

RiskIQ Illuminate® Internet Intelligence Platform

Security Intelligence for Your Interconnected World

Cyber Threat Workshop





BENJAMIN POWELL
RiskIQ



JOSH MAYFIELD
RiskIQ

Benjamin Powell

Director of Technical Marketing (CEH)

Background

Worked in IT for over 30 years.

Focused on Security for over 14 years.

I have personally worked in IT in the following industries:

- State government
- International Airport
- Port District
- Education
- Biotech
- Financial services
- Manufacturing
- Software development



Fun Fact:

- Be careful when you tell people in IT your hobby is spearfishing.

benjamin.powell@riskiq.net

www.linkedin.com/in/benjaminpowell



Josh Mayfield

Senior Director, Security Products

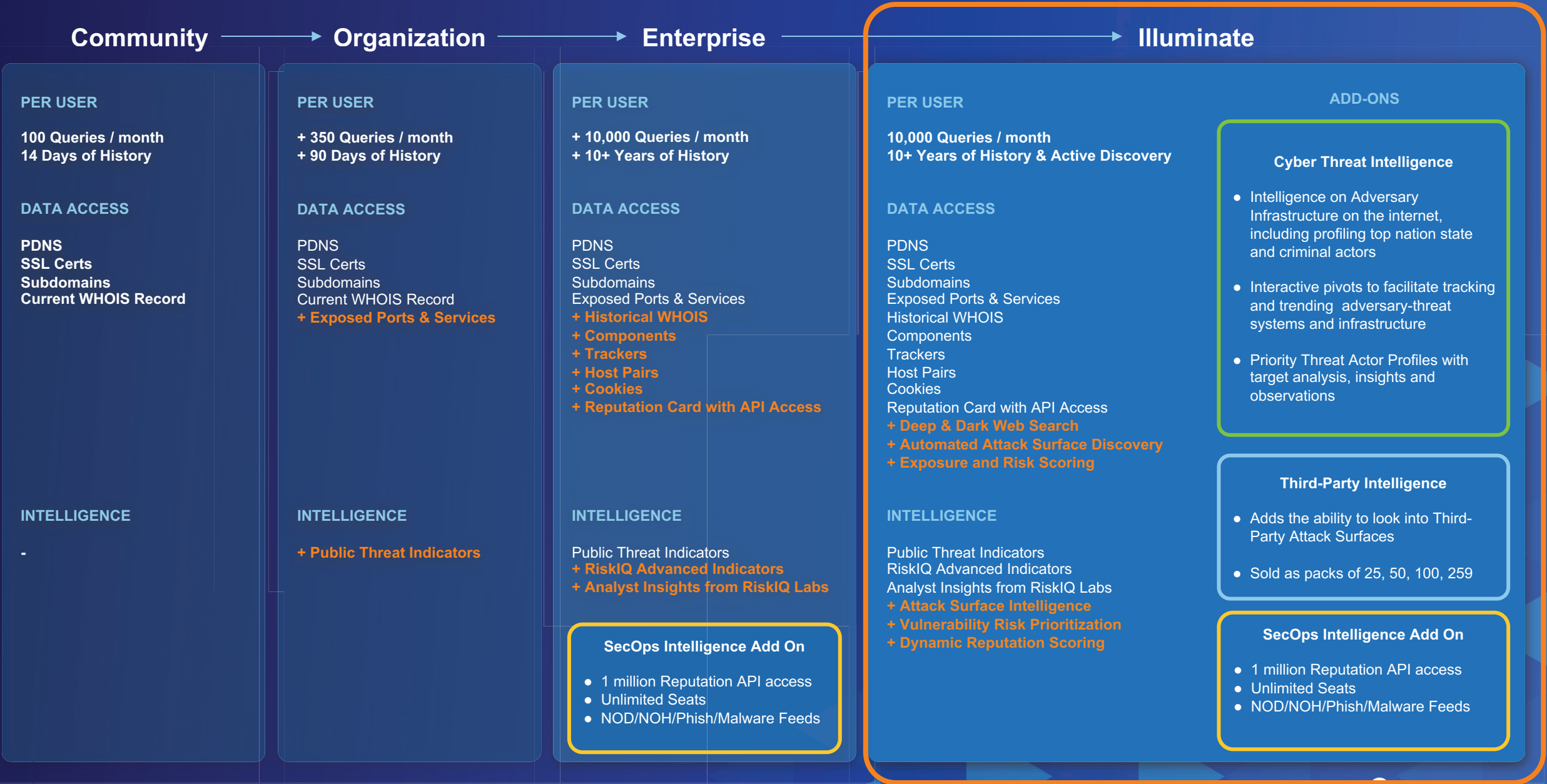
Background

MA, MBA, CCSP

10+ years in cybersecurity with a special focus on network security, frameworks, threat hunting, incident response

Featured in publications including, The Wall Street Journal, USA Today, SC Media, Forbes, and Dark Reading. Often cited by media and journalists for analysis of cryptocurrencies, threat intelligence, and attacker psychology.

