



# REDXRAY<sup>®</sup> HOW-TO

**How To Use the REDXRAY Service.  
For Analysis & Reporting**

<b>RISK DASHBOARD</b>	<b>2-3</b>
<b>COMPANY PAGE</b>	<b>4-5</b>
<b>PORTFOLIO PAGE</b>	<b>6</b>
<b>REPORT WRITING</b>	<b>7-8</b>
<b>REPORT EXAMPLE</b>	<b>9-10</b>
<b>DATA COLLECTIONS</b>	<b>12-16</b>
<b>APPENDIX</b>	<b>17</b>

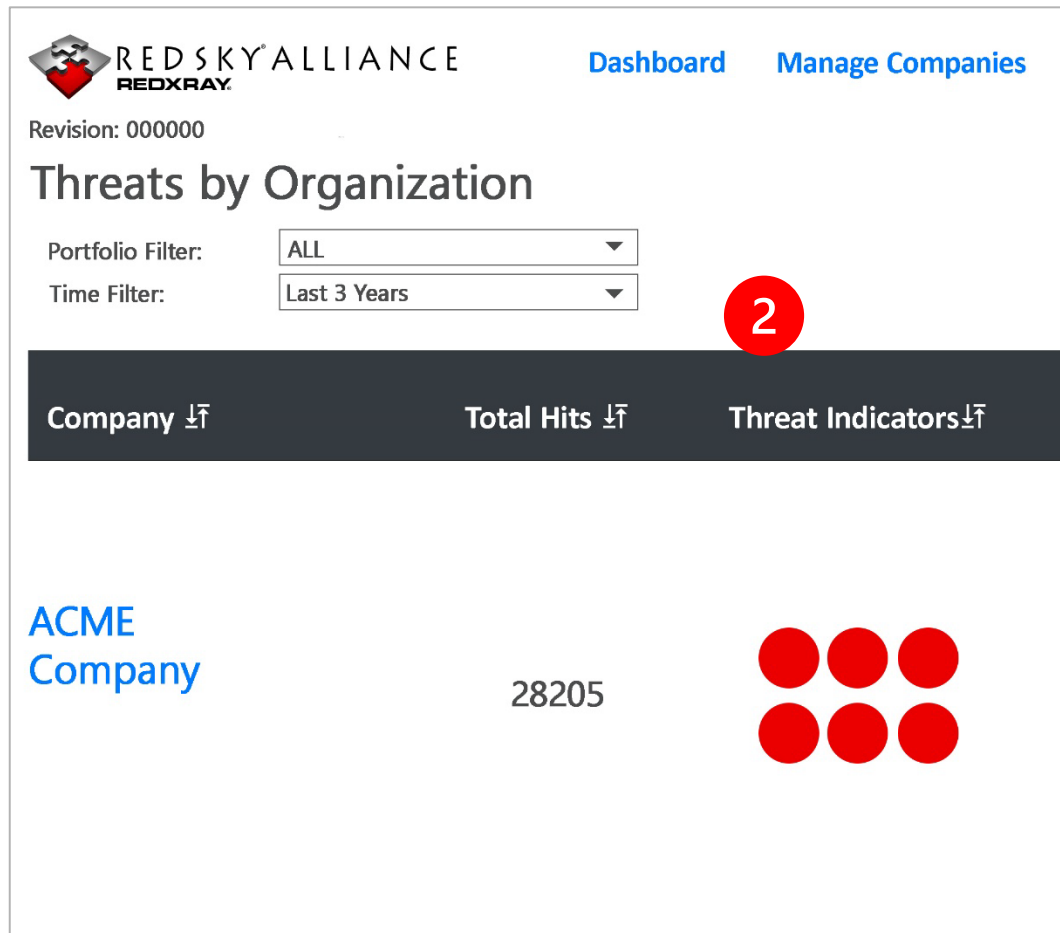


## QUICK START

# Risk Dashboard

**1** Navigation bar: allows access to the different areas of REDXRAY. Dashboard opens the Risk Dashboard, Manage Companies opens the company management page, Manage Portfolios opens the portfolio management page, and Manage Jobs opens the indicator package management page.

**2** Dashboard Filters: multiple filters are available for changing which companies are shown on the dashboard. The Portfolio filter restricts the companies shown to those that are only included in the selected portfolio. The time filter restricts the companies shown to those that only have a positive number of threat indicators during

**1**

REDSKY ALLIANCE  
REDXRAY

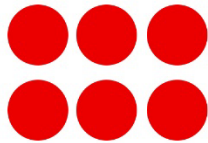
Revision: 000000

Dashboard Manage Companies

## Threats by Organization

Portfolio Filter: ALL

Time Filter: Last 3 Years

Company ↓↑	Total Hits ↓↑	Threat Indicators ↓↑
ACME Company	28205	

**2**

## QUICK START

# Risk Dashboard

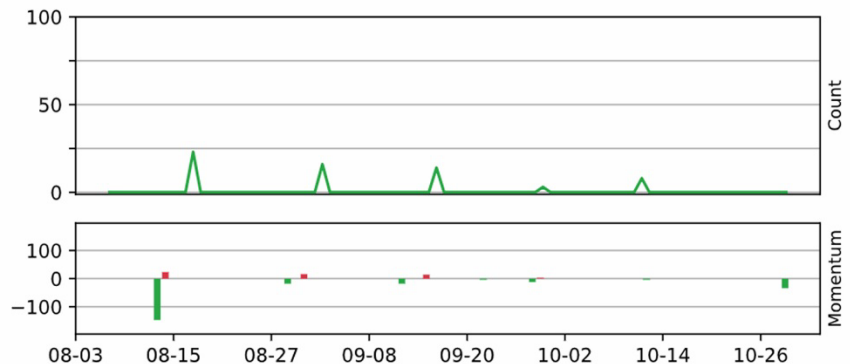
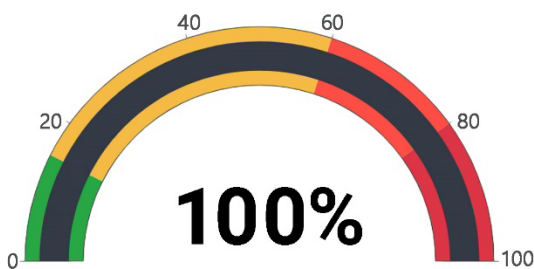
3

