# Doppelgängers: Finding Job Scammers Who Steal Brand Identities

*GIAC (GCIH) Gold Certification*

Author: Ashley Taylor, infosec_taylor@protonmail.com
Advisor: *Dr. Johannes Ullrich*

Accepted: *01/30/2022*

Abstract

Fraud is on the rise and occurs in many forms. A growing number of criminals are impersonating real companies to trick job seekers into handing over their personal information or money. These impersonated companies face risks in terms of damage to their brand identity. What can companies do to protect their brand against fraud? Information security teams often have the tools to help find impersonation fraud before it becomes a problem. Using threat intelligence and a security orchestration, automation, and response (SOAR) platform, suspicious similar domains were found, intelligence about those domains gathered, and the evidence presented to information security teams to make informed decisions on whether to block the domain. Automation reduced the time it took information security analysts to respond to similar domain alerts. Guidance is given to turn this data into an actionable program to begin building brand identity protections into any security program.

# 1. Introduction

Hiring frauds are nothing new, but a rise in criminals posing as legitimate companies prompted the Federal Bureau of Investigations (FBI) to create a public service announcement in early 2020 (Cyber Criminals Use Fake Job Listings To Target Applicants' Personally Identifiable Information, 2021). According to the FBI, these criminals not only defraud victims out of their personally identifiable information (PII), but also out of money. These fake jobs can swindle victims out of thousands of dollars by asking for upfront money to pay for job training or equipment.

Criminals can impersonate legitimate companies by use of typosquat or similar domains. These domains differ by a letter or include the company's name in the title to make emails from fake recruiters seem more legitimate (Rafter, 2020).

Recommendations and advice given by the FBI are targeted towards job seekers and warn them of modern hiring scams. However, a hiring scam that impersonates a legitimate company can damage a company's brand (Rafter, 2020). This paper will explore what companies can do to detect and respond to hiring scams that attempt to scam job seekers and damage the company's brand.

## 1.1. Medical Device Manufacturer Case Study

One company that works in medical device manufacturing (referred to in this paper as Company A) has been impersonated repeatedly in hiring frauds. Criminals register similar domains and set up email servers to begin posting fake jobs on sites like LinkedIn and ZipRecruiter. Examples of similar domains that have been seen include companya-jobs.com, careers-companya.com, and c0mpanya-jobs.com.

Company A became aware of the fake job ads when a victim reached out to the company asking details about the job offer. After contacting the victim, Company A learned the criminals were impersonating a legitimate recruiter at Company A to create interviews and interact with the victims. The criminals would interview the applicant on RingCentral and shortly afterward send a fake job offer for the victim to sign. The criminals would then steal money from the victims either by redirecting the victims to a fake site to buy equipment or by mailing the victim a bonus check that they later asked to

be returned after cashing. If the victim did not fall for either of the monetary frauds, the criminals still had their personal information which could be used to steal the victim's identity.

One solution would be to purchase all typosquat and similar domains, but this would be cost prohibitive. Company A would benefit from earlier detection of registered typosquat domains, but simply receiving an alert that a typosquat domain has been registered would create more work for the information security analysts as they had to research the domains for intent. For example, of the 133 similar domain alerts received in 2021, only four were found to be malicious. On average, the alerts take security analysts 20 minutes to investigate, including enriching data and blocking the domains found to be suspicious. For 133 similar domain alerts, it would take security analysts 44.3 workhours to process when realistically only four domains needed further investigation. A better solution would need to analyze the domain for characteristics seen in the brand attack and automate data enrichment to decrease the workhours needed for investigation by the security team.

## 2. Methodology

The detection for the hiring frauds contains the following workflow: receiving an alert of a typosquat or similar domain being registered, a certificate registered with the domain, a MX record setup for the domain, enriching data with WHOIS information, and alerting the security team to review. After a review by the security team, the response workflow can begin if needed. Figure 1 shows a high-level flowchart of the detection and response method.

