The bridge to possible

Automating detection and response outcomes using Cisco XDR and Generative AI

Aman Sardana, Scott Dozier
Sr. Product Architects, CX Lifecycle Services & Automation
@amsardana, @ScottDozier_

BRKATO-1577

cisco Live!

Cisco Webex App

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKATO-1557

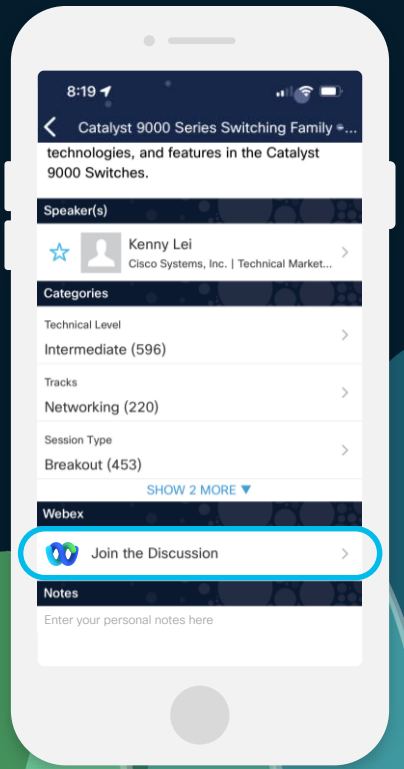
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 7, 2024.

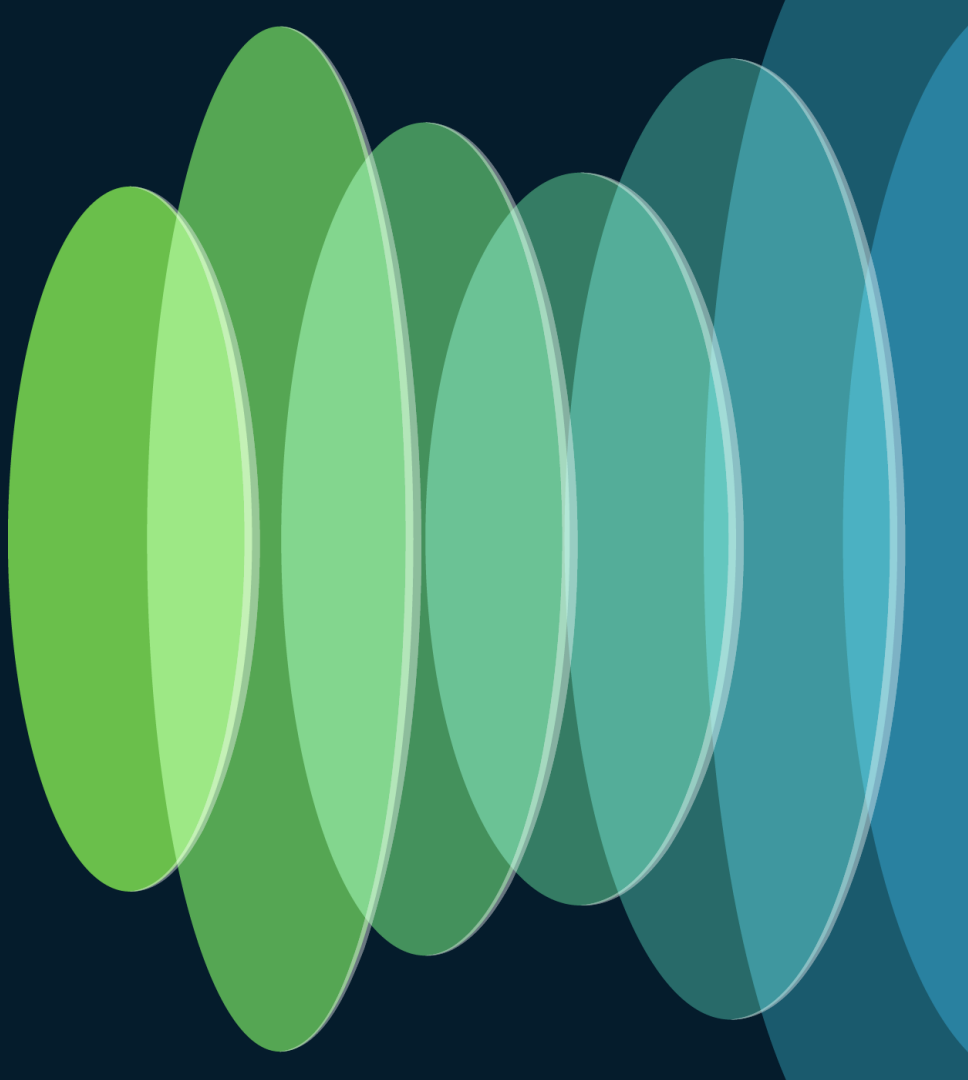


cisco Live!

Agenda

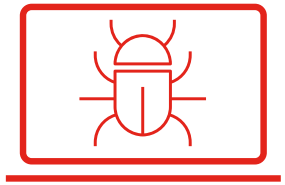
- Automating with XDR Automate
- How can Generative AI help?
- Our Framework
- Demo
- Our Learnings
- Cisco XDR Premier
  We do it for you.
- Q&A

Automating with XDR Automate



cisco Live!

Scenario



Your organization has several remote employees who are using their personal devices to access sensitive company data.

One of the employee's laptops gets infected with ransomware that attempts to establish command and control communication before initiating data encryption.

Detection

Umbrella identifies the DNS request for a malicious domain

Investigation

Cisco XDR gathers the event information generated by Cisco Umbrella

- Nature of threat, associated domain, details about the affected employee's device

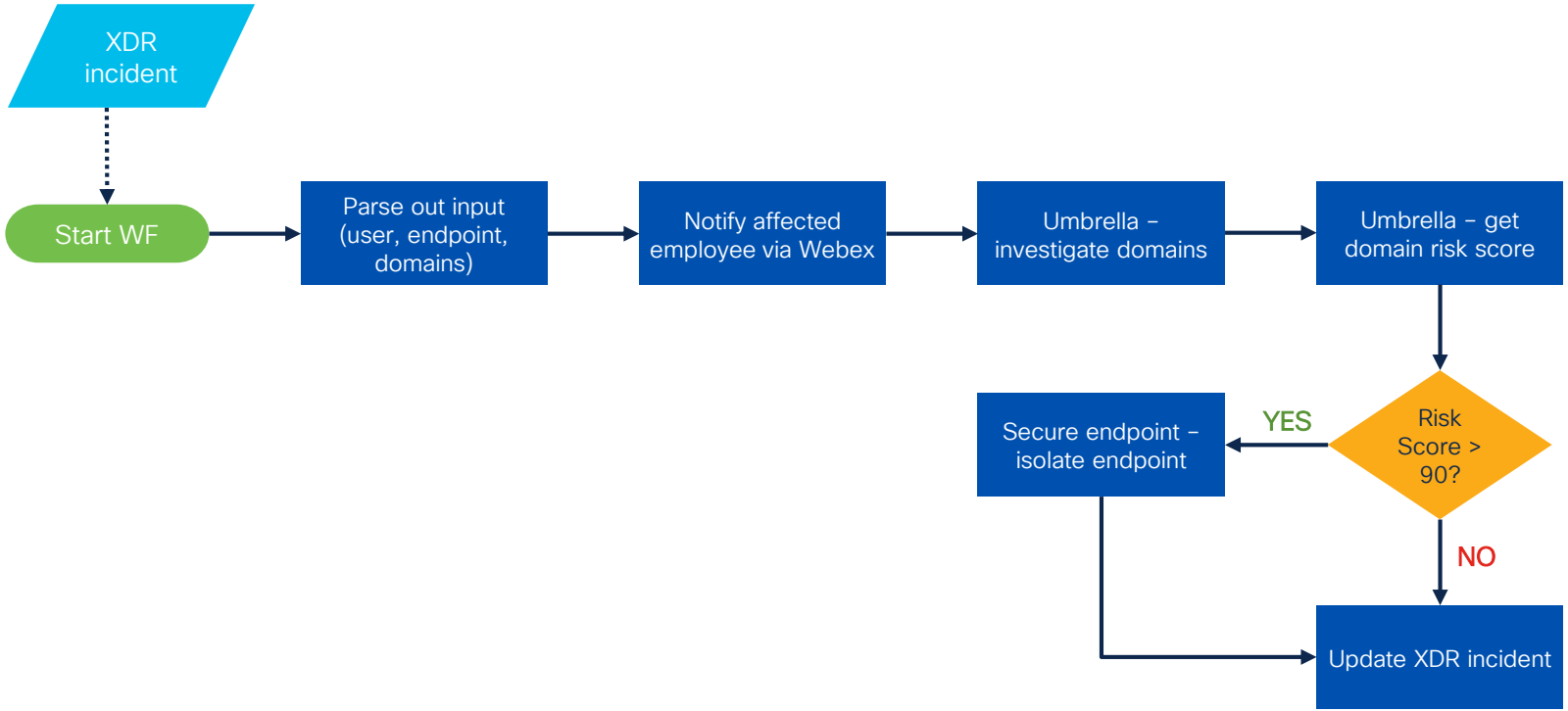
Automated Remediation

Cisco XDR Automate triggers an automated response workflow to remediate impact, notify teams and document actions