Threat Graphs: the Threat Risk gauge shows a calculated "threat risk" score based on the number of threat hits found and their associated collection for the given time frame. The Threat Activity chart visualizes the number of

threat hits found in our system per day in the given time frame. The lower momentum chart shows the changes in the level of activity per day. Red indicators going up means more threats were found than the previous day, green indicators going down means fewer threats were found.

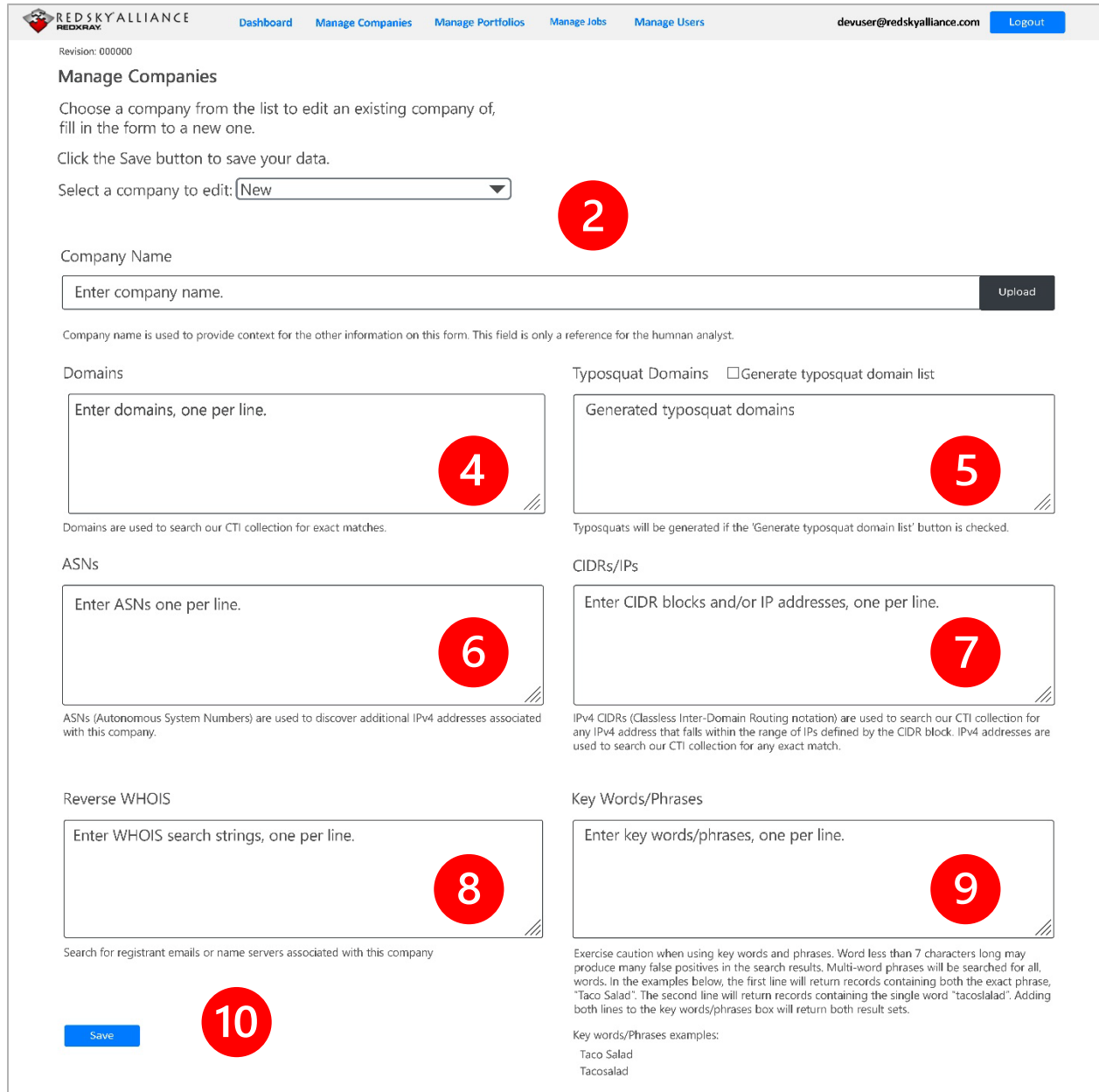
[Manage Portfolios](#)[Manage Jobs](#)[Manage Users](#)

devuser@redskyalliance.com

[Logout](#)3y Threat Risk By Threat Activity 

## QUICK START

# Company Page



Revision: 000000

## Manage Companies

Choose a company from the list to edit an existing company of, fill in the form to a new one.

Click the Save button to save your data.

Select a company to edit:

Company Name

Company name is used to provide context for the other information on this form. This field is only a reference for the human analyst.