Ashley Taylor, infosec_taylor@protonmail.com

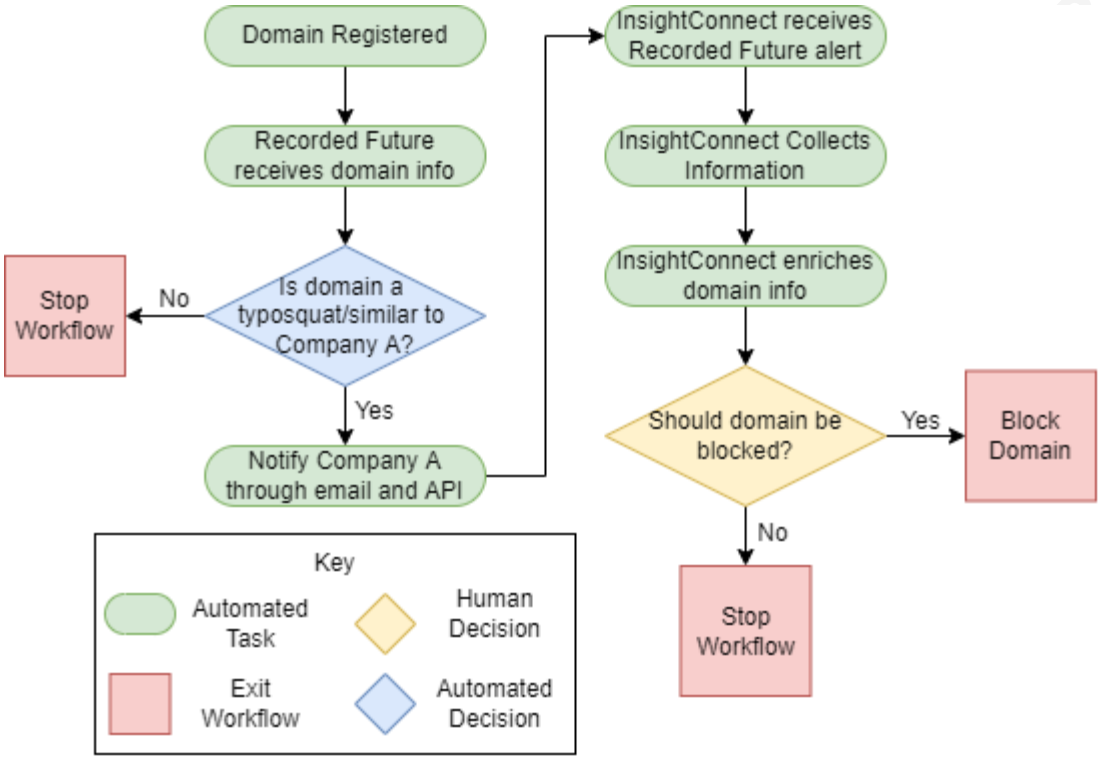


*Figure 1.* High-level workflow of typosquat or similar domain detection

The proposed detection and initial response for finding similar domains targeting Company A utilizes two security tools: a threat intelligence platform and a security orchestration automation response platform (SOAR). For this specific method, Recorded Future and Rapid7 InsightConnect will be used.

## 2.1. Threat Intelligence Platform

The threat intelligence platform used in this study for alerting is Recorded Future. To enable typosquatting and similar domain alerts, the Brand Intelligence module is needed. The Brand Intelligence module monitors and alerts for newly created domains that are similar enough to a list of owned domains provided by the customer (Recorded Future, 2020). The alert provides more information on the domain including if a certificate was registered along with the suspicious domain. For integrations with InsightConnect, an added API key needs to be purchased.

With the correct module, the Domain Watch Lists are updated with Company A's domains. After setting up the domains, the Domain Abuse Alerts are configured to notify

security staff by email of typosquatting events. When an alert is sent to security staff, the Recorded Future API also sends an alert to InsightConnect. The alert was set to alert information security analysts within 15 minutes of a similar domain being registered or a certificate being registered for a similar domain.

## 2.2. Rapid7 InsightConnect Data Enrichment

Rapid InsightConnect is a SOAR platform that uses various triggers, plugins, and an orchestrator to gather information, automate actions, and create human decision points for information security staff (Rapid7, n.d.). Figure 2 shows a detailed flowchart for the InsightConnect workflow to detect and respond to similar domains.

