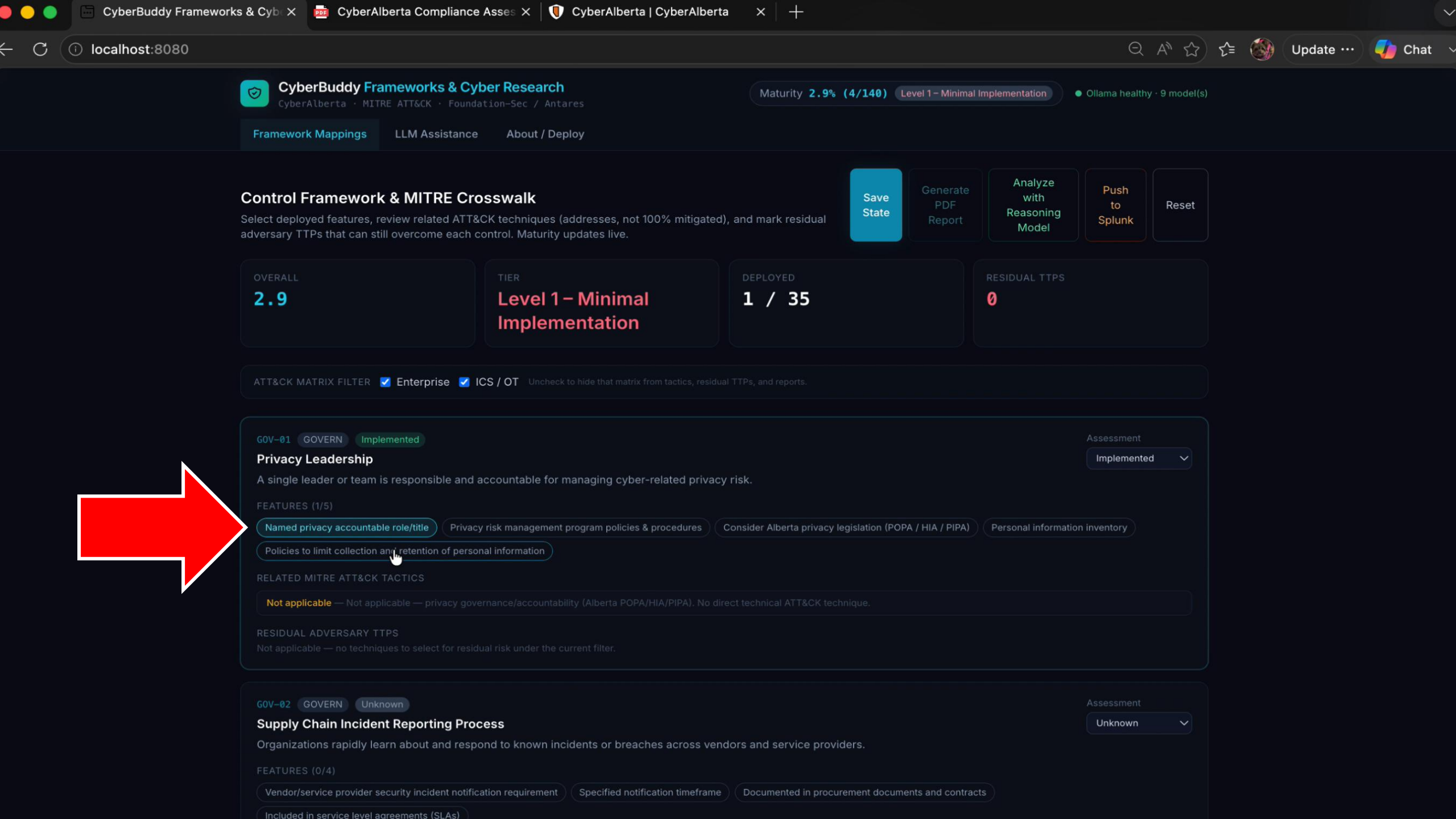
Execute incident response plans, coordinate communications, and conduct analysis during events.