Domains

Domains are used to search our CTI collection for exact matches.

Typosquat Domains  Generate typosquat domain list

Typosquats will be generated if the 'Generate typosquat domain list' button is checked.

ASNs

ASNs (Autonomous System Numbers) are used to discover additional IPv4 addresses associated with this company.

CIDRs/IPs

IPv4 CIDRs (Classless Inter-Domain Routing notation) are used to search our CTI collection for any IPv4 address that falls within the range of IPs defined by the CIDR block. IPv4 addresses are used to search our CTI collection for any exact match.

Reverse WHOIS

Search for registrant emails or name servers associated with this company

Key Words/Phrases

Exercise caution when using key words and phrases. Word less than 7 characters long may produce many false positives in the search results. Multi-word phrases will be searched for all words. In the examples below, the first line will return records containing both the exact phrase, "Taco Salad". The second line will return records containing the single word "tacosalad". Adding both lines to the key words/phrases box will return both result sets.

Key words/Phrases examples:  
Taco Salad  
Tacosalad



## QUICK START

# Company Page

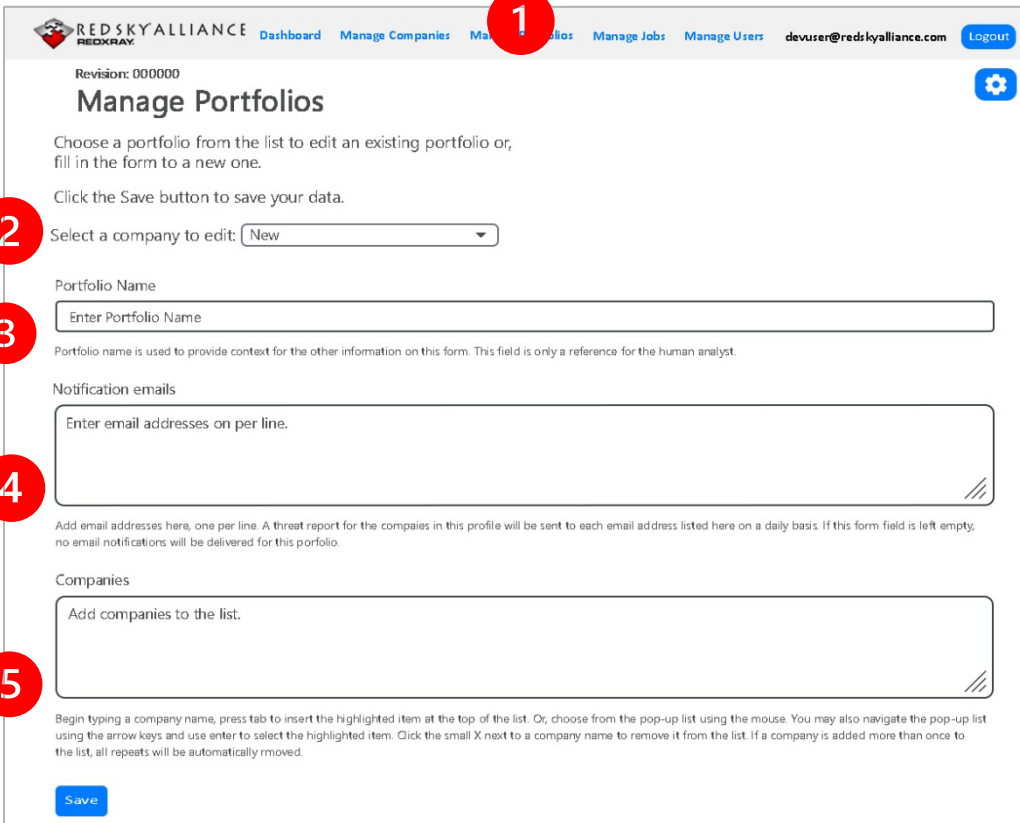
- 1** The Manage Companies page is where you will add or edit companies for your collection campaigns. Be sure to enter parameters thoroughly.
- 2** Company Selection: Select an existing company here to edit it or leave as "New" to create a brand-new company.
- 3** Company Name: The name you wish to provide the company for internal use only. This name has no bearing on search results and will only be used for your campaign management.
- 4** Domains: Enter any domains associated with your company here. Search results will also contain subdomains, so entering "microsoft.com" should also yield "email.microsoft.com" in search results.
- 5** Typosquat Domains: Enter any typo domains, such as "m1crosoft.c0m" into this box. You may enter them manually or check the "Generate typosquat domain list" box to generate a list upon saving the company. Only currently registered domains will be generated for this list.
- 6** ASNs: Enter any associated autonomous service numbers here. As these numbers correspond to sets of CIDR blocks, our backend system will use any ASNs to automatically populate the CIDR block and IP box (7) upon saving the company.
- 7** CIDRs/IPs: Enter any associated CIDR blocks or IP addresses here. Numbers can be entered in either standard IP format: 192.168.0.1 or in CIDR format: 192.168.0.0/32
- 8** Reverse WHOIS: Enter any domain registrant information here, such as email addresses or name servers. Our system will use this information to perform a reverse WHOIS search and automatically populate some of the other parameters on this page. This function will only work on domains that do not have privacy services enabled.
- 9** Keywords: Enter any general keywords, phrases, or numbers here related to the campaign. This is a good place to enter names, emails, products, and services. Take care to consider punctuation. Entering a phone number as "1234567899" rather than "123-456-7899" may produce different search results.
- 10** Save: Press this button once all your parameters have been entered or updated. Our backend system will handle additional generation steps after this and update the company's entry on the dashboard as soon as possible