Validation and Monitoring

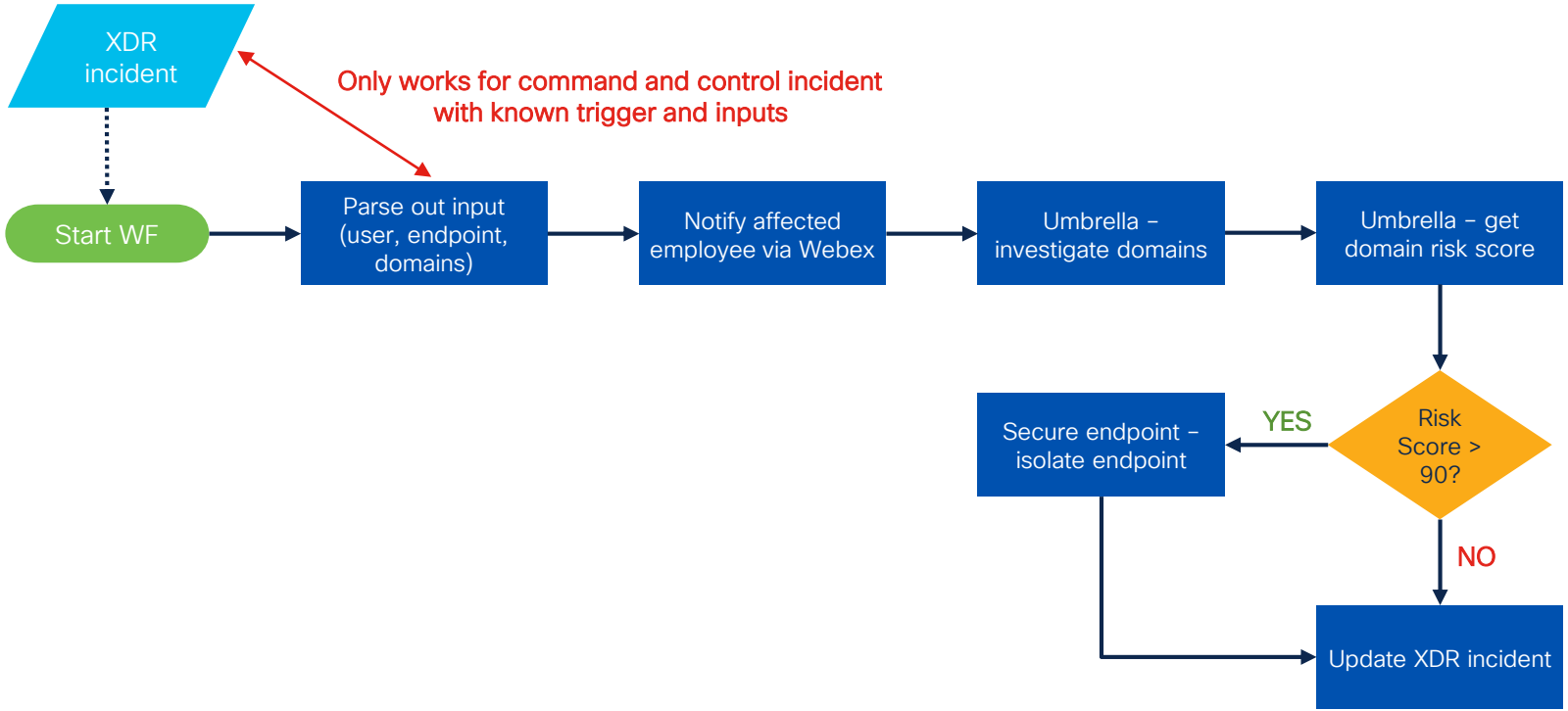
Continuous monitoring to ensure employee's device is secure from future threats

Typical Command & Control Response Workflow



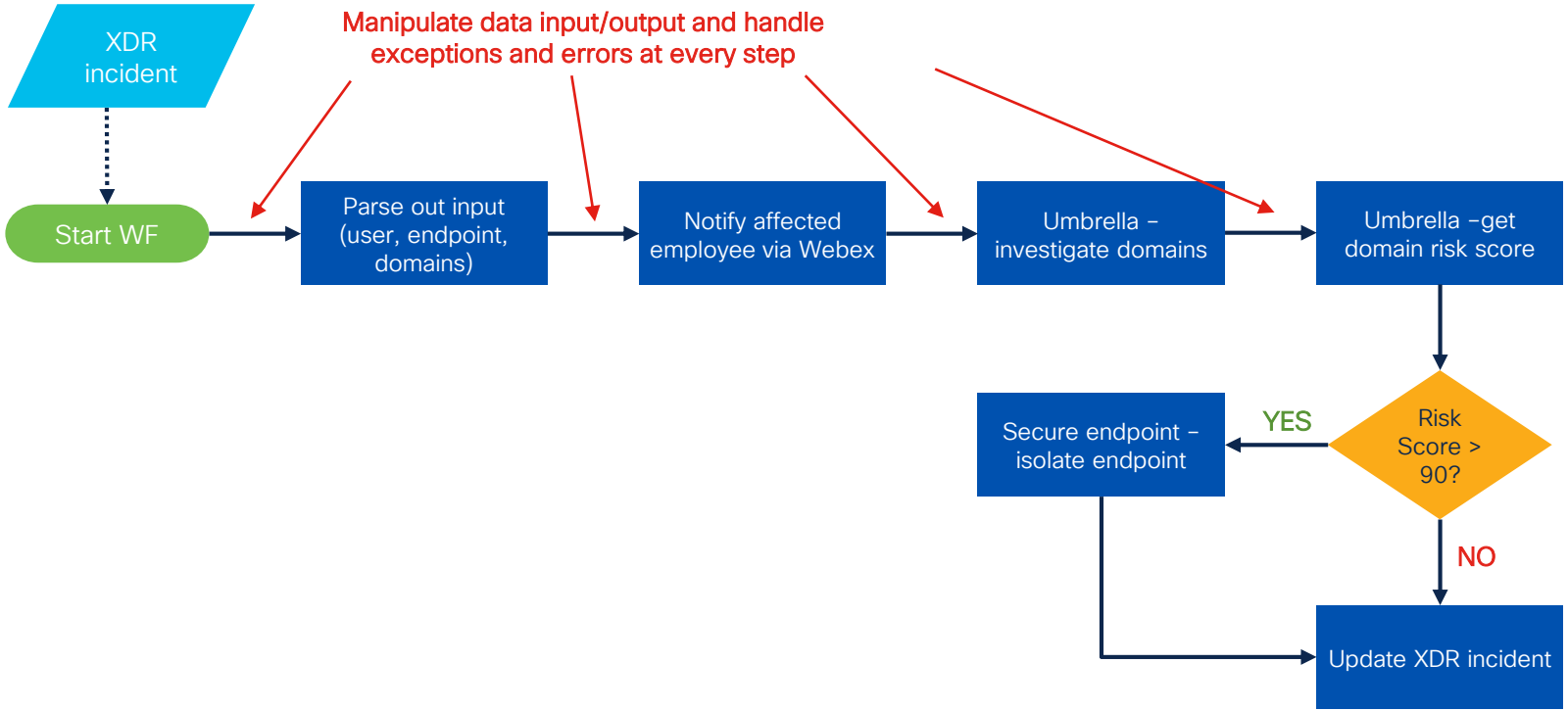
Observations

What kind of incidents can this handle?



