

Automating OSINT Using AI Agents

Chase E Hanson

Western Governors University

## Table of Contents

A.	Proposal Overview	3
A.1	Problem Summary.....	3
A.2	IT Solution.....	4
A.3	Implementation Plan.....	4
B.	Review of Other Works and B .1 Relation of Artifacts to Project Development	6
Review of work 1.....		6
Review of work 2.....		6
Review of work 3.....		7
Review of work 4.....		7
C.	Project Rationale	8
D.	Current Project Environment	8
E.	Methodology	10
F.	Project Goals, Objectives, and Deliverables	12
F1.	Goals, Objectives, and Deliverables Table.....	13
F.2	Goals, Objectives, and Deliverables Descriptions.....	12
G.	Project Timeline with Milestones	14
H.	Outcome	15
I.	References	17

## **Proposal Overview**

### **A.1 Problem Summary**

CT Cyber Team Consulting is an offensive cybersecurity consulting firm facing challenges regarding its operations' efficiency. CT is a small offensive security consulting company with 50 employees in the northeast United States with mostly up-to-date infrastructure and technologies. CTs provides value to its customers by conducting red team engagements to identify vulnerabilities in the client's IT infrastructure. In today's cyber security landscape, CTs red team spends the majority of its time conducting passive reconnaissance. Passive Recon includes activities such as physical site surveys, open source intelligence (OSINT), and any other information gathering on a target without actually interacting with the target. While these activities are certainly crucial to our red team engagements, they can be extremely time-consuming and can potentially bottleneck our engagements. CT red team is proposing a project to the change management board and upper-level management. This proposed project will greatly reduce the amount of time it takes our red team to perform engagements with minimal cost and overhead. The project will achieve this by leveraging AI agents to assist our red team in performing OSINT activities. It is extremely critical for CT to acknowledge and harness this technology to stay ahead of our competitors.

## **A.2 IT Solution**

Our solution is to implement a system to automate the OSINT portion of passive reconnaissance using AI agents. AI agents provide new and powerful capabilities that have never before been seen in the world of cybersecurity. It is important that we leverage these emerging technologies to our benefit. The key components of our solution include selecting a powerful (LLM) Large language model for our machine to run the agents on. Configuring a device to query our agents locally. It is important to understand how the recommended solution works. We select an LLM to connect to via enterprise LLM vendors. Then, we configure our LLM to run AI agents. Then, we configure an AI agent manager locally to control and query our agents. Lastly, crafting specific reusable queries to effectively leverage our agents to achieve maximum efficiency while conducting OSINT.

## **A.3 Implementation Plan**

This implementation will be most successful if carried out in this 3-phase manner. It allows us to break tasks up into easy-to-manage action items. We will be able to effectively document and create project artifacts as we go. At the end of each phase, we will conduct a GAP analysis to determine where we are currently in relation to where we should be in order to keep our project on track and in scope. Lastly, without a phased approach, the project could miss KPIs, objectives, and deliverables. During this process, we will also need to ensure a seamless integration with our ongoing operations. The implementation should naturally be seamless due to the smaller nature of the project. We will continue to conduct business as usual until after the testing phase. Finally, prior to the first phase, we will train our employees on how to use the new technologies.

The implementation of this project will include three phases. These phases offer simplicity and coherence during the project lifecycle. The three phases include. Selecting our LLM and gathering resources. Setting up and configuring the agent's manager. Lastly, we will be querying and training our agents to achieve the desired end result. This phase will also include continually training and making our agents more efficient after the project ends.

In phase one, we will first select the LLM that we will use to run our agents. To select a model, we will need to consider speed, price, and accuracy. We will then need to acquire a device to run our agent manager. The agent's manager is our interface to configure and use the agents that run off of the LLM. Lastly, we will need to work with our infrastructure team to establish our device within the network and make sure it runs properly.