## QUICK START

# Portfolio Page

- 1 The Portfolio page is where you will add or edit portfolios, which will allow you to receive daily notifications on collection campaigns.
- 2 Portfolio Selection: Select an existing portfolio here or leave as "New" to create a new portfolio.
- 3 .Portfolio Name: Enter the name you wish to use for the portfolio. This name will have no effect on search results or notification outcomes. It is for internal use only.
- 4 Notification Emails: Enter the email addresses for those who should receive notifications about the portfolio. Notification emails are sent out daily and will detail any threat matches found in our system for the associated companies in the last 24 hours.
- 5 Companies: Enter the names of the companies to add to the portfolio here. Threat data for these companies will be aggregated for the daily notification email. Companies need to first be created using the Manage Companies page before they can be added to a portfolio.



REDSKY ALLIANCE REDXRAY Dashboard Manage Companies Manage Portfolios Manage Jobs Manage Users devuser@redskyalliance.com Logout

Revision: 000000

## Manage Portfolios

Choose a portfolio from the list to edit an existing portfolio or, fill in the form to a new one.

Click the Save button to save your data.

2 Select a company to edit:

3 Portfolio Name

Portfolio name is used to provide context for the other information on this form. This field is only a reference for the human analyst.

4 Notification emails

Add email addresses here, one per line. A threat report for the compaes in this profile will be sent to each email address listed here on a daily basis. If this form field is left empty, no email notifications will be delivered for this porfolio.

5 Companies

Begin typing a company name, press tab to insert the highlighted item at the top of the list. Or, choose from the pop-up list using the mouse. You may also navigate the pop-up list using the arrow keys and use enter to select the highlighted item. Click the small X next to a company name to remove it from the list. If a company is added more than once to the list, all repeats will be automatically removed.

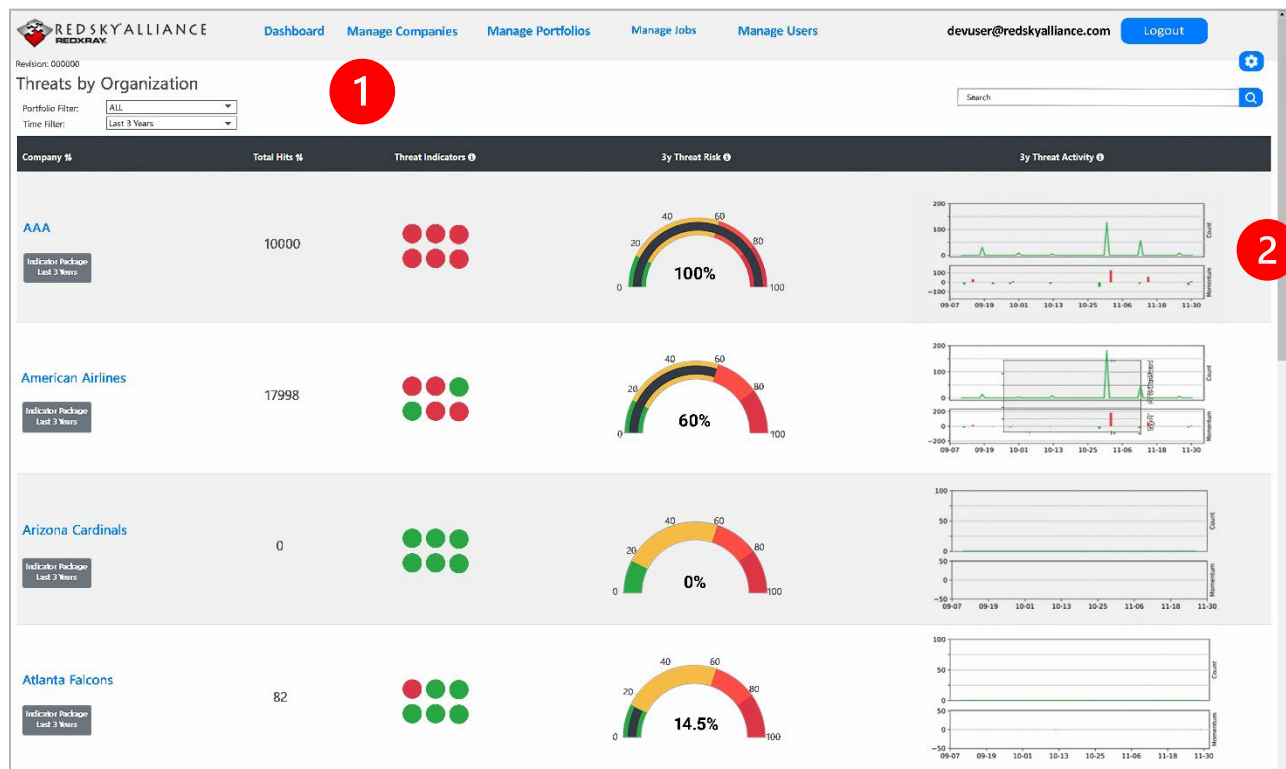
Save

## QUICK START

# Analysis & Report Writing

**1** Now that you have your collection results, it is time to analyze those indicators. Analysis comprehension may vary with the experience of the analyst. Below we provide 'basic' mitigation options.

**2** It is important to note that the REDXRAY tool shows the Total "hits" in the six (6) aggregated data indexes. This is derived from our ten (10) data sets, described below. This is for the ease of REDXRAY analysis. Below is an example of a collection campaign dashboard..