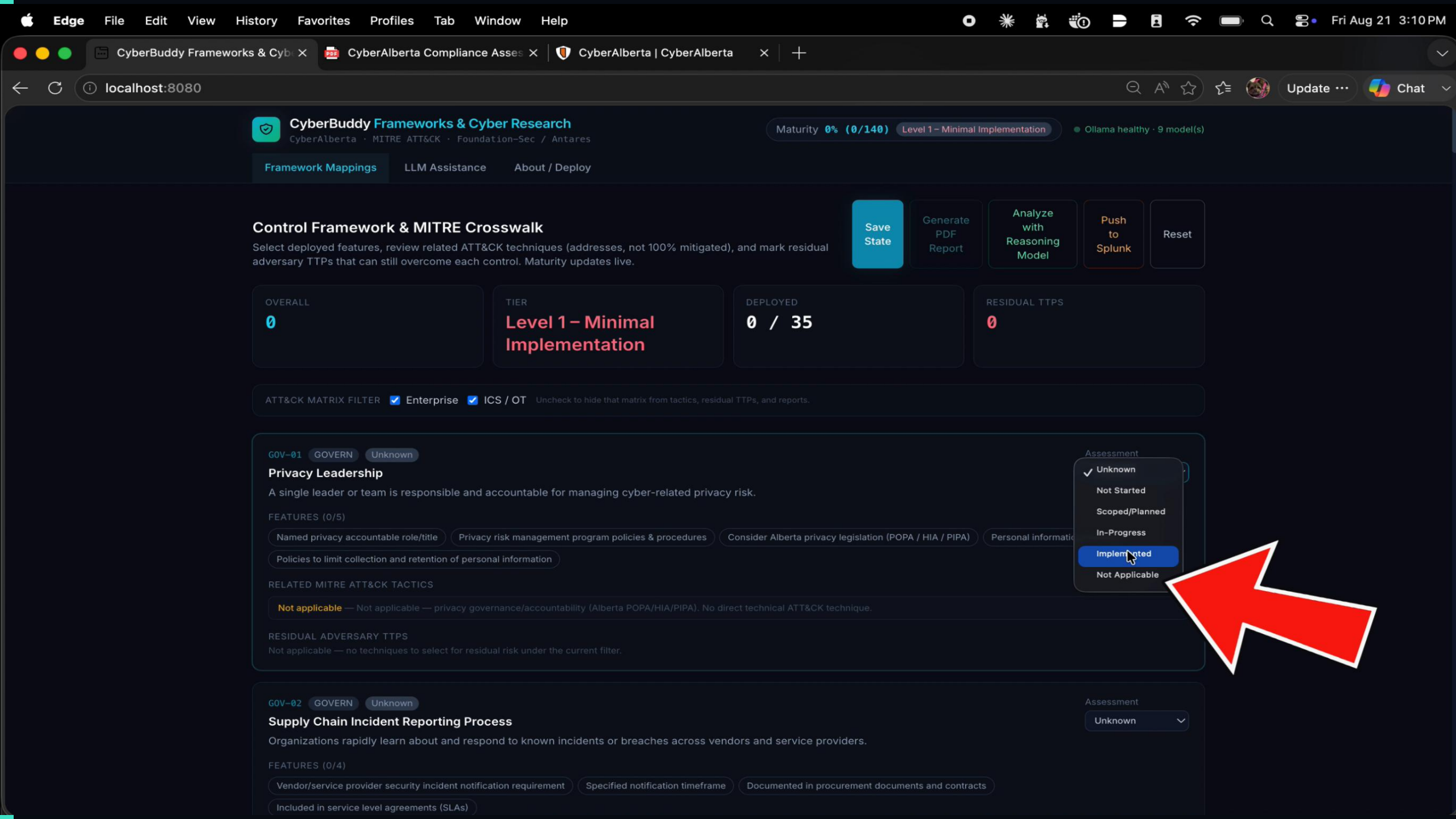
06

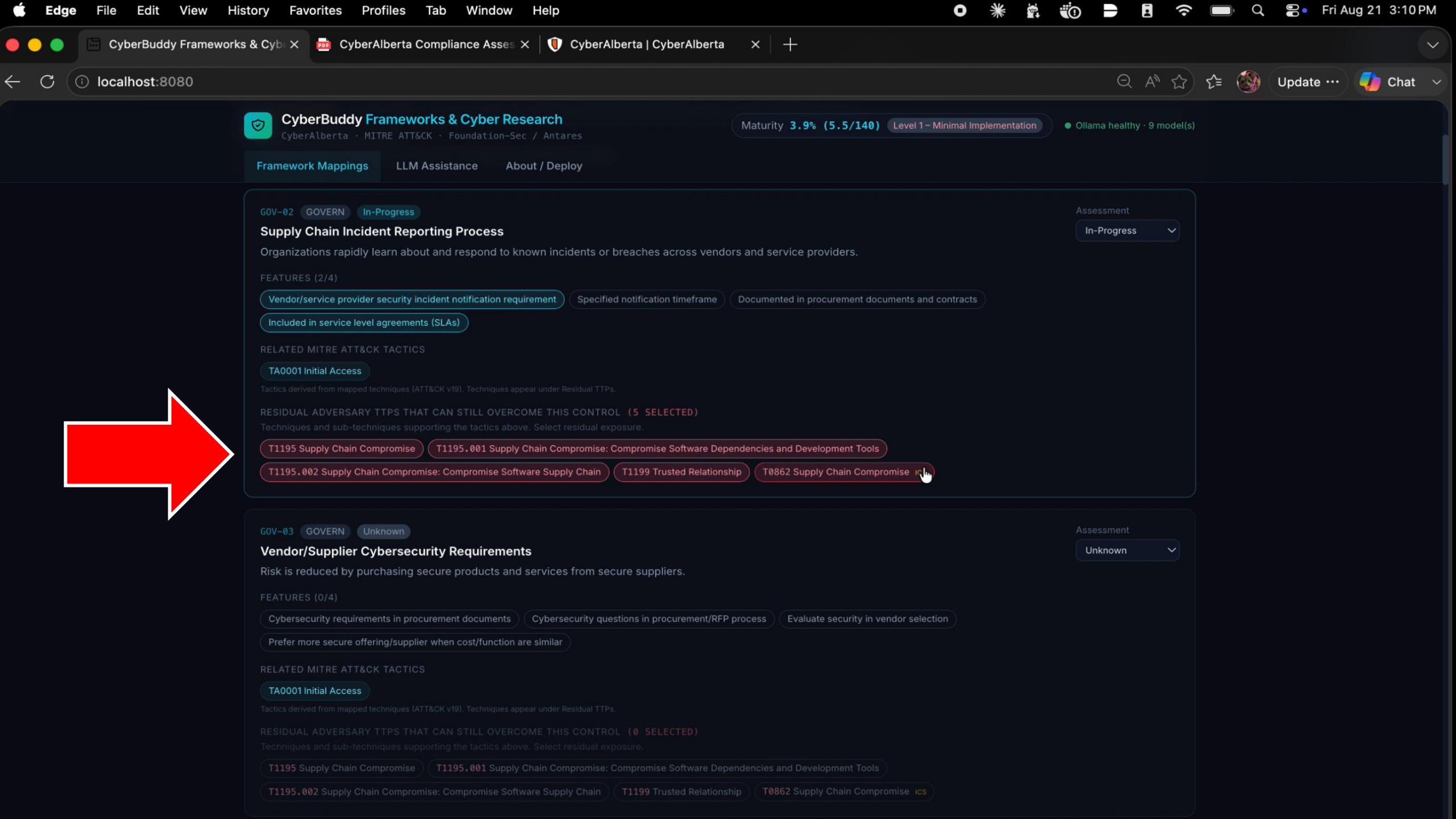
## RECOVER

Restore capabilities, implement improvements, and coordinate recovery communications.


Edge File Edit View History Favorites Profiles Tab Window Help
Fri Aug 21 3:08 PM
CyberBuddy Frameworks & Cyb
localhost:8080
Update
Chat
CyberBuddy Frameworks & Cyber Research
CyberAlberta · MITRE ATT&CK · Foundation-Sec / Antares
Framework Mappings
LLM Assistance
About / Deploy
Control Framework & MITRE Crosswalk
Select deployed features, review related ATT&CK techniques (addresses, not 100% mitigated), and mark residual adversary TTPs that can still overcome each control. Maturity updates live.
Save State
Generate PDF Report
Analyze with Reasoning Model
Push to Splunk
Reset
OVERALL
0
TIER
Level 1 – Minimal Implementation
DEPLOYED
0 / 35
RESIDUAL TTPS
0
ATT&CK MATRIX FILTER
Enterprise
ICS / OT
Uncheck to hide that matrix from tactics, residual TTPs, and reports.
GOV-01
GOVERN
Unknown
Assessment
Unknown
Privacy Leadership
A single leader or team is responsible and accountable for managing cyber-related privacy risk.
FEATURES (0/5)
Named privacy accountable role/title
Privacy risk management program policies & procedures
Consider Alberta privacy legislation (POPA / HIA / PIPA)
Personal information inventory
Policies to limit collection and retention of personal information
RELATED MITRE ATT&CK TACTICS
Not applicable — Not applicable — privacy governance/accountability (Alberta POPA/HIA/PIPA). No direct technical ATT&CK technique.
RESIDUAL ADVERSARY TTPS
Not applicable — no techniques to select for residual risk under the current filter.
GOV-02
GOVERN
Unknown
Assessment
Unknown
Supply Chain Incident Reporting Process
Organizations rapidly learn about and respond to known incidents or breaches across vendors and service providers.
FEATURES (0/4)