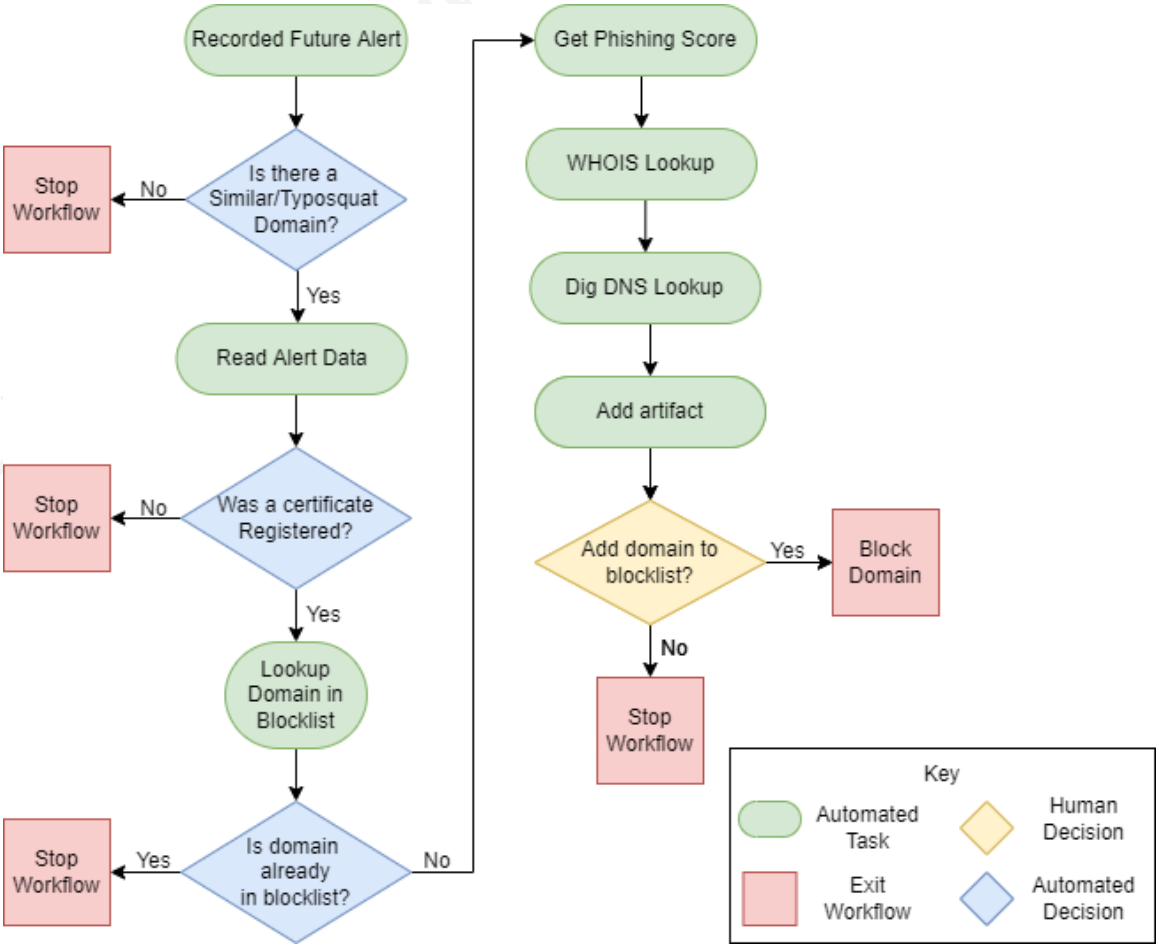


*Figure 2.* InsightConnect Workflow to analyze domain and enrich similar domain information.

To receive alerts from Recorded Future into InsightConnect, the Recorded Future plugin from the Rapid7 Extensions library must be installed and configured using a Recorded Future API key (Rapid7, 2021a). Once the plugin is installed, the Recorded Future API will send alert notifications in JSON format to the extension using the Get New Alerts trigger. Table 1 lists the information that is collected from the Get New Alerts trigger.

| Field Name | Description | Data Type |
|---|---|---|
| **Alert** | Alert information | Object |
| **Alert.id** | Identification code of the alert | String |
| **Alert.title** | Title of the alert | String |
| **Alert.triggered** | Date and time alert was triggered | String |
| **Alert.type** | Type of alert | String |
| **Alert.url** | URL to Recorded Future summary of alert | String |
| **Alert.review** | Alert status information | Object |
| **Alert.review.status** | Action taken in Recorded Future for alert | String |
| **Alert.review.statusInPortal** | Status of the alert in the Recorded Future portal | String |
| | | |
| **Alert.rule** | Rule information | Object |
| **Alert.rule.id** | Identification code of the rule triggers | String |
| **Alert.rule.name** | Rule name that was triggered | String |
| **Alert.rule.url** | URL to Recorded Future rule | String |

*Table 1:* Data points, description, and data types collected from Get New Alerts trigger in InsightConnect extension.

After an alert is received, InsightConnect uses the Alert.rule.name field to decide if the alert name contains Identify Similar Domains, which is the name of the alert

Recorded Future sends when it identifies a potential typosquat or similar domain. If the alert name does not match, then the workflow exits.

Using the Alert.id field, further information about the alert is then pulled from Recorded Future using the Lookup Alert action of the InsightConnect extension, including the suspicious domain that was registered and if a certificate was registered along with it. Figure 3 shows a redacted JSON alert received from Recorded Future.


```
{
  "$success": true,
  "alert": {
    "counts": {
      "documents": 1,
      "entities": 0,
      "references": 2
    },
    "entities": [
      {
        "documents": [
          {
            "references": [
              {
                "entities": [
                  {
                    "id": "idn:www.companya-careers.com",
                    "name": "www.companya-careers.com",
                    "type": "InternetDomainName"
                  }
                ],
                "fragment": "A certificate for the domain www.companya-careers.com has been registered",
                "language": "eng"
              }
            ],
            "source": {
              "id": "******",
              "name": "New Certificate Registrations",
              "type": "Source"
            },
            "title": "Certificate Registration"
          }
        ],
        "risk": {},
        "trend": {}
      }
    ],
    "id": "******",
    "review": {
      "status": "no-action",
      "statusInPortal": "New"
    },
    "rule": {
      "id": "******",
      "name": "Identify Similar Domains",
      "url": "https://app.recordedfuture.com/******"
    },
    "title": "Identify Similar Domains - 1 new references in 1 documents",
    "triggered": "2021-11-30T11:10:58.578Z",
    "type": "EVENT",
    "url": "https://app.recordedfuture.com/****"
  }
}
```


*Figure 3:* JSON return from using the Lookup Alert plugin of the Recorded Future plugin for InsightConnect.

After receiving further information about the alert, InsightConnect checks if there was a certificate registered with the domain. A registered certificate is an indicator that the typosquat domain could be used maliciously in the future. The Alert.entities.0.documents.0.source.name data is used to check if a new certificate was registered. If it was registered, then the workflow continues to analyze the domain. If not, it will end the workflow.

The domain is then compared to the list of blocked domains to see if the domain has previously been analyzed and blocked. If the domain appears on the blocklist, then the workflow ends as no further investigation is needed.

The next part of the InsightConnect workflow attempts to enrich the domain information for information security analysts. The first step of analyzing the domain uses the Typo Squatter plugin available in the Rapid7 Extensions library. The Typo Squatter plugin can use dnstwist and phishing_catcher to assign a score to the domain provided. If the score is above 65, it is likely a phishing domain (Rapid7, 2021b).