In phase two, we will configure our agent manager. To configure the manager, we need to consider our current network posture and company policy. We need to make sure the device and the manager are in compliance with Government and corporate governance. Then, we will first configure our manager in a way that is easy for our red team and compatible with their current workflow. Lastly, we need to make sure that the manager is able to query the LLM effectively and achieve the desired outcome.

In phase three, once we determine that the agent's manager works as intended, we will begin querying and training our agents. When we first configure our manager, it will essentially be bare bones. We need to begin training and testing it to help it successfully achieve OSINT activities. This process will continue well after we are done with the project. This is, in fact, the main benefit of using the agents over a script. We can train and craft our agents over time to be tailored specifically to the way we like.

This implementation plan works perfectly to facilitate a smooth transition from our current posture to the proposed posture. We will be able to efficiently hit our metrics and document the process along the way. It also allows our red team and supporting teams to understand and adapt to the new process. Lastly, conducting a gap analysis at the end of each phase will allow us to make sure our project stays within scope and maintains (GRC) Governance, Risk, and Compliance metrics.

### **Review of Other Works and B.1 Relation of Artifacts to Project Development**

A revision of the following related works demonstrates a use case for AI in gathering OSINT. The works we will be looking at are created by industry professionals on the cutting edge of cybersecurity and AI. By looking at these use cases, we can determine how they can bring value to CT.

#### **Review of work 1**

European governments, with the help of HALA systems, were able to successfully use AI agents to help bring justice to war crimes in Ukraine. As of Dec 2024, EQTYLabs reported that "Over the last 18 months, Hala Systems and EQTY Lab have been working with the German Government as they seek accountability for war crimes in Ukraine in both domestic and international courts." In this specific use case, they used AI to sift through thousands and thousands of social media posts, forums, and telegram channels to identify possible war crimes and wrongdoings within the Russo-Ukraine war. This article shows us how governments are utilizing AI in their OSINT activities and gives us a great model to follow.

#### **Review of Work 2**

In this work, HackerNews reiterates how much time and labor goes into OSINT gatherings. They go into how the (ODNI) Office of the Director of National Intelligence for the United States Government unveiled a new strategy for OSINT gathering using AI to automate sifting through hundreds of thousands of data sources. Here's one of the ways that the Government can use AI to its benefit, "Handling Massive Data Volumes: AI systems can process and analyze enormous amounts of data at speeds far beyond human capabilities. This allows OSINT practitioners to cast a much wider net than previously possible and still deal with the results." This provides us with further insight into how top government agencies are leveraging AI to their benefit and gives us a broad idea of how we should as well.

### **Review of work 3.**

In this next article, Ben Joelson, a global cybersecurity consultant, makes his case for how AI will improve our company's and governments' OSINT gathering process. He specifically delves into real-world examples of how corporate security is changing its OSINT gathering process to use AI to increase productivity massively. He specifically talks about how AI has the ability to "convert images and video to natural language—which can be queried like a search engine—now exists. Tools can crawl troves of images and videos to detect guns, weapons, or even client logos." This gives us yet another valuable use case about how AI is being used in today's corporate cybersecurity landscape.

### **Review of work 4**

The final work we will be reviewing is a blog post written by Mariarosaria Taddeo, Luciano Floridi, and Riccardo Ghioni of the Oxford Internet Institute. This blog post from Feb 2023 reviews how OSINT is evolving with the use of AI to assist government agencies in collecting valuable information on potential bad actors. They also review how important

OSINT has become in today's cybersecurity landscape, "Over the years, OSINT has become an integral part of intelligence practice, with technological progress delivering new collection methods and creating new intelligence sources, such as satellite images, social media, public records, and digital currencies. Indeed, many estimates place OSINT at around eighty percent of all the intelligence material used by law enforcement agencies." This post reminds us of the importance of OSINT in the Government and corporate world and how AI is helping change it.