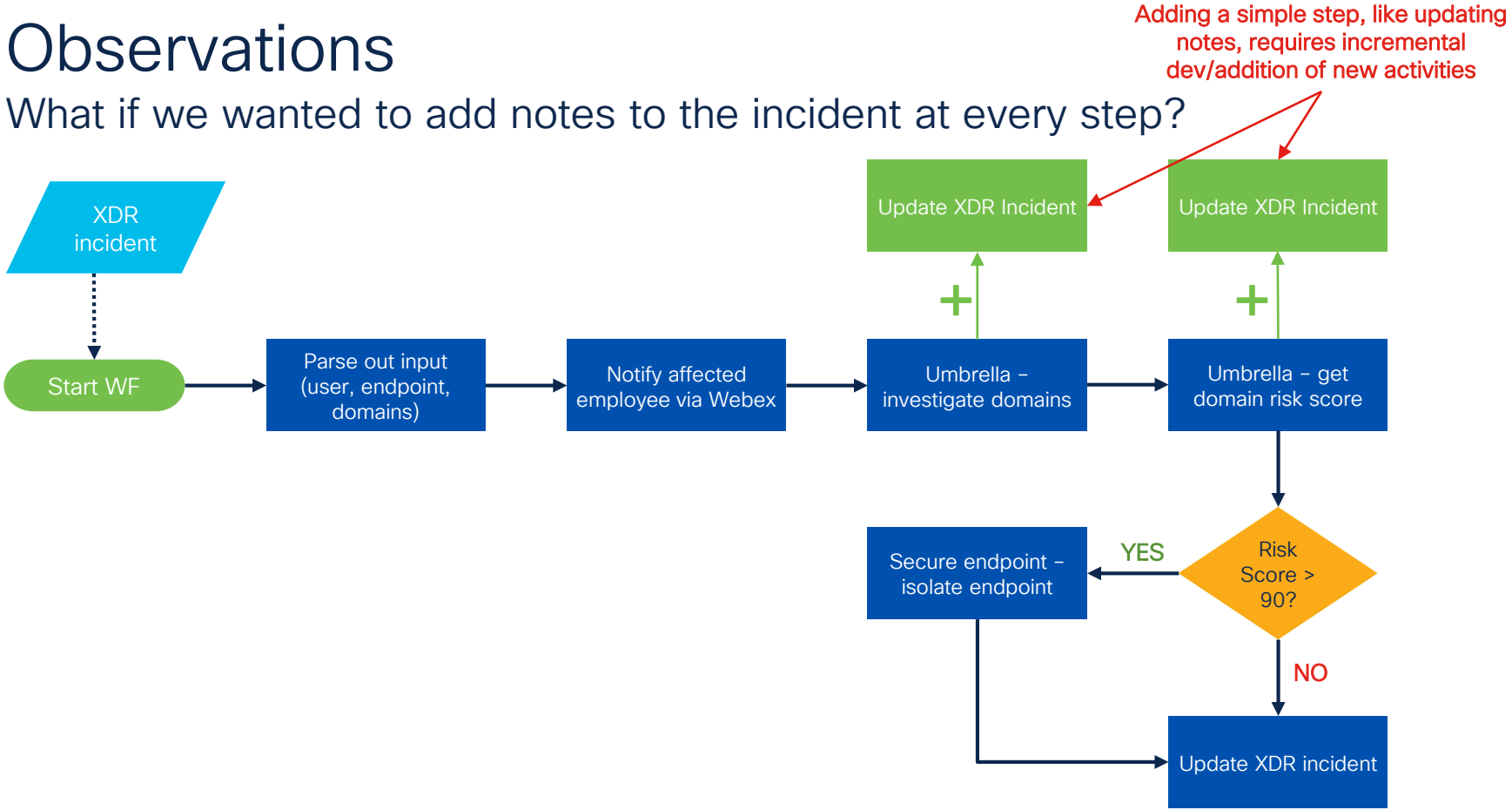
Observations

How do we handle data manipulation and errors/exceptions?

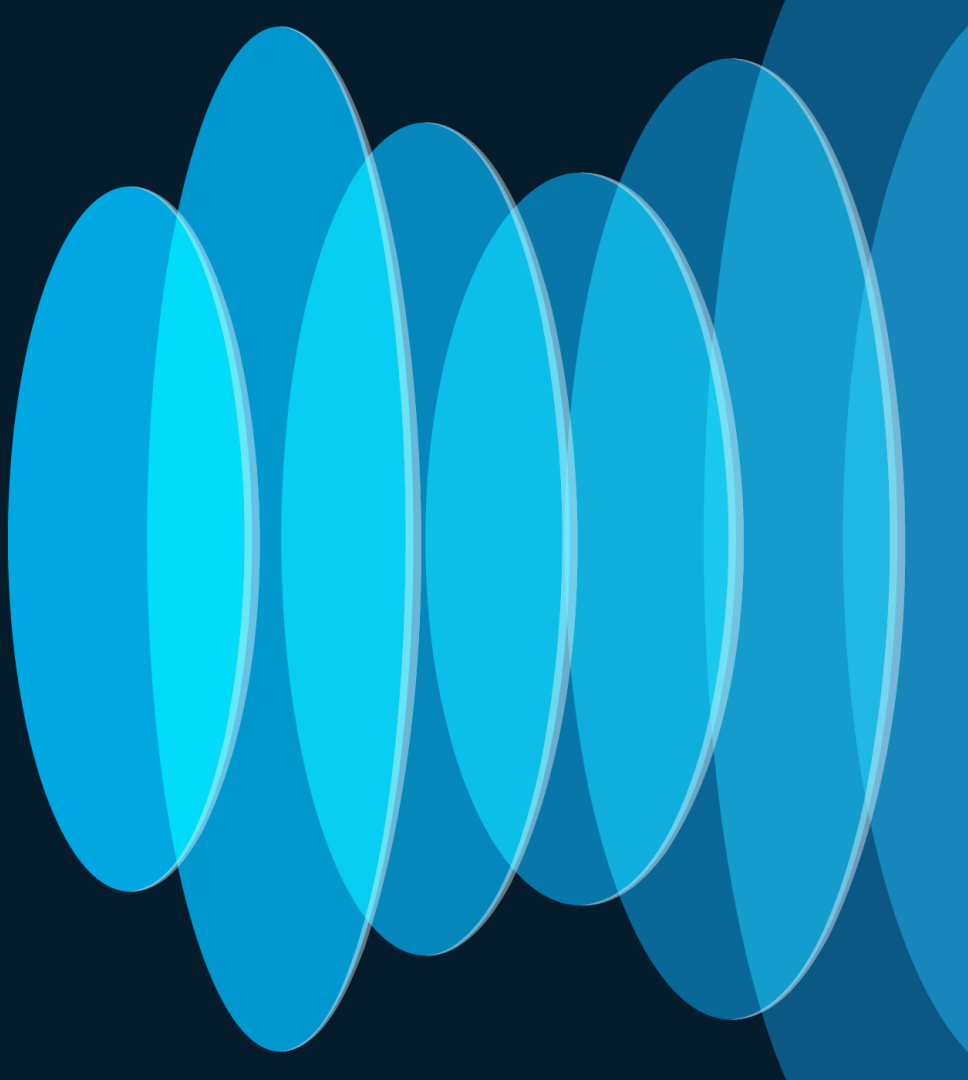


Observations

What if we wanted to add notes to the incident at every step?



How can Generative AI help?