In the next step, the Rapid7 WHOIS plugin is used to provide added intelligence about the suspicious domain (Rapid7, 2021d). Using the Look Up Domain action, the data in Table 2 is provided.

| Field Name | Descriptions | Type |
|---|---|---|
| **["WHOIS Lookup"].[name]** | Domain Name | String |
| **["WHOIS Lookup"].[dnssec]** | DNSSEC Information | String |
| **["WHOIS Lookup"].[registrar]** | Domain Registrar | String |
| **["WHOIS Lookup"].[last_updated]** | Last Updated Date | Date |
| **["WHOIS Lookup"].[name_servers]** | Nameservers | Array |
| **["WHOIS Lookup"].[creation_date]** | Creation Date | Date |
| **["WHOIS Lookup"].[domain_status]** | Domain Status | String |
| **["WHOIS Lookup"].[registrant_cc]** | Registrant Country | String |
| **["WHOIS Lookup"].[registrar_url]** | Registrar URL | String |
| **["WHOIS Lookup"].[expiration_date]** | Expiration Date | Date |
| **["WHOIS Lookup"].[registrant_name]** | Registrant Name | String |
| **["WHOIS Lookup"].[registrar_iana_id]** | Registrar IANA ID | String |
| **["WHOIS Lookup"].[registry_domain_id]** | Registry Domain ID | String |

| | | |
|---|---|---|
| **["WHOIS Lookup"].[registrar_whois_server]** | Registrar WHOIS Server | String |
| **["WHOIS Lookup"].[registrar_abuse_contact_email]** | Registrar Abuse Email | String |
| **["WHOIS Lookup"].[registrar_abuse_contact_phone]** | Registrar Abuse Phone | String |

*Table 2*. Available data returned from Rapid7 WHOIS plugin.

The last step of enrichment is to DNS query the suspicious domain using the DNS plugin from the Rapid7 extensions library. The plugin uses the Domain Information Groper (Dig) to return the DNS information of the domain (Rapid7, 2021c).

After all the information on the domain is collected, an easy-to-read artifact, or executive summary report, is created with the results and a notification is sent to the Information Security department to decide whether or not to block the domain. If the security analyst reviewing the alert chooses to block, then the domain is added to the blocklist. If the security analyst chooses not to block the domain, then the workflow exits. The executive summary is created in an enhanced Markdown language, as shown in Figure 4.

```
{{["Lookup Alert"].[alert].[entities].[0].[documents].[0].[title]}} for {{["Lookup
 Alert"].[alert].[entities].[0].[documents].[0].[references].[0].[entities].[0].[name]}} on {{["Lookup
 Alert"].[alert].[triggered]}}

{{#if ["Typosquatter Plugin - Get Phishing Score"]}}
Phishing Score = {{["Typosquatter Plugin - Get Phishing Score"].[score]}}
{{/if}}

Documents:

{{#each ["Lookup Alert"].[alert].[entities]}}
{{#each documents}}
{{@index}}
{{#if url}}Source = {{url}}{{/if}}
{{#each references}}
{{#each entities}}
Entity = {{name}} ({{type}})
{{#with fragment}}
Reference = {{.}}
{{/with}}
{{/each}}
{{/each}}
{{/each}}
{{/each}}

Domain already in blocklist?
{{["Look up domain in blocklist"].[found]}}

WHOIS lookup:
{{#if ["WHOIS Lookup"]}}
Registrar = {{["WHOIS Lookup"].[registrar]}}
Registrar URL = {{["WHOIS Lookup"].[registrar_url]}}
Registrar Abuse Contact Email = {{["WHOIS Lookup"].[registrar_abuse_contact_email]}}
Registrar Abuse Contact Phone = {{["WHOIS Lookup"].[registrar_abuse_contact_phone]}}
Registrar IANA ID = {{["WHOIS Lookup"].[registrar_iana_id]}}
Registrant Name = {{["WHOIS Lookup"].[registrant_name]}}
Registrant Country = {{["WHOIS Lookup"].[registrant_cc]}}
Creation Date = {{["WHOIS Lookup"].[creation_date]}}
Last Updated = {{["WHOIS Lookup"].[last_updated]}}
Nameservers = {{["WHOIS Lookup"].[name_servers]}}
DNSSEC = {{["WHOIS Lookup"].[dnssec]}}
{{/if}}

dig:
{{#if ["dig - Forward DNS Query"]}}
Question
{{["dig - Forward DNS Query"].[question]}}

Answer
{{["dig - Forward DNS Query"].[answer]}}
{{["dig - Forward DNS Query"].[fulloutput]}}
{{/if}}
```

*Figure 4*. Markdown code to create executive summary

## 3. Testing

To test the response workflow for similar domains that can alert security to staff to fake job impersonation scams, the domain companya-career.com was purchased with Name.com, Incorporated as the registrar. A security analyst created a public certificate, and a hosted email service was setup for the domain. One hour after registering the domain, Recorded Future generated a Identify Similar Domains alert, as seen in Figure 5.

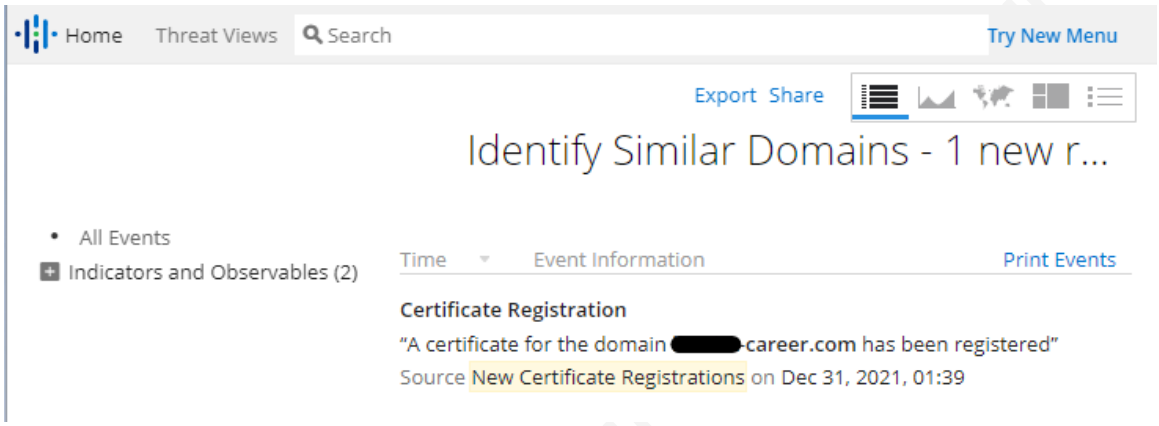


*Figure 5.* Screenshot of Record Future alert on the certificate registration for companya-career.com