CyberBuddy Frameworks & Cyb
CyberAlberta Compliance Asses
CyberAlberta | CyberAlberta
localhost:8080
Update
Chat
CyberBuddy Frameworks & Cyber Research
CyberAlberta · MITRE ATT&CK · Foundation-Sec / Antares
Maturity 2.9% (4/140) Level 1 – Minimal Implementation
Ollama healthy · 9 model(s)
Framework Mappings
LLM Assistance
About / Deploy
Control Framework & MITRE Crosswalk
Select deployed features, review related ATT&CK techniques (addresses, not 100% mitigated), and mark residual adversary TTPs that can still overcome each control. Maturity updates live.
Save State
Generate PDF Report
Analyze with Reasoning Model
Push to Splunk
Reset
OVERALL
2.9
TIER
Level 1 – Minimal Implementation
DEPLOYED
1 / 35
RESIDUAL TTPS
0
ATT&CK MATRIX FILTER
Enterprise
ICS / OT
Uncheck to hide that matrix from tactics, residual TTPs, and reports.
GOV-01
GOVERN
Implemented
Assessment
Implemented
Privacy Leadership
A single leader or team is responsible and accountable for managing cyber-related privacy risk.
FEATURES (1/5)
Named privacy accountable role/title
Privacy risk management program policies & procedures
Consider Alberta privacy legislation (POPA / HIA / PIPA)
Personal information inventory
Policies to limit collection and retention of personal information
RELATED MITRE ATT&CK TACTICS
Not applicable — Not applicable — privacy governance/accountability (Alberta POPA/HIA/PIPA). No direct technical ATT&CK technique.
RESIDUAL ADVERSARY TTPS
Not applicable — no techniques to select for residual risk under the current filter.
GOV-02
GOVERN
Unknown
Assessment
Unknown
Supply Chain Incident Reporting Process
Organizations rapidly learn about and respond to known incidents or breaches across vendors and service providers.
FEATURES (0/4)
Vendor/service provider security incident notification requirement
Specified notification timeframe
Documented in procurement documents and contracts
Included in service level agreements (SLAs)


Edge File Edit View History Favorites Profiles Tab Window Help
Fri Aug 21 3:10 PM
CyberBuddy Frameworks & Cyb
CyberAlberta Compliance Asses
CyberAlberta | CyberAlberta
localhost:8080
Update
Chat
CyberBuddy Frameworks & Cyber Research
CyberAlberta · MITRE ATT&CK · Foundation-Sec / Antares
Maturity 0% (0/140) Level 1 – Minimal Implementation
Ollama healthy · 9 model(s)
Framework Mappings
LLM Assistance
About / Deploy
Control Framework & MITRE Crosswalk
Select deployed features, review related ATT&CK techniques (addresses, not 100% mitigated), and mark residual adversary TTPs that can still overcome each control. Maturity updates live.
Save State
Generate PDF Report
Analyze with Reasoning Model
Push to Splunk
Reset
OVERALL
0
TIER
Level 1 – Minimal Implementation
DEPLOYED
0 / 35
RESIDUAL TTPS
0
ATT&CK MATRIX FILTER
Enterprise
ICS / OT
Uncheck to hide that matrix from tactics, residual TTPs, and reports.
GOV-01
GOVERN
Unknown
Privacy Leadership
A single leader or team is responsible and accountable for managing cyber-related privacy risk.
Assessment
Unknown
Not Started
Scoped/Planned
In-Progress
Implemented
Not Applicable
FEATURES (0/5)
Named privacy accountable role/title
Privacy risk management program policies & procedures
Consider Alberta privacy legislation (POPA / HIA / PIPA)
Policies to limit collection and retention of personal information
RELATED MITRE ATT&CK TACTICS
Not applicable — Not applicable — privacy governance/accountability (Alberta POPA/HIA/PIPA). No direct technical ATT&CK technique.
RESIDUAL ADVERSARY TTPS
Not applicable — no techniques to select for residual risk under the current filter.
GOV-02
GOVERN
Unknown
Supply Chain Incident Reporting Process
Organizations rapidly learn about and respond to known incidents or breaches across vendors and service providers.
Assessment
Unknown
FEATURES (0/4)
Vendor/service provider security incident notification requirement
Specified notification timeframe
Documented in procurement documents and contracts
Included in service level agreements (SLAs)


Edge File Edit View History Favorites Profiles Tab Window Help
Fri Aug 21 3:10 PM
CyberBuddy Frameworks & Cyb
CyberAlberta Compliance Asses
CyberAlberta | CyberAlberta
localhost:8080
Update
Chat
CyberBuddy Frameworks & Cyber Research
CyberAlberta · MITRE ATT&CK · Foundation-Sec / Antares
Maturity 3.9% (5.5/140) Level 1 – Minimal Implementation
Ollama healthy · 9 model(s)
Framework Mappings
LLM Assistance
About / Deploy
GOV-02 GOVERN In-Progress
Supply Chain Incident Reporting Process
Assessment
In-Progress
Organizations rapidly learn about and respond to known incidents or breaches across vendors and service providers.
FEATURES (2/4)
Vendor/service provider security incident notification requirement
Specified notification timeframe
Documented in procurement documents and contracts
Included in service level agreements (SLAs)
RELATED MITRE ATT&CK TACTICS
TA0001 Initial Access
Tactics derived from mapped techniques (ATT&CK v19). Techniques appear under Residual TTPs.
RESIDUAL ADVERSARY TTPS THAT CAN STILL OVERCOME THIS CONTROL (5 SELECTED)
Techniques and sub-techniques supporting the tactics above. Select residual exposure.
T1195 Supply Chain Compromise
T1195.001 Supply Chain Compromise: Compromise Software Dependencies and Development Tools
T1195.002 Supply Chain Compromise: Compromise Software Supply Chain
T1199 Trusted Relationship
T0862 Supply Chain Compromise ICS
GOV-03 GOVERN Unknown
Vendor/Supplier Cybersecurity Requirements
Assessment
Unknown
Risk is reduced by purchasing secure products and services from secure suppliers.
FEATURES (0/4)
Cybersecurity requirements in procurement documents
Cybersecurity questions in procurement/RFP process
Evaluate security in vendor selection
Prefer more secure offering/supplier when cost/function are similar
RELATED MITRE ATT&CK TACTICS
TA0001 Initial Access
Tactics derived from mapped techniques (ATT&CK v19). Techniques appear under Residual TTPs.
RESIDUAL ADVERSARY TTPS THAT CAN STILL OVERCOME THIS CONTROL (0 SELECTED)
Techniques and sub-techniques supporting the tactics above. Select residual exposure.
T1195 Supply Chain Compromise
T1195.001 Supply Chain Compromise: Compromise Software Dependencies and Development Tools
T1195.002 Supply Chain Compromise: Compromise Software Supply Chain
T1199 Trusted Relationship
T0862 Supply Chain Compromise ICS