## REPORT

# Analysis & Report Writing

- 1 The Threat Indicators (Red and Green Dots) show the current number Indicators of Compromise (IoCs) in association to the selected Time Filter. The Threat Risk dial is a weighted percentage of IoCs in relation to the selected Time Filter. The higher the percentage – the higher the predictive IoC Risk. The Threat Activity shows a timeline of IoCs in relation to a specified time filter. The Indicator Package box provides the IoCs in CSV formats. REDXRAY also has an API provide threat IoCs in JSON format. See Appendix: A.

Threat Type	Count	Status	Indicator	Indicator Type	Threat Hits	Newest Hit	
Breach Data	964	●	com	domain	945	2023-06-24T03:40:49	<a href="#">View Threats</a>
Malware Data	0	●	23.4.0.0/19	cidr	32	2023-08-14T18:00:01	<a href="#">View Threats</a>
Malicious Email Hits	28	●	2.22.0.0/21	cidr	12	2023-09-15T17:36:22	<a href="#">View Threats</a>
Phishing Hits	4	●	2.17.0.0/21	cidr	9	2022-11-30T19:23:29	<a href="#">View Threats</a>
OSINT	19	●	23.6.0.0/19	cidr	8	2023-01-13T18:42:32	<a href="#">View Threats</a>
Darkweb	0	●	23.61.80.0/20	cidr	5	2023-01-13T18:42:27	<a href="#">View Threats</a>
			69.192.192.0/20	cidr	2	2023-05-04T14:55:28	<a href="#">View Threats</a>
			2.16.46.0/23	cidr	1	2023-03-15T11:31:41	<a href="#">View Threats</a>

**You can now write a REDXRAY report for sales or a client.**

- 2 To view the raw data collected, there are two options: On the first page, the 'Indicator Package' and be downloaded with a .csv or JSON format, or the "View Threats" button which provides similar results.
- 3 The IP package can also be loaded into an organization's SIEM and these identified cyber threats can be blocked/blacklisted if they are observed again. This helps cyber threat defenders to be proactive in avoiding cyber breaches and to comply with on-going cyber threat defense sections of CMMC and NIST 800-171 assessments.



## REPORT

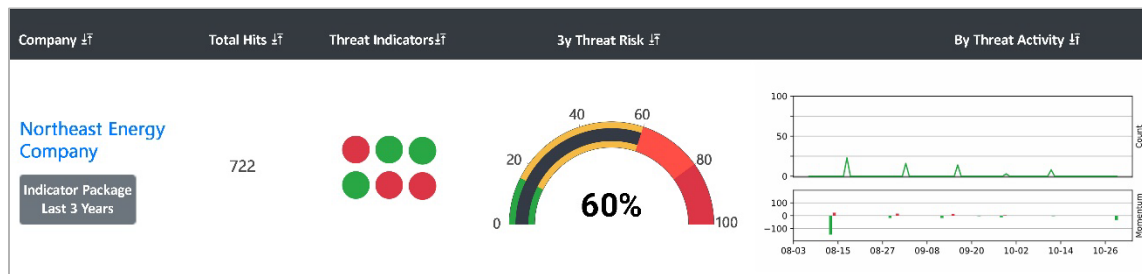
# Report Example

## Northeast Energy Company Analysis

Below is a real-life example of a collection campaign against an anonymous named energy company in the Northeast United States. This is a sample analysis to help train REDXRAY users. Analysts created numerous collection parameters in the Manage Companies page:

### Summary

A preliminary intelligence collection and research effort of open and proprietary sources identified threats and vulnerabilities associated with Northeast Energy Company.



Our search includes the following indicators as defined by our analysts ahead of time within the 'Manage Companies' page. All results displayed and the depth of our analysis will be from the previous 3-year time span.

1

Northeast Energy Company

Time Filter: Last 3 Years

Threat Type	Count	Status	Indicator	Indicator Type	Threat Hits	Newest Hits	
Breach Data	709	●	eversource.com	domaon	706	2023-11-15T204026	<a href="#">View Threats</a>
Malware Hits	0	●	156.73.0/16	cidr	13	2022-06-01P1912	<a href="#">View Threats</a>
Malware Email Hits	0	●	159.508.0/16	cidr	2	2023.05.04T5528	<a href="#">View Threats</a>
Phishing Hits	0	●	eversource.com	typosquats	1	2022-11-16T05:3513	<a href="#">View Threats</a>
OSINT	13	●	Joseph H. Nolan, Jr.	keywords	0		<a href="#">View Threats</a>
Darkweb	0	●					

## REPORT

# Report Example

## Northeast Energy Theat Type Descriptions

### Breach Data

1

After examining the breach data results from the domain, we can observe username and password data in differing formats: `firstname.lastname`, `LastnameFirstname`, and `FirstInitialLastname`. When examining these patterns, we could verify that the username and password combinations for the `firstname.lastname` pattern could belong to former and current employees.

Examining farther back to the COMB breach in 2021, we noticed many of these emails duplicated 6 times with deferring simple passwords. Each of these passwords were 8 characters composed of numbers and lowercase letters. We have determined that these passwords may be employee account recovery codes, allowing for malicious actors to take control of employee accounts.

***Mitigation: The company in this instance would require changing all recovery codes for every employee contained within the breach.***

Beach results within the CIDR block `157.108.0.0/16` displayed a single result that was duplicated in 2 differing breaches of similar names (the latter likely being republished). Information included in this breach appeared to be username, email, ip addresses for an array of domains in various sectors, uncracked password information, and another undefined 5<sup>th</sup> field.