Within one minute of the Recorded Future alert, the InsightConnect workflow began analyzing the domain. First, the InsightConnect was notified of the alert from Recorded Future as seen in the code snippet in Figure 6. The identification code of the alert is used in the following step.

```
{
    "alert": {
        "id": "lIqLAP",
        "rule": {
            "id": "d9-z6s",
            "name": "Identify Similar Domains",
            "url": "Link to Recorded Future alert"
        }
    }
```

*Figure 6.* JSON code snippet of the Identify Similar Domain alert received by InsightConnect from the Recorded Future API.

The identification code is then used by InsightConnect to query other information about the alert from Recorded Future, including the suspicious domain. Figure 7 shows the input and Figure 8 shows the output of the query.

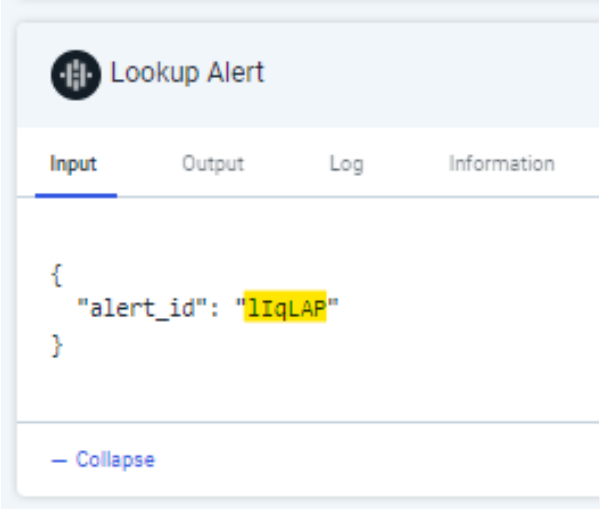


*Figure 7.* Input query sent to the Recorded Future API from InsightConnect. Note the only information needed is the alert identification code.


```
{
    "$success": true,
    "alert": {
        "entities": [
        {
            "documents": [
            {
                "references": [
                {
                    "entities": [
                    {
                        "id": "idn:companya-career.com",
                        "name": "companya-career.com",
                        "type": "InternetDomainName"
                    }
                    ],
                    "fragment": "A certificate for the domain compaya-career.com has been registered",
                    "id": "GhkJ_tAHRX4",
                    "language": "eng"
                }
                ],
                "source": {
                    "id": "beD_4-",
                    "name": "New Certificate Registrations",
                    "type": "Source"
                },
                "title": "Certification Registration"
            }
            ],
        }
        ],
    }
}
```


*Figure 8*. JSON code snippet from Recorded Future for the Identify Similar Domains alert, which includes the suspicious domain.

The next part of the workflow triggers the first two decision points: was the alert received 'Identify Similar Domains' and was a certificate registered? Figure 8 shows the query InsightConnect used to automate these decisions and the results of the decision.

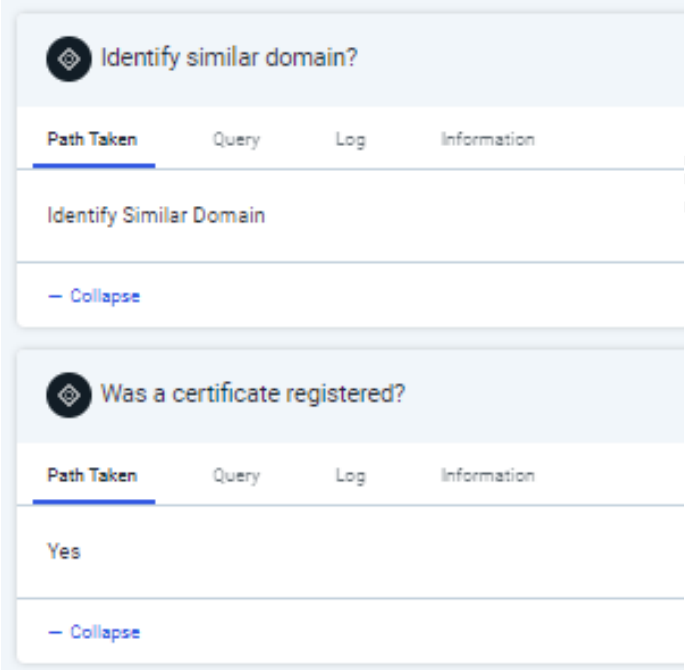


*Figure 9*. Automated decisions taken during InsightConnect workflow based on defined logic.

The next part of the workflow determines if the domain has already been seen by a security analyst and added to the block list. Figure 9 shows the input query to find the domain on the blocklist. As seen in Figure 10, since this test domain has not been seen before by InsightConnect, the workflow continues to process.


*Figure 10.* Suspicious domain name is checked against the block list and returns a Boolean value.