Workflow Authoring Approaches

1

Rules based workflow authoring

Define purpose-built actions, logic, handle errors/exceptions *(but that's so 2023?!)*

When to use: Singular use-case trigger, consistent inputs and outputs, require highly predictable path to outcome

2

AI driven workflows + specialized tools

Large language models drive the workflow, augmented with specialized tools

When to use: Multitude of use-cases as triggers, well-known and documented actions, controlled flexibility in path to get to outcome

3

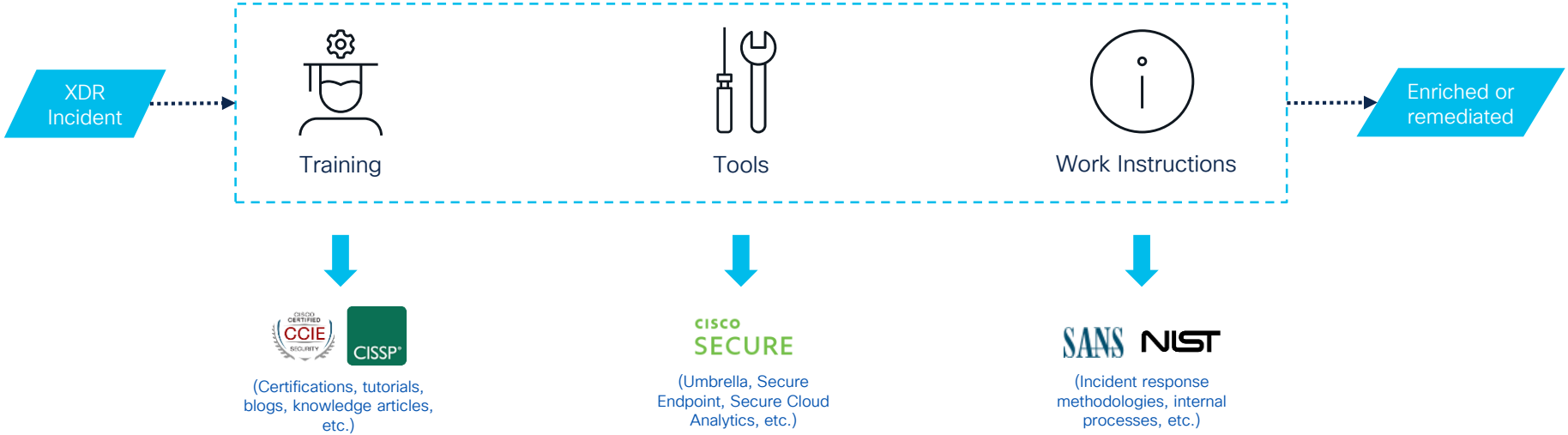
Natural language-based workflow authoring

Describe what you want a response workflow to do in natural language and AI creates the right agents and tools for you

When to use: Low complexity workflows with well-known documented actions, unpredictable path to outcome acceptable

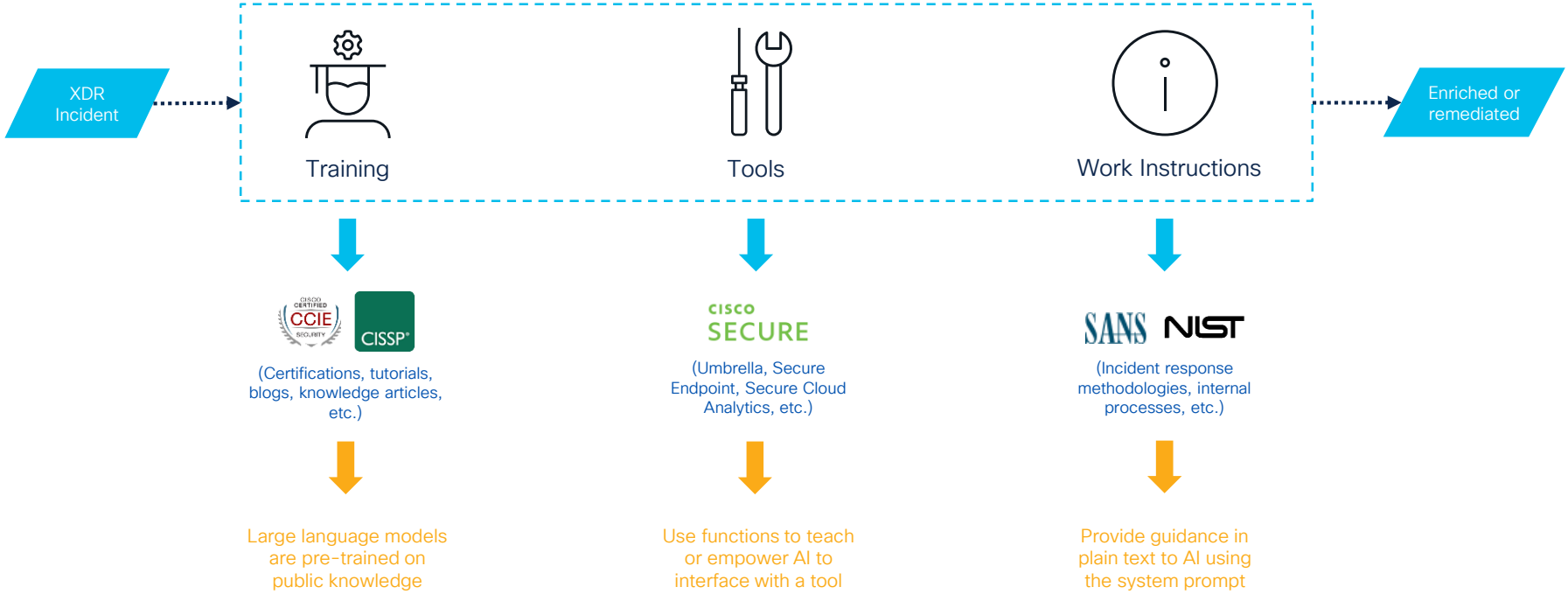
AI driven workflows + specialized tools

How would you train a SOC investigator to deal with security incidents?