ATT&CKcon 7.0 in-person tickets are open! Join us October 27-28, 2026 in McLean, VA. Register here for in-person tickets; hotel and location details can be found in the FAQ.

TACTICS
Enterprise
Reconnaissance
Resource Development
Initial Access
Execution
Persistence
Privilege Escalation
Stealth
Defense Impairment
Credential Access
Discovery
Lateral Movement
Collection
Command and Control
Exfiltration
Impact

Home > Tactics > Enterprise > Privilege Escalation

# Privilege Escalation

The adversary is trying to gain higher-level permissions.

Privilege Escalation consists of techniques that adversaries use to gain higher-level permissions on a system or network. Adversaries can often enter and explore a network with unprivileged access but require elevated permissions to follow through on their objectives. Common approaches are to take advantage of system weaknesses, misconfigurations, and vulnerabilities. Examples of elevated access include:

- SYSTEM/root level
- local administrator
- user account with admin-like access
- user accounts with access to specific system or perform specific function

These techniques often overlap with Persistence techniques, as OS features that let an adversary persist can execute in an elevated context.

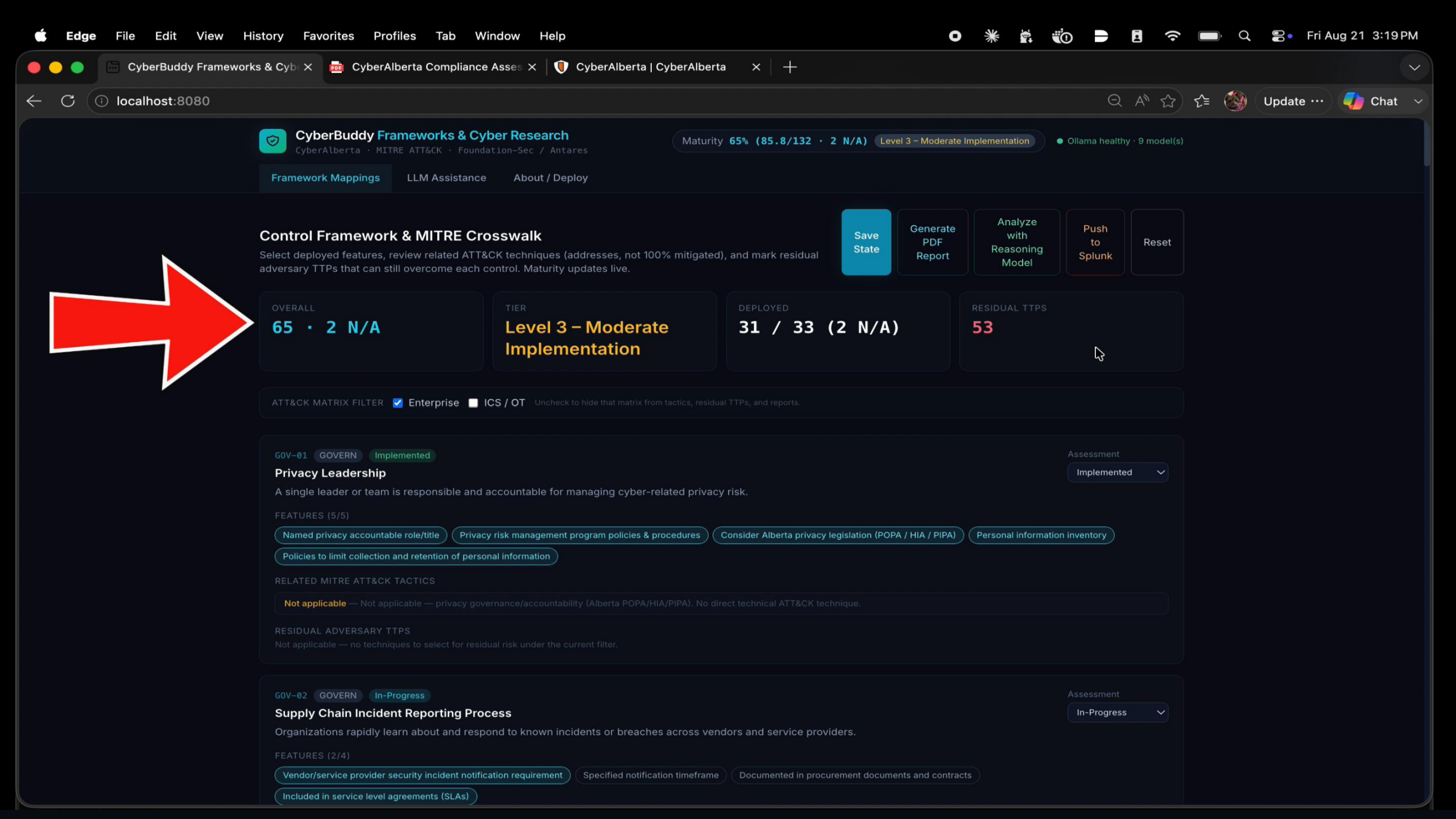
**ID:** TA0004
**Created:** 17 October 2018
**Last Modified:** 25 April 2025