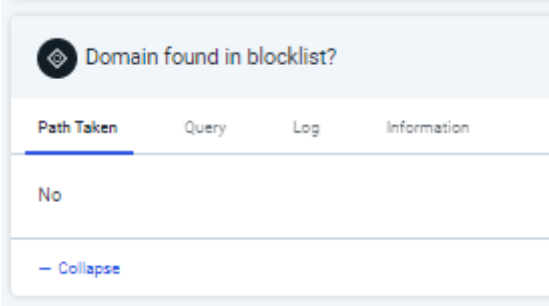


*Figure 11.* Suspicious domain was not found in the block list, so the workflow continues.

At this point in the workflow, the domain is considered suspicious and further intelligence is gathered to allow the security analyst to make an informed decision over whether to block the domain or not. The first enrichment module uses the Typo Squatter plugin to assign a Phish Score based on certain key indicators. As shown in Figure 11, the phish score assigned to companya-career.com is a twenty-two.

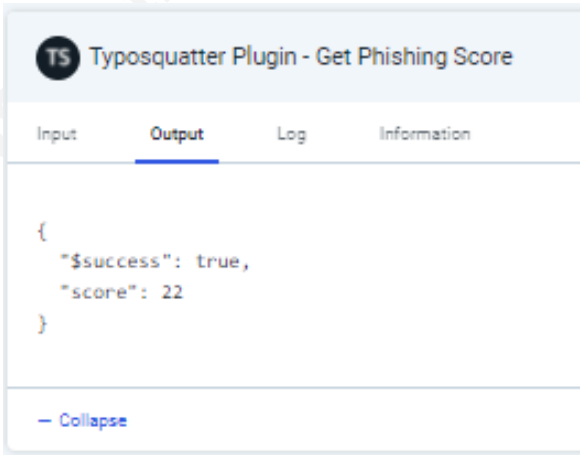


*Figure 12.* Phish Score response from InsightConnect Typo squatter Plugin.

After receiving the DNS information, continued enrichment is performed by querying the WHOIS record of the name. In Figure 12, the query shows that Name.com, Inc. is the registrar.

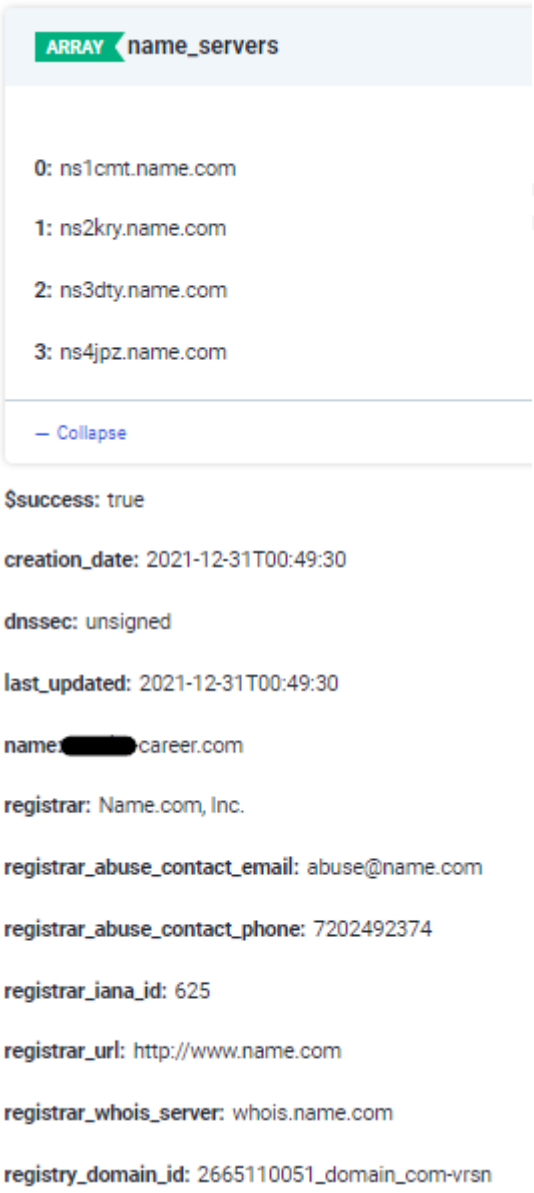


*Figure 13.* WHOIS return for companya-career.com

Finally, the executive report is created so the enrichment information is easier to read. The report is emailed to the information security analysts who then can decide whether to block the domain. Information security analysts then log into the InsightConnect portal and answer the human decision point. If the choice is to block, the domain is automatically added to the blocklist. If not, the workflow exits. Figures 13 and 14 show the executive report and block button.

InsightConnect Job Paused

Hi Ashley Taylor,

Job "RecordedFuture Alert" is paused for a human decision.

Click to view job "RecordedFuture Alert" and make a decision.

Job ID: 567911e3-1fea-41ed-935b-697fb7f40bc2

Executive Report

Certificate Registration for [redacted]-career.com on 2021-12-31T01:44:19.558Z

Phishing Score = 22

Documents:

0

Entity = [redacted]-career.com (InternetDomainName)

Reference = A certificate for the domain [redacted]-career.com has been registered

Domain already in blocklist?

false

WHOIS lookup:

Registrar = Name.com, Inc.

Registrar URL = http://www.name.com

Registrar Abuse Contact Email = abuse@name.com

Registrar Abuse Contact Phone = 7202492374

Registrar IANA ID = 625

Registrant Name =

Registrant Country =

Creation Date = 2021-12-31T00:49:30

Last Updated = 2021-12-31T00:49:30

Nameservers = ["ns1cmt.name.com","ns2kry.name.com","ns3dty.name.com","ns4jpz.name.com"]

DNSSEC = unsigned

dig:

Question

[redacted]-career.com

Answer

""

; <<>> DiG 9.14.12 <<>> [redacted]-career.com ANY

;; global options: +cmd

*Figure 14.* Executive Report emailed to information security analysts.