***Mitigation: Immediately change passwords and if needed, the email addresses.***

### OSINT

Indicators contained within these OSINT results were false flags. This was confirmed by visiting the original Pastebin source these indicators were collected from. It was determined that each result happened to be a substring within a larger string containing numbers separated at various points by the `'.'` character.

***Mitigation: Determine the malicious data context. Determine the severity of the finding with your IT staff and consider the value of the information in a social engineering context.***

## REPORT

# Report Example

**Malware Hits (example Botnet Tracker, Sinkhole)**

No Hits in a condensed set from our Botnet Tracker and proprietary Sinkhole collection source. See below appendix for further descriptions.

***Mitigation: Use network diagnostic tools to validate the findings. Add the malicious domain to your firewall, web proxy, IDS, or IPS block list. Determine if the organization's chosen antivirus solution is effective against the associated malware.***

**Malicious Email Hits**

No Hits - These type collection indicators of compromise are extracted from the headers of emails where malicious attachments are detected. This includes the company email routing information, senders, recipients, and subject lines. On these records analysis can determine industry sector (energy) and geolocation of the sources.

***Mitigation: These emails need to be blacklisted. Check organization's chosen antivirus solution is effective against the associated malware.***

**Phishing Hits**

No Hits – Phishing Hits indicate that known malware was being directed at the Energy Company.

***Mitigation: Blacklist emails used to phish and employee. Change passwords and if needed, domains of the victim employee.***

## SOURCES

# Data Sets

## Monitor Botnets

Botnets are often used to steal data, commit distributed denial of service (DDoS) attacks, send malicious emails, or simply proxy for malicious internet traffic. If your IP address is found in the botnet tracker, it means that it was seen in communication with a malicious endpoint. The botnet does not automatically indicate a malware infection as there are many reasons why two IP addresses might communicate but typically shows suspicious/malicious activity.

### Monitor Botnets Action Items

**1**

Use network diagnostic tools to validate the finding. Identify any internal systems communicating with the botnet or proxy server IP address identified in the result. Tools will help you determine how widespread a potential malware infection may be.

**2**

If there is no use case for your organization to be communicating with the identified malicious IP address, add it to your firewall, IDS, or IPS block list.

**3**

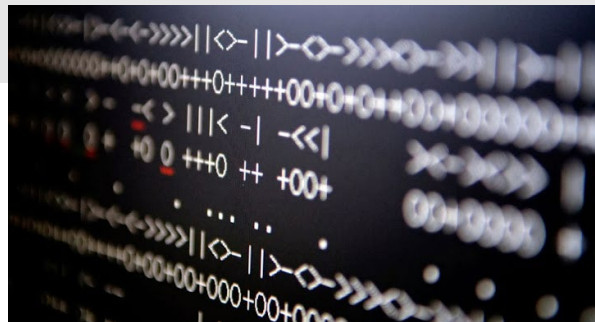
If there is no use case for your organization to be communicating with the identified malicious IP address, add it to your firewall, IDS, or IPS block list.

**4**

Determine if the organization's chosen antivirus solution is effective against the associated malware. If not, conduct a network hunt for indicators of compromise associated with the identified malware.

**5**

Ensure all antivirus and OS updates have been applied to the affected systems



## SOURCES

# Data Collections

## Data Breach Research

Breach data hits are from public database leaks. Depending on the nature of the leaked database, exposed information may vary from just email addresses to username and password combinations and other personally identifiable information. REDXRAY contains the raw breach data so you can easily see what type of data has been exposed. If the breach data includes passwords, then Red Sky® Alliance recommends enforcing a password reset and investigating whether there has been unauthorized access to that account. Some companies believe that the disclosure of "old" or historical passwords is low risk. This is false, however, as many attackers use old passwords to brute force/predict current passwords. Old passwords can also be used in fraud/phishing attacks as a way to build trust.

## Breach Data Action Items

**1**

Activate multi-factor authentication for affected user accounts to reduce the efficacy of leaked account credentials.

**2**

For recently dated breach data, force password resets for affected user accounts.

**3**

Audit the raw breached password to determine if password policies enforce adequate length and complexity requirements.

**4**

Audit for password re-use of leaked account credentials.

**5**

For older breach data, check the date of the last password change for the affected user accounts to determine the probability that the password may still be in use. Force a password change if in doubt.



## SOURCES

# Data Collections

## Compromised Keylogger

An email address was observed in clipboard data on an infected computer. For example, a user infected with keylogger malware cut & pasted an email address belonging to your organization. The raw source data can be investigated to determine the best course of action. 1) Keylogger malware runs on your network. A username and password belonging to an employee were captured by a keylogger. An email address was observed in clipboard data on an infected computer. For example, a user infected with keylogger malware cut & pasted an email address belonging to your organization. The raw source data can be investigated to determine the best course of action.

## Compromised Keylogger Action Items

**1**

Determine if the organization's chosen antivirus solution is effective against the associated malware.

**2**

Conduct a network hunt for indicators of compromise associated with the identified keylogger and remove them if found.

**3**

Use the finding to identify the host system and user account infected with the keylogger.

**4**

Force password changes for all accounts for users who use a system infected with a keylogger.

**5**

Disable any user accounts identified in the finding as infected with a keylogger.

**6**

All account credentials used by all users on this system to log in to other systems have a high probability of being captured and exfiltrated.

**7**

Disable any user accounts used to log in to the host system identified in the finding as infected with a keylogger.

**8**

Force password changes for any user accounts used on the host system identified in the finding as infected with a keylogger.