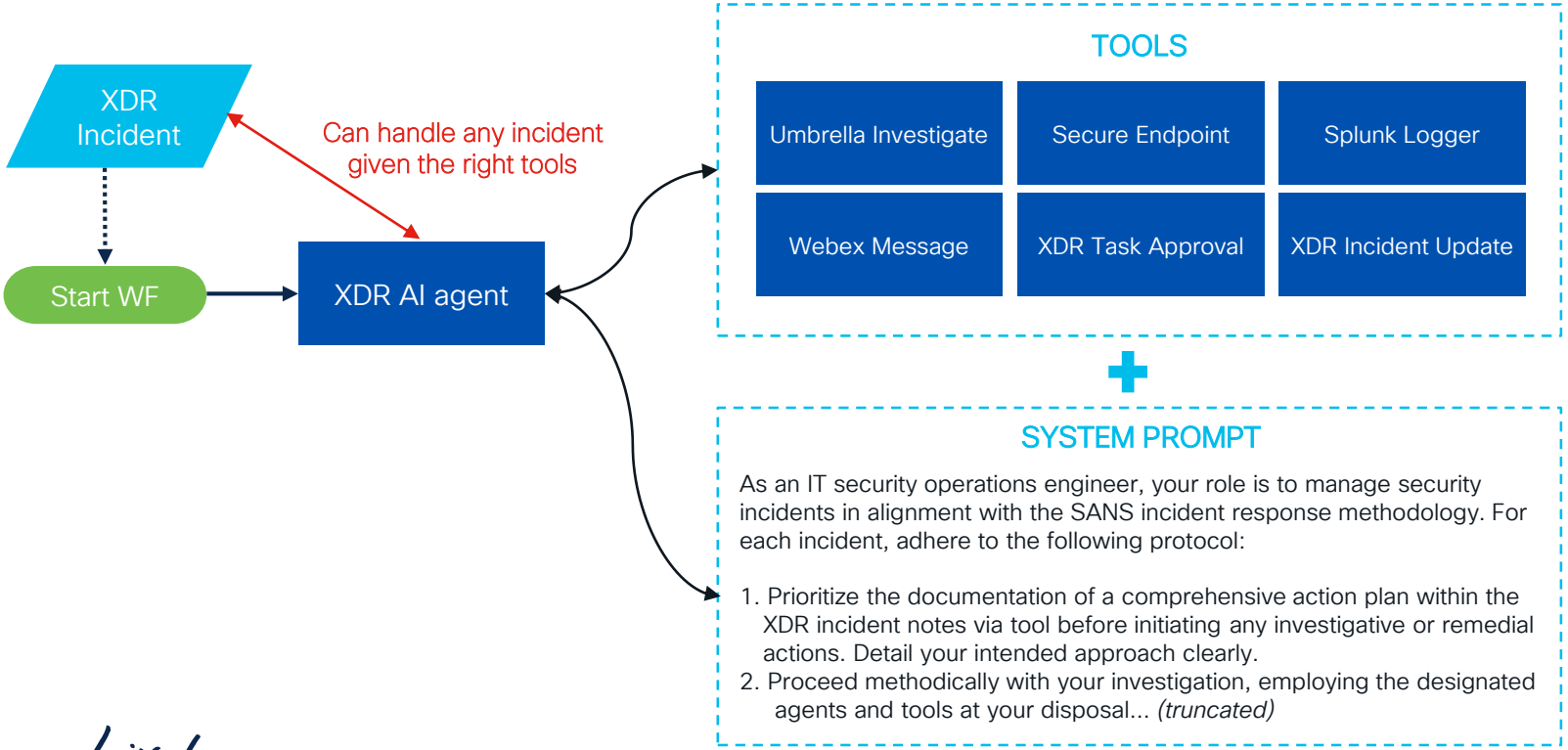
AI driven workflows + specialized tools

AI as a natural extension of how humans learn and operate



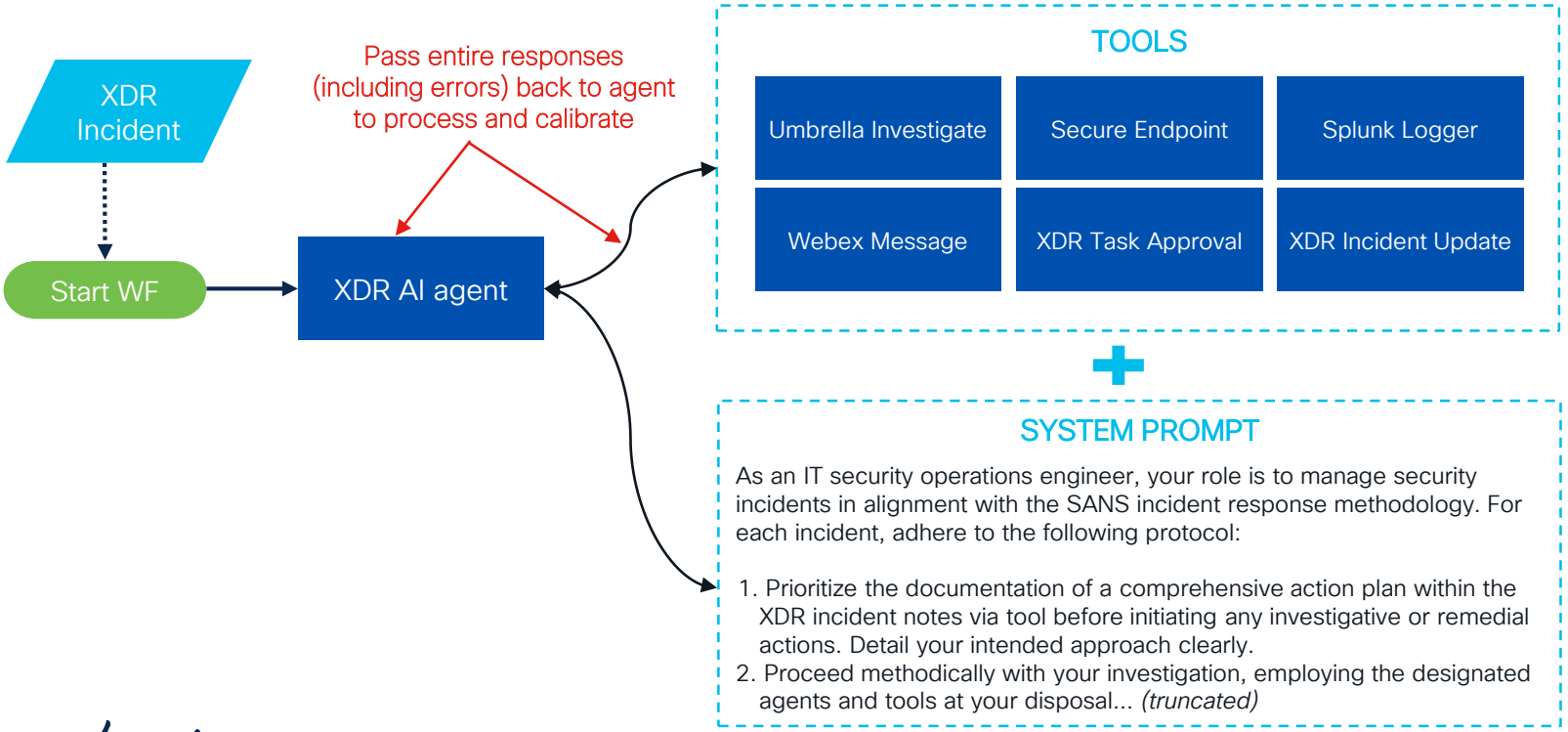
AI driven workflows + specialized tools

What kind of incidents can this architecture handle?



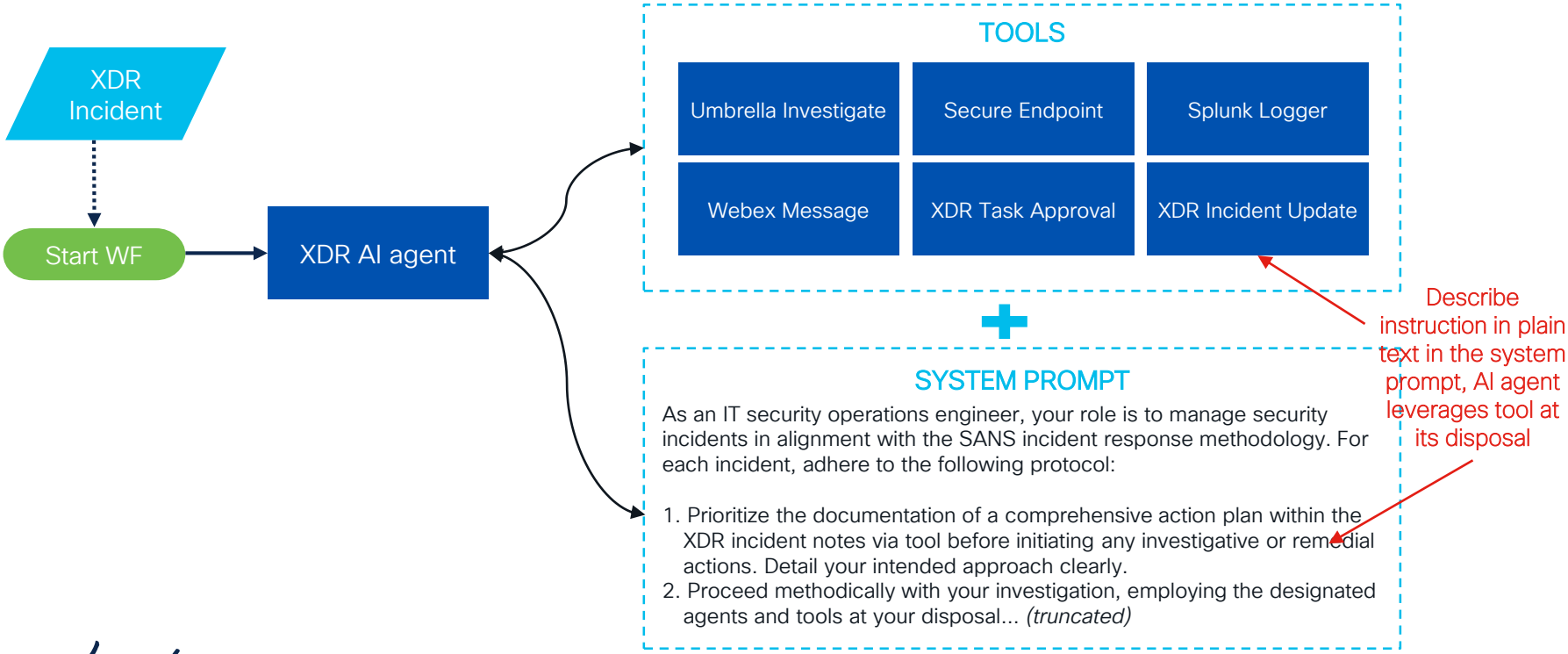
AI driven workflows + specialized tools

How do we handle data manipulation and errors/exceptions?