Version Permalink

## Techniques

Techniques: 13

| ID | Name | Description |
|---|---|---|
| T1548 | Abuse Elevation Control | Adversaries may circumvent mechanisms designed to control privilege elevation to gain higher-level |


Edge File Edit View History Favorites Profiles Tab Window Help
Fri Aug 21 3:19 PM
CyberBuddy Frameworks & Cyb
CyberAlberta Compliance Asses
CyberAlberta | CyberAlberta
localhost:8080
Update
Chat
CyberBuddy Frameworks & Cyber Research
CyberAlberta · MITRE ATT&CK · Foundation-Sec / Antares
Maturity 65% (85.8/132 · 2 N/A) Level 3 – Moderate Implementation
Ollama healthy · 9 model(s)
Framework Mappings
LLM Assistance
About / Deploy
Control Framework & MITRE Crosswalk
Select deployed features, review related ATT&CK techniques (addresses, not 100% mitigated), and mark residual adversary TTPs that can still overcome each control. Maturity updates live.
Save State
Generate PDF Report
Analyze with Reasoning Model
Push to Splunk
Reset
OVERALL
65 · 2 N/A
TIER
Level 3 – Moderate Implementation
DEPLOYED
31 / 33 (2 N/A)
RESIDUAL TTPS
53
ATT&CK MATRIX FILTER
Enterprise
ICS / OT
Uncheck to hide that matrix from tactics, residual TTPs, and reports.
GOV-01 GOVERN Implemented
Assessment
Implemented
Privacy Leadership
A single leader or team is responsible and accountable for managing cyber-related privacy risk.
FEATURES (5/5)
Named privacy accountable role/title
Privacy risk management program policies & procedures
Consider Alberta privacy legislation (POPA / HIA / PIPA)
Personal information inventory
Policies to limit collection and retention of personal information
RELATED MITRE ATT&CK TACTICS
Not applicable — Not applicable — privacy governance/accountability (Alberta POPA/HIA/PIPA). No direct technical ATT&CK technique.
RESIDUAL ADVERSARY TTPS
Not applicable — no techniques to select for residual risk under the current filter.
GOV-02 GOVERN In-Progress
Assessment
In-Progress
Supply Chain Incident Reporting Process
Organizations rapidly learn about and respond to known incidents or breaches across vendors and service providers.
FEATURES (2/4)
Vendor/service provider security incident notification requirement
Specified notification timeframe
Documented in procurement documents and contracts
Included in service level agreements (SLAs)

# CyberBuddy Frameworks & Cyber Research

CyberAlberta · MITRE ATT&CK · Foundation-Sec / Antares

Maturity 65% (85.8/132 · 2 N/A) Level 3 – Moderate Implementation

Ollama healthy · 9 model(s)

Framework Mappings | LLM Assistance | About / Deploy

## Control Framework & MITRE Crosswalk

Select deployed features, review related ATT&CK techniques (addresses, not 100% mitigated), and mark r
adversary TTPs that can still overcome each control. Maturity updates live.

Analyze with Reasoning Model | Push to Splunk | Reset

| OVERALL | TIER | DEPLOYED | RESIDUAL TTPS |
|---|---|---|---|
| 65 · 2 N/A | Level 3 – Moderate Implementation | 31 / 33 (2 N/A) | 53 |

ATT&CK MATRIX FILTER ☑ Enterprise ☐ ICS / OT Uncheck to hide that matrix from tactics, residual TTPs, and reports.

GOV-01 GOVERN Implemented

Assessment: Implemented

### Privacy Leadership

A single leader or team is responsible and accountable for managing cyber-related privacy risk.