**9**

Reenable user accounts after password changes have been completed or create new accounts for the affected users..

**10**

Ensure all antivirus and OS updates have been applied to the affected systems.

## SOURCES

# Data Collections

## Malicious Email Attachments

If your domain or IP address shows up in this collection, it means it was observed in the header of an email that has been identified as malicious (1 or more AV detection).

The raw email should be inspected to see whether it was sent to or from your organization or if it was spoofed using your organization's data. It should be noted that some AV vendors classify emails as malicious when they are actually benign. All malicious email hits only indicate targeting but can sometimes indicate a malware infection.

## Malicious Email Action Items

**1**

Using a sample of any malicious attachments identified in the finding, determine if the organization's chosen antivirus solution is effective against the associated malware. If not, conduct a network hunt for indicators of compromise associated with the identified malware.

**2**

If the email was sent to your organization: audit the targeted user's email account and client computer to determine if the malicious email was read and if any malicious attachments were downloaded.

**3**

If the email was sent FROM your organization, analyze the email header data to determine if the information was spoofed or if the email legitimately originated from your organization. If it legitimately originated from your organization, audit your email.

**3****3**

## SOURCES

# Data Collections

## Proprietary Sinkhole Collection

A sinkhole hit means your IP was observed in weblogs from our sinkhole server. Similar to the botnet tracker hits, it means that communication to a malicious domain was observed. The nature of that communication needs to be determined from the raw sinkhole record. If the sinkhole is a result of a malware infection, then the information should be referred to incident responders

### Proprietary Sinkhole Action Items

**1**

Use network diagnostic tools to validate and identify any internal, this will help you determine how widespread malware infection may be.

**2**

Add the malicious domain to your firewall, web proxy, IDS, or IPS block list.

**3**

Assess systems associated with the IP address identified in the finding and remove any malware or unauthorized proxy software.

**4**

A network hunt for indicators of compromise associated with the identified malware on your organization's IT assets and remove them if found.

**5**

Ensure all antivirus and OS updates have been applied to the affected systems.

## Identifying Phishing Emails

When you want to know if someone was using your company's domain to commit phishing attacks against customers or even employees? CTAC is a service developed and owned by Red Sky® Alliance, of both primary sourced indicators and open-source indicators from dozens of sources. Each hit from this collection should be individually analyzed as each source has a different context. According to CSO Online, phishing attacks account for more than 80% of reported security incidents. Reputational damage aside, \$17,700 is lost every minute due to a phishing attack

### Identifying Phishing Emails Action Items

**1**

Add malicious phishing domains to your organization's firewall, web proxy, IDS, or IPS block list.

**2**

Consider notifying supply chain partners and customers about phishing domains and links that appear to be impersonating your organization.



## SOURCES

# Data Collections

## Source Code Secrets

Disclosure of sensitive information can be found with Source Code Secrets. The Source Code Secrets dataset is available to users who want to monitor GitHub, GitLab, and Bitbucket for accidental disclosure of sensitive information. Sometimes, programmers will purposely or accidentally add credentials such as API keys, cryptography keys, or usernames & passwords for third party services to their publicly visible software repository without thinking about the security implications.

Source Code Secrets data can be used for any/all industry segment investigation including critical infrastructure Defense Industrial Base Sector and all commercial segments

## Source Code Action Items

**1**

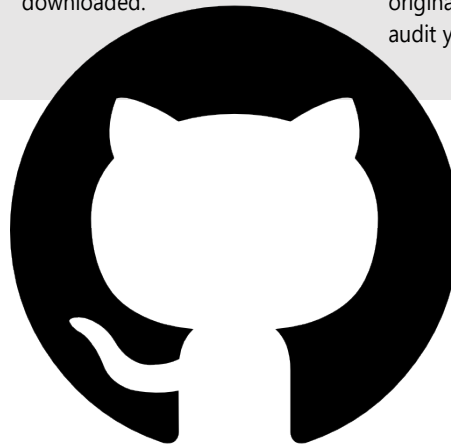
Using a sample of any malicious attachments identified in the finding, determine if the organization's chosen antivirus solution is effective against the associated malware. If not, conduct a network hunt for indicators of compromise associated with the identified malware.

**2**

If the email was sent to your organization: audit the targeted user's email account and client computer to determine if the malicious email was read and if any malicious attachments were downloaded.

**3**

If the email was sent FROM your organization, analyze the email header data to determine if the information was spoofed or if the email legitimately originated from your organization. If it legitimately originated from your organization, audit your email.



## SOURCES

# Data Collections

## Dark Web (REDPANE)

This data set actively monitors dozens of underground and dark websites where criminal activity takes place and is discussed. This data includes information gathered from Tor sites and a few select surface web cybercrime sites. Using dark web data, analysts can learn about what threat actors are talking about, and where the discussion is taking place. Threat actors often advertise access to victim networks or leak sensitive information stolen during attacks. The data contains indicators from dark web forums, marketplaces, and ransomware leak sites. Threat actors often discuss or brag about their attacks. They also share tactics, techniques, and procedures. Analysts can search through dark web forums to see what threat actors are saying about them, their company, or their industry.

Attackers are not just stealing data, they are selling it. Some are even selling the access they obtained illegally on purchase websites. Companies can monitor what threat actors are selling and monitor for attackers claiming to have access to, or stolen data from, their company.

Ransomware actors have evolved from simply holding a network hostage. Ransomware groups are now working together to earn higher profits. Dark web ransomware data allows analysts to see who has been breached, who is selling access to which networks, and which data ransomware groups are publishing simply as punishment for non-payment. Companies can also monitor when their supply chain is compromised which may lead to future cyber-attacks.