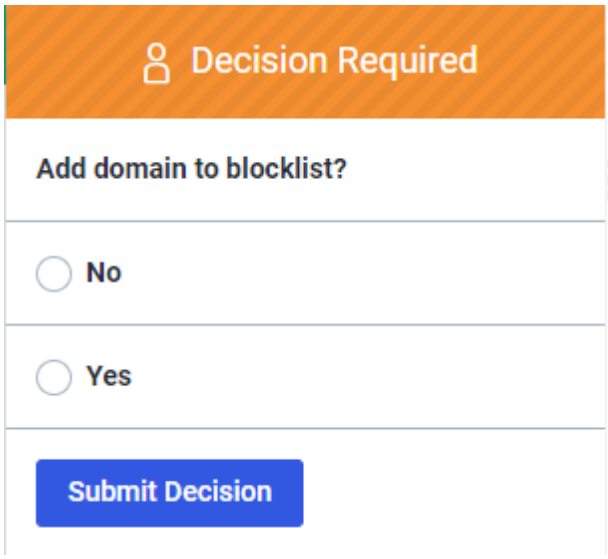


*Figure 15.* Human decision needed to block the domain in InsightConnect.

In case a domain was registered first and a certificate added at a later date, the workflow was tested again. A second domain of companya-careers.com was registered. The alert for the similar domain was generated by Recorded Future, but the workflow exited without notification since a certificate was not yet registered for the domain. Later when a public certificate was registered for companya-careers.com, a second Recorded Future alert was generated, and the workflow was completed as expected to alert information security analysts to evaluate the domain.

Before the detection was developed, information security analysts were alerted to job impersonation frauds by victims who reached out to provide further information. For one domain involved in the fraud, the criminals had registered and used a similar domain three months prior to security staff becoming aware of the issue. With this detection, new domains will generate an alert within an hour of being registered or registering a new certificate.

A security analyst timed themselves receiving the domain, logging into various security platforms, enriching the domain information, and finally blocking to domain if needed. The manual process of responding to similar domain alerts took an average of 20 minutes from receiving the alert to blocking the domain. With the automated workflow, the same security analyst took two minutes to read the enriched data and make the decision to block the domain. Company A responded to 17 Identify Similar Domain

alerts over a three-month period which, based the average above, would take an information security analyst 5.67 work hours. With the new automated workflow, the same work could be done be the analyst in .57 work hours with a total savings of 5.10 workhours.

# 4. Recommendations and Implications

Job impersonation frauds are just one part of overall brand identity protection, but a growing risk according to the FBI (Harper, 2021). Companies should take precautions and watch how cyber criminals are using their brand identity through threat intelligence. The workflow presented with this research can easily be changed to enrich data from other intelligence sources beyond brand protection.

## 4.1. Recommendations for Practice

The tools used in this study were bought and used by Company A, but there are other tools that can carry out similar goals.

For the SOAR platform, a system that has integrations with other security tools, the ability to write custom workflows, and has diverse ways of triggering the workflows is the best option. Rapid7 InsightConnect provides great flexibility and a library of ready-made extensions, plugins, and workflows (Rapid7, n.d.). A workflow can be triggered using any API, from other Insight products, at a certain period of time, or by any integration that has a trigger built into the plugin, like Recorded Future and the Get New Alerts trigger.

Each action in this InsightConnect workflow used existing plugins and functionality. However, custom action can be scripted using common programming languages like Python. The ability to customize the actions taken makes InsightConnect a powerful SOAR platform.

Recorded Future was used for this project as it was set up with the domain watchlists to trigger when a similar domain is registered. For businesses with InsightConnect, but not Recorded Future, the same workflow can be achieved by using the Rapid7 Typo Squatter plugin (Rapid7, 2021b). The Typo Squatter plugin can create a trigger that searches Certstream for any domains that are similar to the list of domains

provided. Certstream is an open-source real-time certificate transparency log that lists SSL certificates as soon as they are registered (Calidog, 2021a). The workflow's detection time might improve by monitoring Certstream directly rather than relying on a third-party intelligence service. However, Recorded Future provides greater detail about domains that can be incorporated into the workflow.

It is worth noting that technical solutions will only partially help in protecting brand identity. The information security team can receive the detections and block verified suspicious domains, but other company resources are needed to fully prevent the damage from criminals. Recruiting teams should be notified at once of any domains impersonating the company in a hiring fraud so they can update the recruiting website and job descriptions to warn of criminals targeting job seekers. Corporate communication and legal teams should also be informed of the risk to create the email or letter sent to future victims of the fraud. The identification workflow can aid information security staff towards providing valuable brand intelligence information to teams that must know.

This workflow ends at blocking the domain, but the original design opened a ticket in a popular ticket platform that could then be sent to the proper recruiting, communication, and legal team members. The connection to the ticketing platform was not completed at the time of this study but would help track and create useful metrics for the executive team. It is highly recommended to integrate a ticketing platform in this workflow if deploying into production.

Finally, further action can be taken to help mitigate similar domains. If proof is obtained that scammers are actively using the domain to impersonate the business, a takedown request can be sent to the registrar. Proof can be obtained by asking the victim to supply the original email sent to them by the scammers or taking a screenshot of the webpage impersonating the business. Recorded Future can be contracted to take down malicious similar domains for widespread campaigns but automating the process would lead to faster response times.