### **C. Project Rationale**

CT is currently facing bottlenecks and inefficiencies in its current OSINT gathering process. While OSINT is traditionally time-consuming, it is also one of the most essential parts of passive reconnaissance for our red team. It is critical that we leverage this new technology to our benefit. This project will help us incorporate AI into our pre-existing workflow seamlessly, thus creating a massive increase in productivity for our red team. In the past couple of years, AI has become significantly more inexpensive and efficient. If we don't act now, our firm is at serious risk of falling behind our competition.

### **D. Current Project Environment**

CT currently has a well-defined and structured red team engagement workflow. Due to the nature of red team engagements, we like to visualize our current environment in four phases. It is important to understand these phases and this workflow to understand the benefit of the proposed project. In our first phase, our team meets with the client to determine many things, including scope, timing and approved IP ranges. We then outline all agreed-upon topics in a (MSA) Master Service Agreement to ensure both parties understand the parameters of the



engagement as agreed upon. This is the most crucial phase of the engagement, and adhering to the MSA throughout the engagement is mission-critical.

The second phase is the reconnaissance and planning phase. This phase is where OSINT gathering resides and is part of our process that will benefit from the proposed project. In this phase, we begin with passive Recon and then move into active Recon, where we are actually interacting with the target. For passive Recon, we do activities such as physical information gathering and OSINT. Once we gather all the possible information from passive Recon, we will move to active Recon. This includes activities such as port scanning and phishing. After we have thoroughly completed active and passive Recon, we can begin mapping the target's attack surface and make a plan for the attack. Without comprehensive and thorough Recon, the plan and the subsequent attack may be inadequate for CT's high standards. Thus, it is important that we prioritize passive Recon containing OSINT and active Recon.

The third phase is the attack phase. In this phase, we begin the engagement and attempt to gain unauthorized access to specific items outlined in the MSA. Currently, for this phase, we follow the MITRE ATTACK framework in conjunction with the attack plan we developed in phase two to carry out the attack. The MITRE ATTACK framework is a globally recognized framework for conducting red-team engagements and for developing blue-team defenses. During this process, it is critical that we document and preserve all relevant information collected during the engagement so that it can be later given to the target. It is also extremely critical that we adhere strictly to the MSA and government regulations during this phase. After attacking the target, it is also important that we return their environment to the exact same way it was before our attack.

The fourth phase is the presentation phase. Here, we gather all of our documented findings and prepare them in a digestible format for our client. We then meet with them and share our findings. We also give the client guidance on the recommended course of action to mitigate the vulnerabilities found within their environment. Lastly, we establish if the client would like another red team engagement after a specified period of time.

In conclusion, the proposed project will fit in with our current posture and culture. The project plugs right into our second phase during passive Recon. This will make it easy for our red team to adopt and digest. Our red team will also gain the new capability of training its AI to their specific wants and needs. Considering the previous statements, this project benefits us tremendously and fits right into our current process.

### **E. Methodology**

The methodology behind our project implementation will be similar to an Agile framework. The agile framework is great for projects that require flexibility and changes as the project progresses. Within this framework, we will implement 5 phases. The Planning & Design phase, the Development phase, the Implementation phase, the Testing phase, and the Maintenance phase. After each phase, we will conduct a gap analysis to compare where we are to where we want to be. Gap analysis and combination with our phased approach will help us ensure that we are meeting our project objectives in an efficient and responsible way.

In our Planning & Design phase, we will compare our current red team infrastructure with where we want it to be after the project. We will then plan out and design how we can most effectively integrate the new process into our existing processes. Specifically, in this phase, we will do things like select our LLM. Next, we will work with supporting teams to

determine any additional resources we will need to gather for the project. Finally, we will determine the budget that is required for the project.

For our development phase, we will develop a new framework for conducting red team engagements. We will develop a framework that maintains a lot of the same principles our current framework uses. We will specifically be looking at the passive recon section of our red team engagement workflow. Along with developing a new red team framework, we will configure our agent manager to work with our LLM. And lastly, we will configure and develop a database for our agent manager to store collected information.