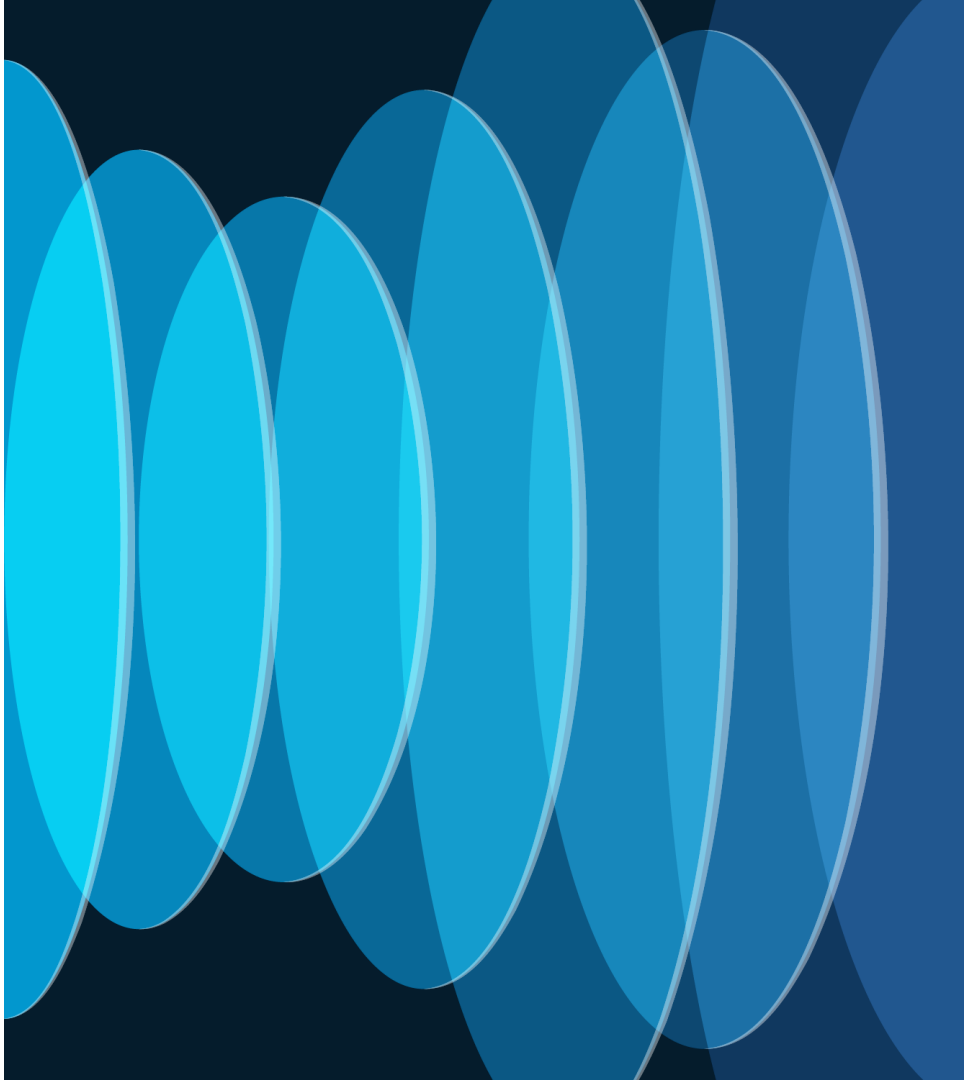
AI driven workflows + specialized tools

What if we wanted to add notes to the incident at every step?



Let’s talk about the *how.*

A primer on OpenAI chat completion



cisco Live!

A Basic OpenAI Chat Completion Request

User query

How can I isolate an endpoint?

Chat completion request

System message

You are an expert on Cisco Secure Endpoint. Provide a single sentence answer.

User message

How can I isolate an endpoint?

LLM response

Assistant message

You can isolate an endpoint by navigating to the device's trajectory page in the console and clicking on the "Isolate" button.

OpenAI Tools (Functions) as Enabler

AI *without* functions

- An LLM can only respond with the data in the request or its training data
  - No real-time data, only knowledge up to time of training
  - No access to the outside

AI *with* functions

- Function calling allows you to connect the LLM to external tools
  - Create powerful AI applications!
    - Allow the LLM to perform reasoning and decide which tools to use to solve the task.
    - The LLM will now utilize tool calls to perform actions, pull real-time information, etc.

NOTE: Access to outside is only given indirectly through the application.

Chat Completion Request with Functions

User query

Tell me about domain monsteradds.at

Chat completion request

System message

You are an IT security expert, use tools and knowledge to answer questions.

User message

Tell me about domain monsteradds.at

Functions

Umbrella Investigate

Uses Investigate API to lookup a domain.

Inputs:

- domain_name

LLM response

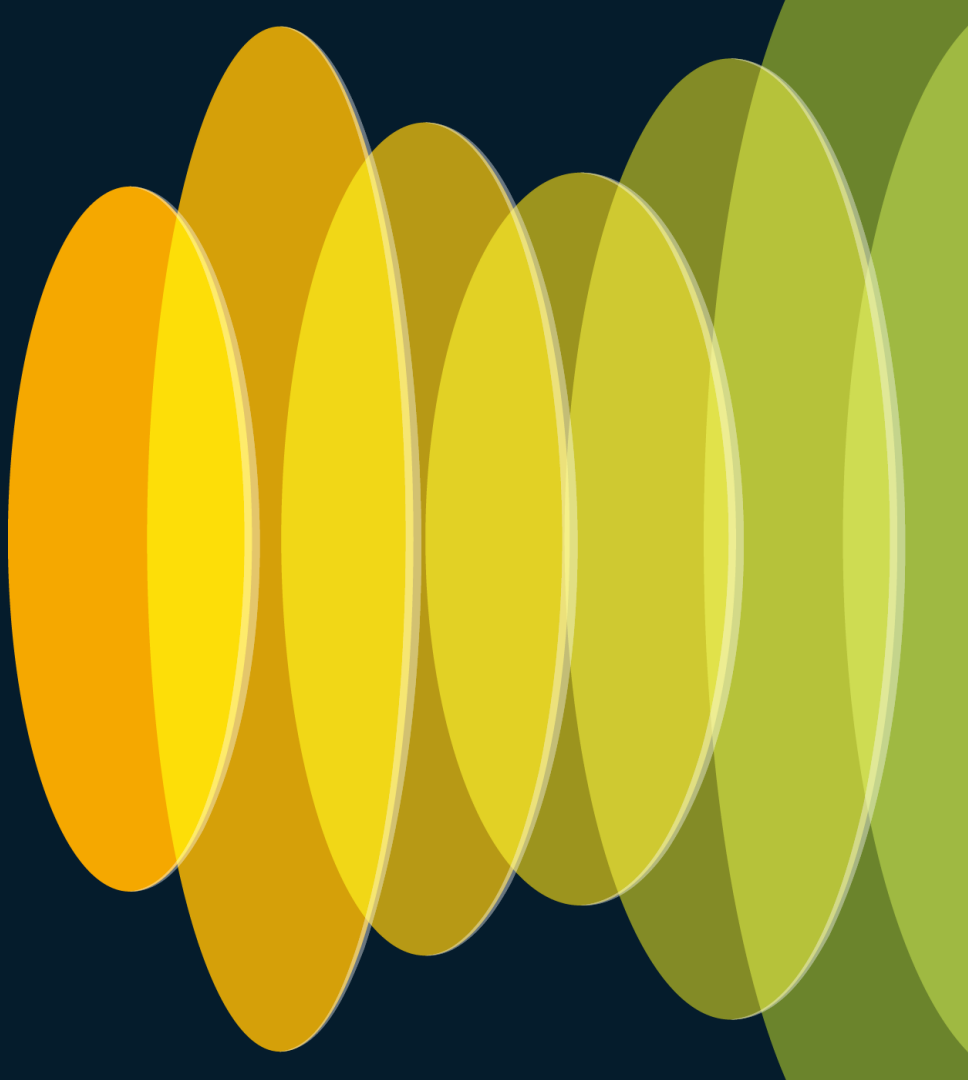
Assistant message

I will investigate the domain with Umbrella Investigate

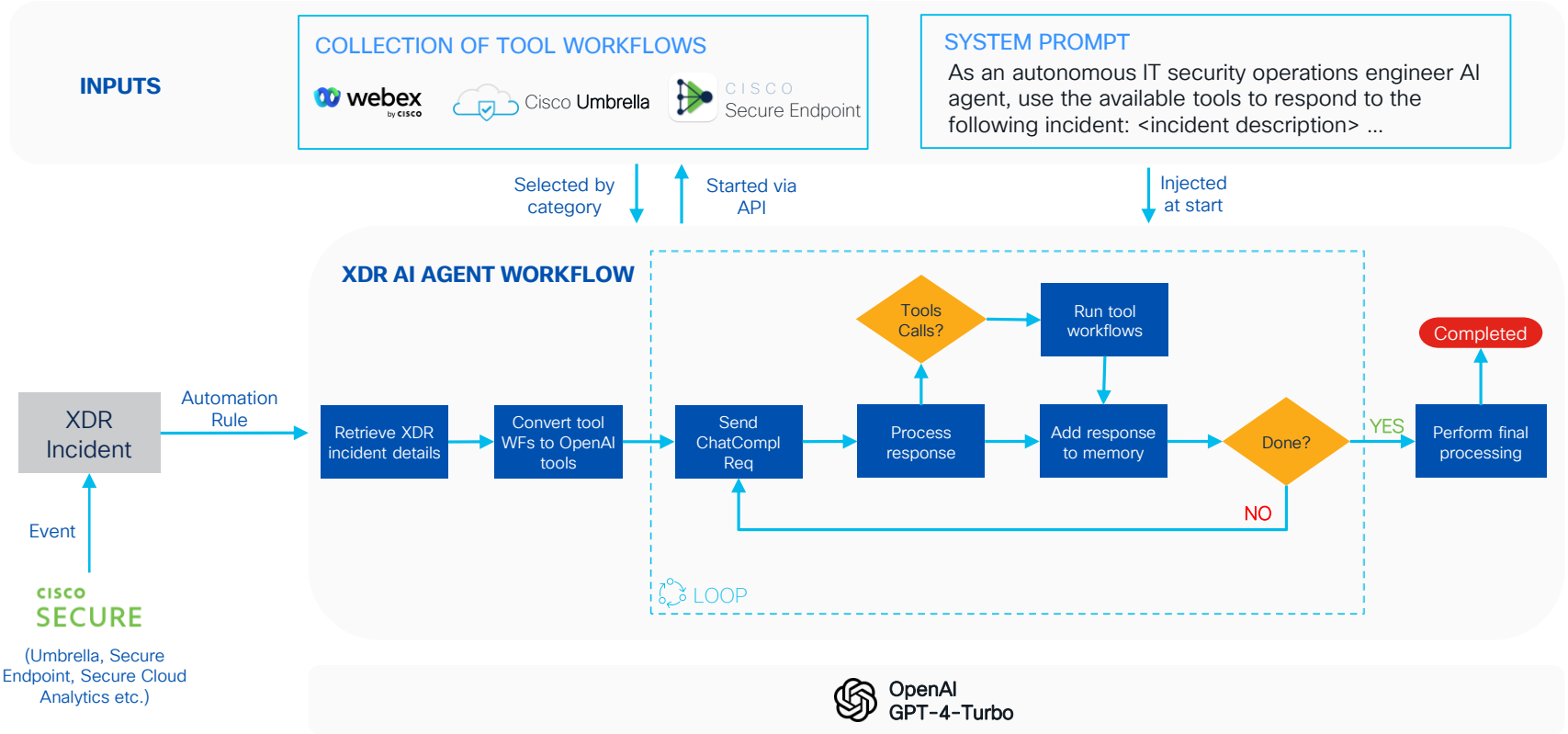
Function call

Function Name: Umbrella Investigate
domain_name: monsteradds.at

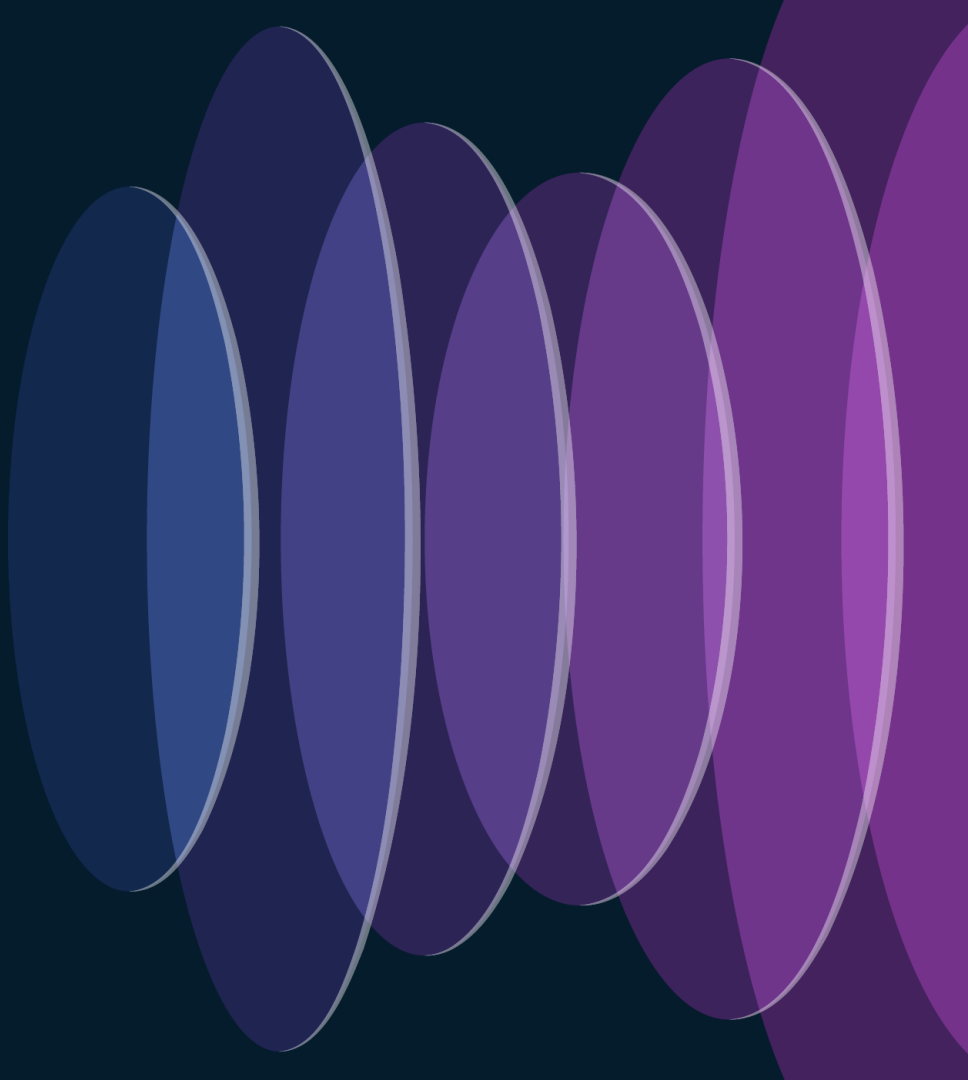
Our Framework



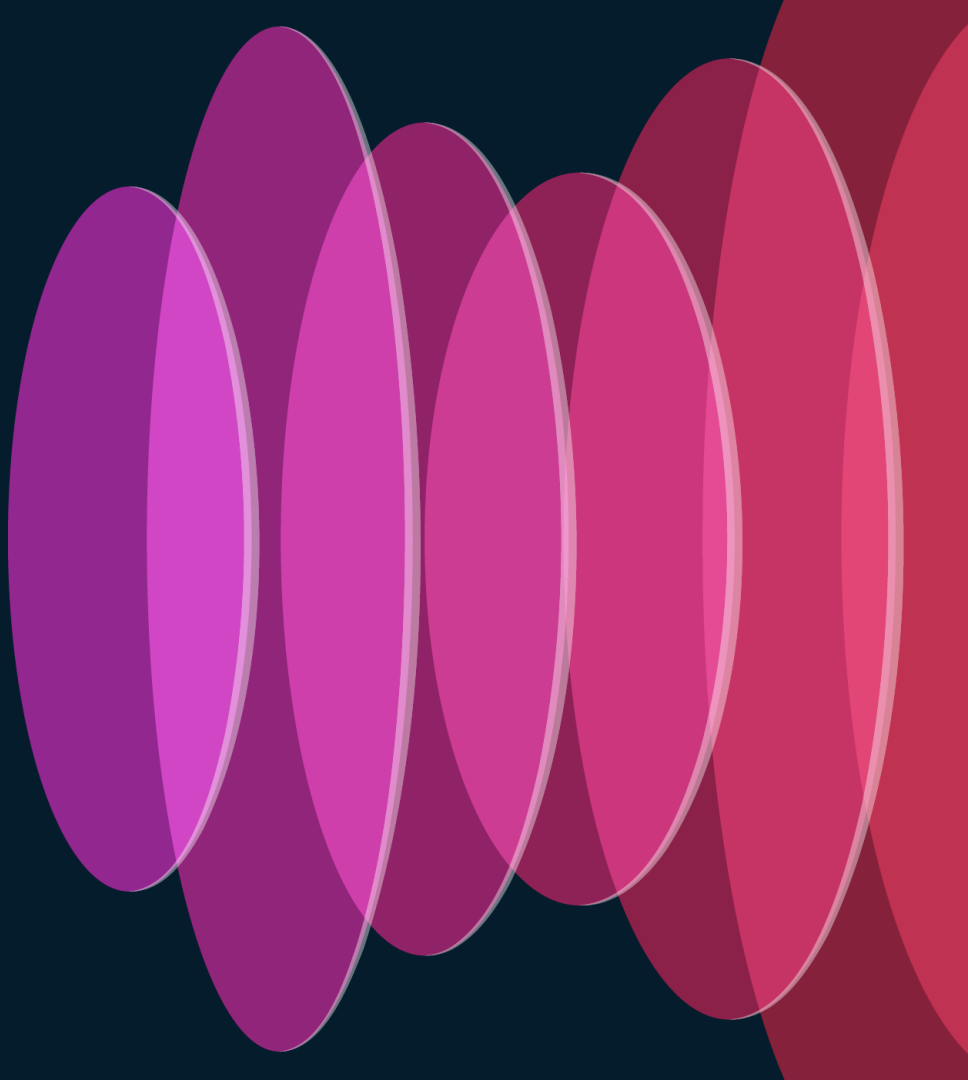
Architecture



Demo



Our Learnings



Learnings and Considerations

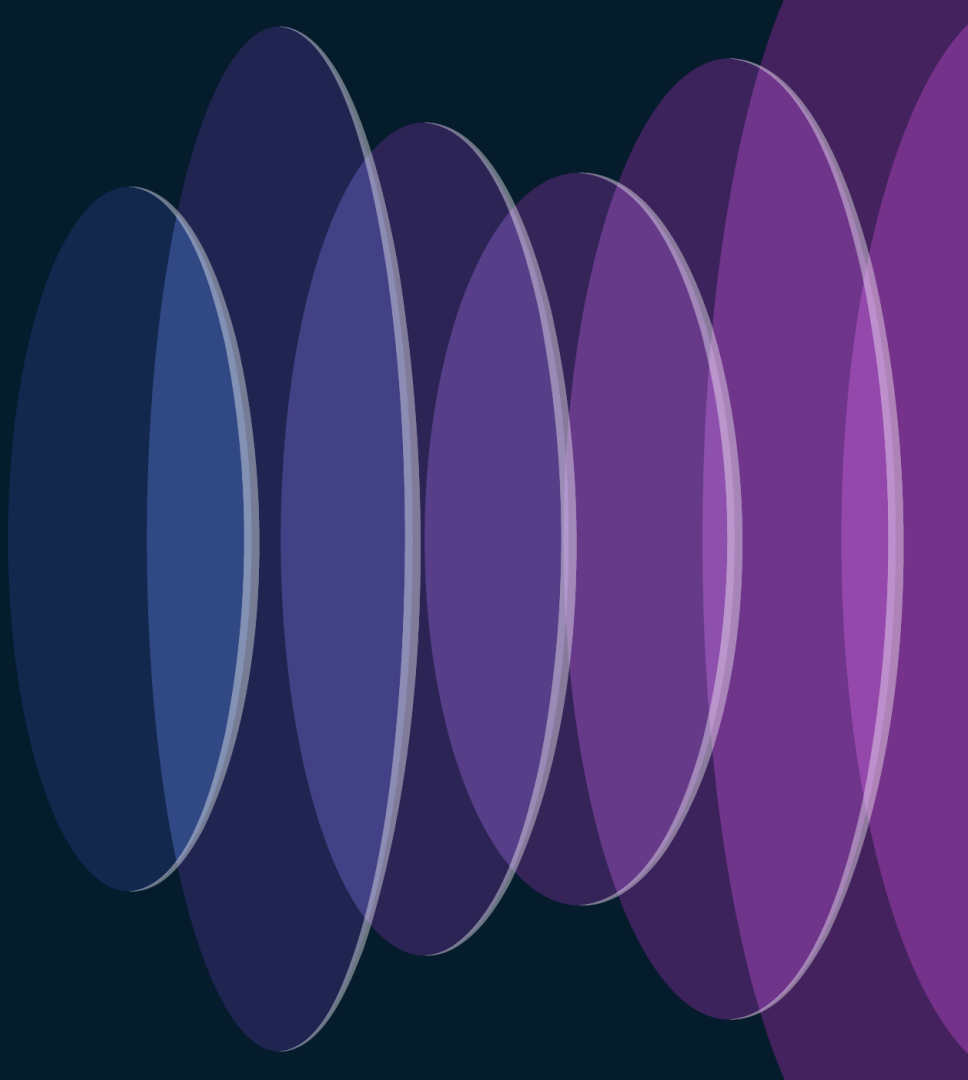
- Be specific in your descriptions
  - For example, say Webex is for notification only
- Don’t assume the LLM understands all APIs equally
  - Add more context to tool descriptions or abstract it to a series of actions for better results
- Limit length of responses from tools through prompting and/or workflow truncation
  - Secure Endpoint can send VERY large responses!
- Don't assume AI will add parameters to URLs
  - Instead give params as an input

What tools could you create?

- More AI Agents
  - Agent to work through specific change processes
  - Agent to interact with users
- ServiceNow
  - Lookup information from your CMDB
  - Update incidents and changes
- Change auto approver based on decision trees
- Google search