## 4.2. Implications for Future Research

This study aims to using SOAR systems to detect brand identity risks. Job impersonation frauds are not the only threat to a brand's identity. CEO or high-level

employee impersonation can lead to CEO frauds. Phishing or credential thefts website can be set up on similar domains to trick employees into handing over their credentials. A former employee could set up a website to leak company secrets. Malicious exploits for the company's product could be published. Monitoring for suspicious similar domains can increase a company's awareness allowing the organization to discover potential problems before they become threats. Brand identity is often a missed component of many security programs because it requires good threat intelligence which take precious resources away from other employee duties.

Along with increasing the scope of how brand identity protection can elevate a security program, researching which open source and free products could accomplish the same goal would be helpful for the community. Not all business can afford these security tools and they must be careful with how they spend their limited information security resources. Most of the steps in this solution are done using open-source products, like Dig and WHOIS. Certstream has developed libraries in Python, Go, Java, and Javascript which are available on their Github page (Calidog, 2021b). A custom script could be developed to carry out the same goal of alerting and responding to similar domain attacks.

## 5. Conclusion

Dr. Eric Cole once said, "Cyber threat prevention is ideal, but detection is a must." When job scammers impersonate companies to target job seekers, prevention is difficult. However, a company's brand and reputation can still be damaged by these frauds.

Ideally, a company will purchase all typosquat and similar domains to protect their brand identity, but this option can be cost prohibitive. Cyber security tools allow companies to detect when typosquat and similar domains are registered. These alerts serve as a warning to the company that their brand identity is in danger, but information security analysts can struggle finding the time needed to respond to these alerts.

This paper proposed that by using a mixture of threat intelligence and a SOAR platform, a workflow could be mostly automated to analyze typosquat or similar domains

that were registered. It also suggested that giving companies an early warning to website impersonations can reduce risk to both the company and jobseekers. After testing, the workflow showed an excellent improvement to the intelligence gathered and reduced the time is takes for an information security analyst to process similar domain alerts.

The workflow analyzed in this paper provides real world advice for implementing similar automation at other companies. The foundation created can be improved with future research that can either (1) find more brand identity risks worth automating or (2) that can recreate this solution using completely open source or free tools. Instead of stopping the workflow at blocking the domains, further functionality can be developed, such as automatically reporting abuse to registrars for verified malicious domains. Also, this a purely technical solution to reduce the time it takes information security analyst to identify and respond to similar domain registrations. For a more effective solution, companies should find a way to include their recruiting, legal, and communication teams on these alerts so they can implement solutions to further protect brand identity.

As information security teams develop solutions to protect their systems, the criminals will change their tactics and target those who are the most vulnerable, like jobseekers. Through observation and creative problem solving, we can work towards a more secure future for all.

Ashley Taylor, infosec_taylor@protonmail.com

# References


Better Business Bureau. (n.d.). Retrieved from bbb.org: https://bbb.org/local/0734/scamstudies/jobscams/jobscamsfullstudy

Calidog. (2021a). Retrieved from Certstream: https://certstream.calidog.io

Calidog. (2021b). *Calidog Certstream*. Retrieved from Github: https://github.com/search?q=org%3ACalidog+certstream

*Cyber Criminals Use Fake Job Listings To Target Applicants' Personally Identifiable Information*. (2021, January 21). Retrieved from Internet Crime Complaint Center: https://www.ic3.gov/Media/Y2020/PSA200121

Harper, S. A. (2021, April 21). Retrieved from fbi.gov: https://www.fbi.gov/contact-us/field-offices/elpaso/news/press-releases/fbi-warns-cyber-criminals-are-using-fake-job-listings-to-target-applicants-personally-identifiable-information

Rafter, D. (2020, October 6). *What is typosquatting? How misspelling that domain name can cost you*. Retrieved from Norton: https://us.norton.com/internetsecurity-online-scams-what-is-typosquatting.html

Rapid7. (2021a, August 17). *InsightConnect Recorded Future Plugin*. Retrieved from https://extensions.rapid7.com/extension/recorded-future

Rapid7. (2021b, August 17). *InsightConnect TypoSquatter Plugin*. Retrieved from Rapid7 Extensions: https://extensions.rapid7.com/extension/typo-squatter

Rapid7. (2021c, August 17). *InsightConnect DNS Plugin*. Retrieved from Rapid7 Extensions: https://extensions.rapid7.com/extensions/dig

Rapid7. (2021d, August 17). *InsightConnect WHOIS Plugin*. Retrieved from Rapid7 Extensions: https://extensions.rapid7.com/extension/whois

Rapid7. (n.d.). *InsightConnect*. Retrieved from Rapid7: https://www.rapid7.com/products/insightconnect

Recorded Future. (2020, April 09). *Domain Abuse Alerts*. Retrieved from Recorded Future Support: https://support.recordedfuture.com/hc/en-us/articles/360056261654-Domain-Abuse-Alerts-

*Recruitment Fraud & Job Scam Alerts*. (n.d.). Retrieved from ServiceNow: https://www.servicenow.com/fraudulent-job-scams.html


Ashley Taylor, infosec_taylor@protonmail.com

Security, U. D. (2021, January 15). *Job Scam Impersonation Email "UMBC Student Job"*. Retrieved from University of Maryland, Baltimore County: https://itsecurity.umbc.edu/home/covid-19-news/post/98486/



Ashley Taylor, infosec_taylor@protonmail.com