FEATURES (5/5)

Named privacy accountable role/title | Privacy risk management program policies & procedures | Consider Alberta privacy legislation (POPA / HIA / PIPA) | Personal information inventory | Policies to limit collection and retention of personal information

RELATED MITRE ATT&CK TACTICS

Not applicable — Not applicable — privacy governance/accountability (Alberta POPA/HIA/PIPA). No direct technical ATT&CK technique.

RESIDUAL ADVERSARY TTPS

Not applicable — no techniques to select for residual risk under the current filter.

GOV-02 GOVERN In-Progress

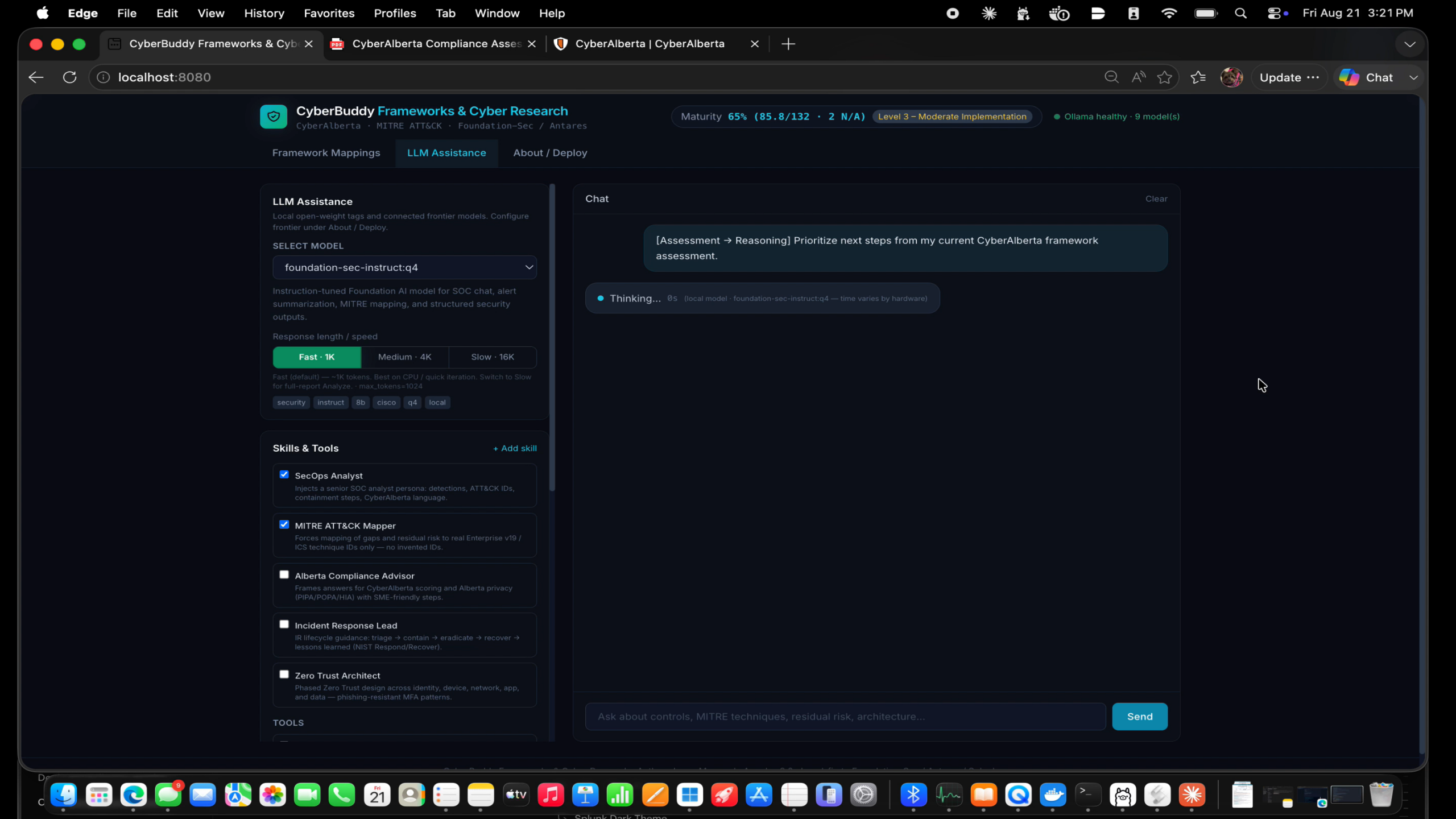
Assessment: In-Progress

### Supply Chain Incident Reporting Process

Organizations rapidly learn about and respond to known incidents or breaches across vendors and service providers.