Next, for our implementation phase, we will move all of the developed technologies and frameworks into our production environment. Right before we begin this phase, we will need to notify all affected parties and give guidance on how they will be affected. During this implementation process, we need to ensure that it is done in a timely manner to minimize downtime. And finally, we will make sure to maintain backups of our previous infrastructure to mitigate any potential risk of failure.

Then, for our testing phase, we will ensure that the previous phase was conducted correctly. We will have our red team query the agent manager to ensure that it is functioning as intended. Then, we will look into our database to see if data is being sent correctly. Finally, we will ensure our red team can effectively utilize the new technologies for their intended purpose. Without this important phase, we could miss certain key deliverables and objectives.

And finally, for our maintenance phase, we will continually update and maintain the implemented infrastructure. It is important that this phase lasts beyond the project timeline. Specifically, during this phase, we will maintain the physical infrastructure on which our technologies lie. We will also continue to train and improve our LLM to match business and red

team engagement needs. Lastly, any supporting software and firmware will need to be routinely updated and patched to mitigate vulnerabilities and optimize performance.

### **F. Project Goals, Objectives, and Deliverables**

The primary goal of this project is to increase the red team's operational efficiency at CT. We will achieve this goal by achieving the three following supporting objectives. Automate OSINT gathering activities using an LLM, improve the quality of OSINT gathering and establish continuous improvement for OSINT. By breaking up our primary goal into these three supporting objectives, we can more effectively achieve it. By achieving our primary goal, we can optimize the business and drive more value for our clients.

The first supporting objective we will be looking at is "Automate OSINT gathering activities using an LLM." To do this, we will select an LLM for our agent manager to query. It is important that we select an LLM that most aligns with the red team OSINT gathering objectives. Next, we will need to source and configure a database for our LLM to store any data that is found. After this, we will need to configure our agent manager to query our LLM. The manager will be configured across red team endpoints for effective use by the team.

The second supporting objective is to "Improve the quality of OSINT data." To achieve this objective, we need to establish a database of effective queries. This is one of the most critical steps of the process due to the nature of AI. Next, we will need to train our employees to ensure end-user acceptance. Lastly, we will need to utilize our LLM to expand the sources from which we can gather OSINT. The process of gathering OSINT means scouring the internet from hundreds of thousands of potential sources. Utilizing AI, we will be able to gather information much more effectively from all of these potential sources.

The third and final supporting objective is "Establish continuous improvement for OSINT." To achieve this, of course, we will need to train our LLM over time. This is, in fact, one of the primary benefits of using AI, which is its capability to change and adapt over time. Next, of course we will need to update our LLM, and agent manager over time. Just like any other software we might use, we will need to ensure our new tools are up-to-date and patched. Lastly, we will frequently test new queries and train our LLM on what we want to see from it and what we do not. Following these steps will allow us to harness the greatest benefit of using AI, which is its unique ability to adapt and train based on exactly what we want to see from it.

### F1. Goals, Objectives, and Deliverables Table

	Goal	Supporting objectives	Deliverables enabling the project objectives
1	Increase red team operational efficiency	Automate OSINT gathering activities using an LLM	Select LLM for AI Agents manager
			Configure database for information gathered from OSINT
			Configure agent manager to query LLM
		Improve quality of OSINT data	Establish a database of effective queries
			Train our employees on how to use agent manager
			Use our LLM to expand OSINT gathering sources
		Establish continuous improvement for OSINT	Train our LLM over time
			Keep our LLM and agent manager up to date
			Frequently test new queries and continue to optimize

**G. Project Timeline with Milestones**

To best achieve our project's primary goal, we need to break it down into five distinct phases in a project timeline. Keep in mind this timeline will be flexible and can change as projects routinely require adjustments throughout their life cycles. The first phase is our planning and design phase. During this phase, we will do things like to identify resources essential to the project, design infrastructure changes to integrate the project into our current infrastructure and design an end-user acceptance manual. The next phase is the development phase; in this phase, we will develop and acquire the necessary resources outlined in the first phase. In the implementation phase, we will implement all of the processes and resources outlined in the implementation plan above. In the testing phase, we will ensure that our newly implemented infrastructure functions as intended, as well as our legacy infrastructure. In the maintenance phase, we will engage in continuous deployment and improvement to ensure maximum effectiveness now and in the future.