Dark Web data can be used for any/all industry segment investigation including critical infrastructure Defense Industrial Base Sector and all commercial segments.

## Dark Web Action Items

**1**

Investigate to see if your company's data or network access is for sale on the dark web.

**2**

Are there threats against your company officers or locations posted?

**3**

Are there ransomware threats or ransomware payments posted?

**4**

Track hacker network penetration methods or malware that is for sale.

## SOURCES

# Data Collections

## Paste Storage Sites (OSINT)

This includes various sources such as paste websites, forums, and other sites where malicious activity may take place. Is one of your employee email addresses listed in an Anonymous targeting operation? Is someone running vulnerability scans against your networks and posting the results publicly? Find out by searching through the REDXRAY OSINT collection.

## OSINT Action Items

**1**

Using a sample of any malicious attachments identified in the finding, determine if the organization's chosen antivirus solution is effective against the associated malware. If not, conduct a network hunt for indicators of compromise associated with the identified malware.

**2**

If the email was sent to your organization: audit the targeted user's email account and client computer to determine if the malicious email was read and if any malicious attachments were downloaded.



## SOURCES

# Appendix

## A. Red Sky Alliance Data Sets

(It should be noted that these ten [10] data sets described below are combined in the REDXRAY provided collection results, at six [6]. This was for the ease of an analyst.)

We daily collect on the below threat indices:

**Botnet Tracker** - Before 2020, this data set tracked IPs that communicated with known botnet IPs. From 2020 to present, we track publicly accessible open web proxies. This is because bad actors can use these proxies to leverage attacks while masking their own IP.

**Breach Data** - We collect from more than just the large known data breaches. We have proprietary processes to collect breach data from less visible sources.

**Dark web Data** - Dark web data is collected from a variety of pages on the Tor network and their plain web mirrored counterparts or plain-web forums with intent overlap. This includes forums, ransomware listings, and marketplaces. Data found in this is broad as it will contain companies already breached, various login credentials (personal and business), and variety of software, identification papers, and counterfeit items for sale.

**Open Source Data (OSINT)** - OSINT includes miscellaneous sources such as paste websites, forums, and other sites where malicious activity may take place.

**Keylogger Data** - We collect against known keylogger aggregation points. We use propriety processes to determine where these aggregation points are and collect against them. We have not yet seen other companies with the same data from this collection. Data includes the attacking server, indicators, and victim IP (if known).

**Malicious Emails** - This is a collection of indicators extracted from the headers of emails where malicious attachments are detected. This includes email routing information, senders, recipients, and subject lines. On records where possible, we have determined industry sector and geolocation.

**"Paste" type Sites (i.e., Pastebin)** - This index contains domains, emails, and IP addresses extracted from sites, such as pastebin.com. Indicators in this collection are geolocated when possible. We personally store these references for informational requests, well after the original link may have been removed.

**Sinkhole Traffic** - We run a proprietary sinkhole and collect indicators from known former malicious domains. This data is not available from any other source.

**Source Code Secrets** - We collect authentication keys, usernames and passwords, and API keys from open sources where users may have failed to properly configure their GitHub, GitLab, or bitbucket repositories.

**Threat Recon** - Aggregation of other open-source threat intel mainly concerning IPs of known threat actors.

## B. Quick Start Video Instructions

*Do we want to put the video in a private link or page? I would not share with the public but just our partners.*

Red Sky Alliance Corporation is a Cyber Threat Analysis and Intelligence Service organization. For sales, questions or training please contact our office directly at 1-844-492-7225, or [feedback@redskyalliance.com](mailto:feedback@redskyalliance.com)

## Red Sky® Alliance

Red Sky® Alliance Corp. is a privately held USA-owned cyber threat intelligence firm that delivers proprietary cyber threat intelligence datasets and services. Our company delivers insightful, actionable intelligence in formats best suited to your strategic, operational, and tactical needs.

**Founded in 2011** by the developer of the world's first enterprise payment server that allowed for credit card transactions on the Internet in 1996. Red Sky Alliance focuses on identifying targeted cyber threats against specific entities and providing the detail behind the threats, including entering the cyber threat intelligence into any SIEM and blacklisting the threats from future attacks.

Red Sky Alliance Targeted cyber threat intelligence is delivered to clients in the format they request text, email, dashboard, and API. The company's proprietary services mines Red Sky Alliance's proprietary collections, underground forums, and the dark web. The findings are then divided into ten (10) data sets that are constantly updated. Datasets can be ordered on a subscription basis too. New sources are continually being researched and added to our collections. Our approach allows clients to choose both raw indexed data and finished targeted intelligence reporting. The final product can be in the form of reports, feeds delivered via API. Analysis and notifications client services such as REDXRAY's family of services and our Cyber Threat Analysis Center (CTAC), both of which were developed and owned by Red Sky Alliance have been in service globally for over seven years.

**Jim McKee, Founder & CEO, 01 March 2024**  
[jmckee@redskyalliance.com](mailto:jmckee@redskyalliance.com)

**For More Information Contact Us:**  
**1-844-492-7225)**  
[jmckee@wapacklabs.com](mailto:jmckee@wapacklabs.com)

**Red Sky® Alliance Corp.**  
1815 Central Park Drive, Suite 337  
Steamboat Springs, Colorado 80477 USA  
[www.wapacklabs.com](http://www.wapacklabs.com)

Red Sky® Alliance and REDXRAY® are Registered Trademarks of Red Sky® Alliance Corp.