FEATURES (2/4)

Vendor/service provider security incident notification requirement | Specified notification timeframe | Documented in procurement documents and contracts | Included in service level agreements (SLAs)


Edge File Edit View History Favorites Profiles Tab Window Help
Fri Aug 21 3:21 PM
CyberBuddy Frameworks & Cyb
CyberAlberta Compliance Asses
CyberAlberta | CyberAlberta
localhost:8080
Update
Chat
CyberBuddy Frameworks & Cyber Research
CyberAlberta · MITRE ATT&CK · Foundation-Sec / Antares
Maturity 65% (85.8/132 · 2 N/A) Level 3 – Moderate Implementation
Ollama healthy · 9 model(s)
Framework Mappings
LLM Assistance
About / Deploy
LLM Assistance
Local open-weight tags and connected frontier models. Configure frontier under About / Deploy.
SELECT MODEL
foundation-sec-instruct:q4
Instruction-tuned Foundation AI model for SOC chat, alert summarization, MITRE mapping, and structured security outputs.
Response length / speed
Fast · 1K
Medium · 4K
Slow · 16K
Fast (default) — ~1K tokens. Best on CPU / quick iteration. Switch to Slow for full-report Analyze. · max_tokens=1024
security
instruct
8b
cisco
q4
local
Skills & Tools
+ Add skill
SecOps Analyst
Injects a senior SOC analyst persona: detections, ATT&CK IDs, containment steps, CyberAlberta language.
MITRE ATT&CK Mapper
Forces mapping of gaps and residual risk to real Enterprise v19 / ICS technique IDs only — no invented IDs.
Alberta Compliance Advisor
Frames answers for CyberAlberta scoring and Alberta privacy (PIPA/POPA/HIA) with SME-friendly steps.
Incident Response Lead
IR lifecycle guidance: triage → contain → eradicate → recover → lessons learned (NIST Respond/Recover).
Zero Trust Architect
Phased Zero Trust design across identity, device, network, app, and data — phishing-resistant MFA patterns.
TOOLS
Chat
Clear
[Assessment → Reasoning] Prioritize next steps from my current CyberAlberta framework assessment.
Thinking... 0s (local model · foundation-sec-instruct:q4 — time varies by hardware)
Ask about controls, MITRE techniques, residual risk, architecture...
Send

# If you give it hands, give it a leash.

Open WebUI is a co-pilot. Skills are text. Tools are reviewed. You stay in the loop.

OpenClaw-style agents remember, run in the background, and can hold a shell. That is an intern with admin and a company card.

Start with the co-pilot and the earn the intern.

OPENCLAW



# Govern. Inspect. Prove.

01

## Govern



Admit, quarantine, or block. Nothing loads until it is scanned.

02

## Inspect




Observe. Action. Action + HiTL. HIGH pauses for a person. CRITICAL does not wait.

03

## Prove




Allow, alert, confirm, or block — on the tape. Attributable action.

Observe → Action → HiTL. Shared language: NIST AI RMF, MITRE ATLAS, OWASP LLM/Agent Top 10. DefenseClaw is Apache 2.0



Confidential

ATTACK PATHS

# Inspect every hop or the last hop owns you.

User → Agent → Agent → MCP → Tools / Skills



| 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|
| **Install** | **Poison** | **Inherit** | **Inject** | **Act** | **Leave** |
| Shadow agent on a laptop. Often authentication is off. | Helpful skill / MCP / weights. | Dev token + mailbox. No identity. | Ticket body becomes the runbook. (the payload) | Tools fire as the user. No repudation | Secrets out, data lost. Incident begins |



Confidential

LEAVE WITH THIS

# Monday morning blueprint.

1

## Stand up local

Ollama + Open WebUI + Docker. Load quantized Foundation-Sec Instruct.

2

## Write one skill

Your triage SOP. Output contract. No invented ATT&CK IDs.

3

## Add one corpus

Playbooks and standards you already trust. Classify it first.

4

## Add tools last

One reviewed lookup. Treat it as a new processing activity.

5

## Govern autonomy

If it gets hands, put DefenseClaw — or equivalent — in front of them.



Confidential

RESOURCES

# Sharing is caring.

### LLM Security Leaderboard

leaderboard.aidefense.cisco.com/rankings

### Antares collection

huggingface.co/collections/fdtn-ai/antares

### AI Defense Explorer Edition

explorer.aidefense.cisco.com

### Foundry Security Spec

github.com/CiscoDevNet/foundry-security-spec

### DefenseClaw

github.com/cisco-ai-defense/defenseclaw

### Project CodeGuard

project-codeguard.org

### Foundation-Sec-8B

huggingface.co/fdtn-ai/Foundation-Sec-8B

### Agentic Identity

duo.com/solutions/agentic-ai-security

### Framework Mapping

learn-cloudsecurity.cisco.com/ai-security-framework



Confidential

# OWN THE BOX.
# WRAP THE MODEL.
# LEASH THE HANDS.

Jason Maynard · Field CTO, Cybersecurity – Canada · Cisco

I will stay after. Bring the weird edge case — especially the privacy one.



Confidential