- Other security products (ISE, Secure Firewall, Crowdstrike, SonarCube, etc.)

XDR Premier

We do it for you.



Cisco XDR Premier Highlights

Strengthened security, empowered customers

Cisco Managed Extended Detection and Response

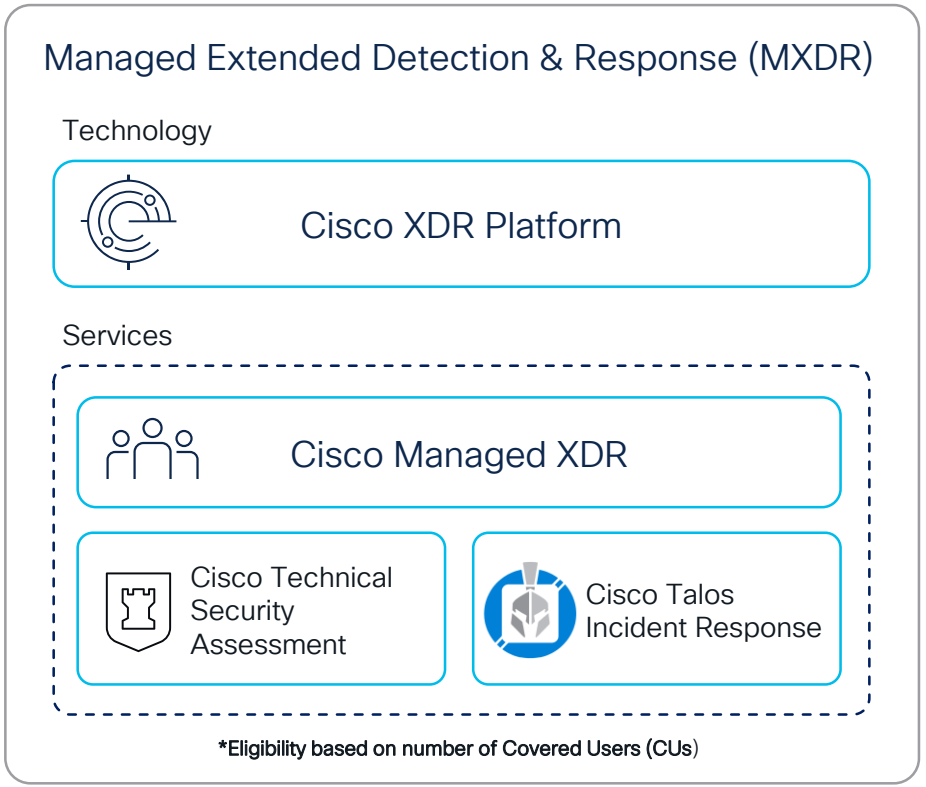
- 24x7x365 Monitoring
- Dedicated threat intelligence team
- Human-centric customer engagement
- Expert analysis and investigation
- XDR Premier Service Portal
- Limited false positive tuning
- Tailored incident mitigation recommendation

Cisco Technical Security Assessment

- Threat modeling
- Threat mitigation: security architecture assessments
- Threat simulation exercises: Red Team and Pen Testing

Cisco Talos Incident Response

- Prepare IR plans or playbooks
- Testing with Tabletop exercise
- Provides digital forensics



What's next?

Interact with experts on Webex:
https://ciscolive.ciscoevents.com/ciscolivebot/#BRKATO-1557

Visit the XDR Premier booth at the World of Solutions

View session content on GitHub:
http://cs.co/cl-xdr-automate-genai

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn **exclusive prizes!**

Complete your surveys in the **Cisco Live mobile app.**

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Thank you