Milestone or deliverable	Duration (hours or days)	Projected start date	Projected end date
Planning & Design Phase	30 days	2026-03-31	2026-04-30
Development Phase	45 days	2026-05-01	2026-06-14
Implementation Phase	60 days	2026-06-15	2026-08-14
Testing Phase	30 days	2026-08-15	2026-09-14
Maintenance Phase	Continuous	2026-09-15	N/A

## **H. Outcome**

By implementing this project, we hope to greatly improve the efficiency of our red team. This project includes automating our processes by leveraging the powerful capabilities of AI. We will use well-defined objectives and goals. And deliverables to assist in delivering a successful project. We will also use a simple project timeline with milestones that allow us to break down our project into digestible and achievable actionable items. While this project is not a massive overhaul of business processes, it is still important to plan and establish these goals and timelines to mitigate the risk of things like scope creep and missing objectives.

This project will impact our business functions by making the passive recon phase of our red team engagements more efficient. Currently, we conduct OSINT manually and with the use of scripts. The methods and scripts we use today are of the highest quality and are outlined within globally accepted frameworks for red team engagements. While this process does provide us with valuable information, it is extremely time-consuming. Testimonials from our red team tell us that the majority of the time spent during their engagements is spent conducting passive recon. This severely limits the output of our red teams. By achieving the goals outlined in the project, we will make this process exponentially more efficient. It will remove the single biggest bottleneck for our red teamers. Not only will using AI make the process more efficient, but it will also give our team higher-quality information. Together, these two things will help our team provide much more value to our clients and customers.

We have set clear goals and objectives to measure the success of the project. Together, these goals and objectives will help us achieve our primary goal of increasing Red Team operational efficiency. We know our project will be successful if our red team's time to conduct passive recon is lowered. To measure this, we will use qualitative and quantitative data. The quantitative

data will include information from our past assessments and get an average time duration for our red team's passive recon phase. We will measure this average duration against our post-implementation average duration. If our project is successful, we will observe a decrease in the amount of time it takes our red team to conduct passive recon. On the other hand, if the project is unsuccessful, we would observe an increase in the average duration of passive recon. The qualitative measure we will use to determine project success is feedback from our red team. Throughout the process and after (as part of our continuous improvement), we will gather testimonials from our red team. To do this, we will ask questions such as "Do you like the new process?", "Does it speed up passive recon?" and "Is it providing you with more valuable OSINT data?" The answers to these questions will provide us with valuable insights into how the project is doing on the ground with our team. In conclusion, by combining the insights from the qualitative and quantitative measures, we can accurately determine the success of the project and ensure that it aligns with our current infrastructure.



## I. References

The Hacker News. (2024, July 3). *The emerging role of AI in open-source intelligence*.

<https://thehackernews.com/2024/07/the-emerging-role-of-ai-in-open-source.html>

Mitre ATT&CK®. MITRE ATT&CK®. (n.d.). <https://attack.mitre.org/>

Murray, E. (2024, October 1). *Ben Joelson explores how AI will improve OSINT*. The Chertoff Group.

<https://chertoffgroup.com/ben-joelson-explores-how-ai-will-improve-osint/>

*Open source intelligence (OSINT) and ai: The informational pivot of intelligence analysis*.

OII. (n.d.).

<https://www.oii.ox.ac.uk/news-events/open-source-intelligence-osint-and-ai-the-informational-pivot-of-intelligence-analysis/>

*Verifiable compute and Hala*. Verifiable Compute and Hala | EQTY Lab - AI Integrity

Suite. (n.d.). <https://www.eqtylab.io/blog/verifiable-compute-and-hala>