RiskIQ Illuminate Internet Intelligence Platform | Products



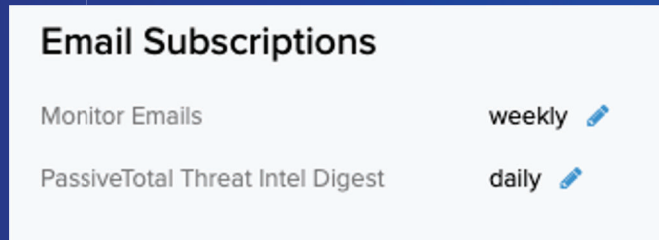
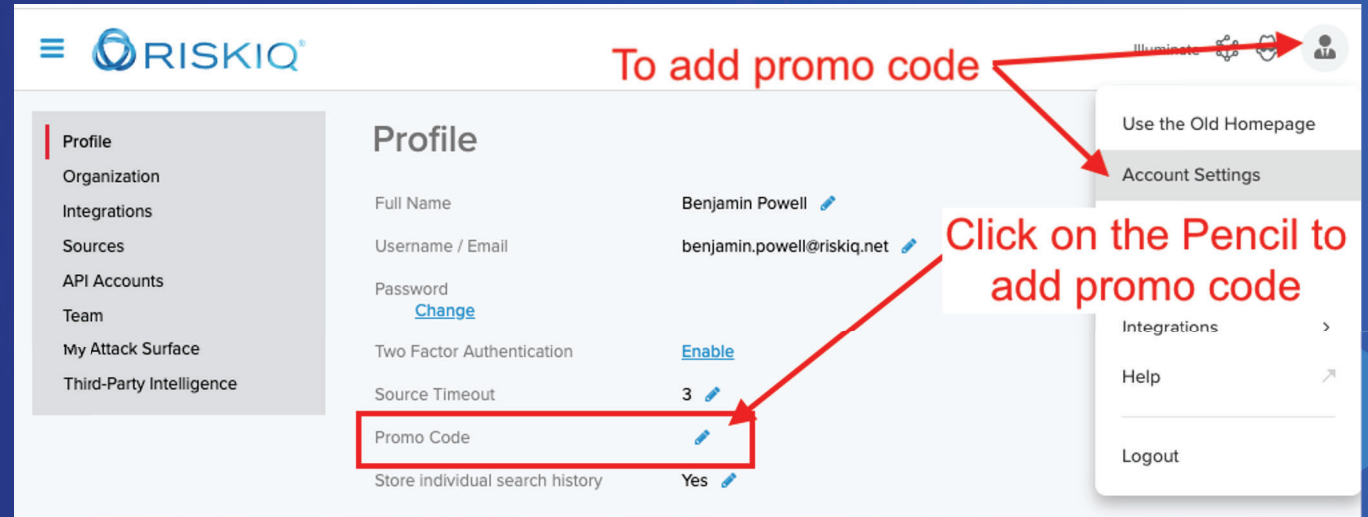
Create Your Own RiskIQ Community Account

Use a corporate email account to start your 30-day trial or enter the promo code to get 7-days of enterprise access.

1. Open your browser and go to <https://community.riskiq.com/registration>
1. Create your own RiskIQ Community Account using your company's email address.
1. Use promo code: **ctw-illuminate** (the code is case sensitive).
1. Check your email and verify your email account.

PassiveTotal Promo Code

- Please add the promo code **ctw-illuminate** to your account
- The promo code extended queries so you can have fun and investigate as much as you desire.



Tools to use in the exercises today

During the investigations we will be using the following tools.

Please bookmark the following websites.

- RiskIQ PassiveTotal <https://community.riskiq.com>
- Google Safe Browsing Check <https://transparencyreport.google.com/safe-browsing/search?hl=en>
- urlscan.io <https://urlscan.io>
- Hybrid Analysis <https://hybrid-analysis.com>

DISCLAIMER

RiskIQ's Cyber Threat Workshops include live, real-time observations from the internet.

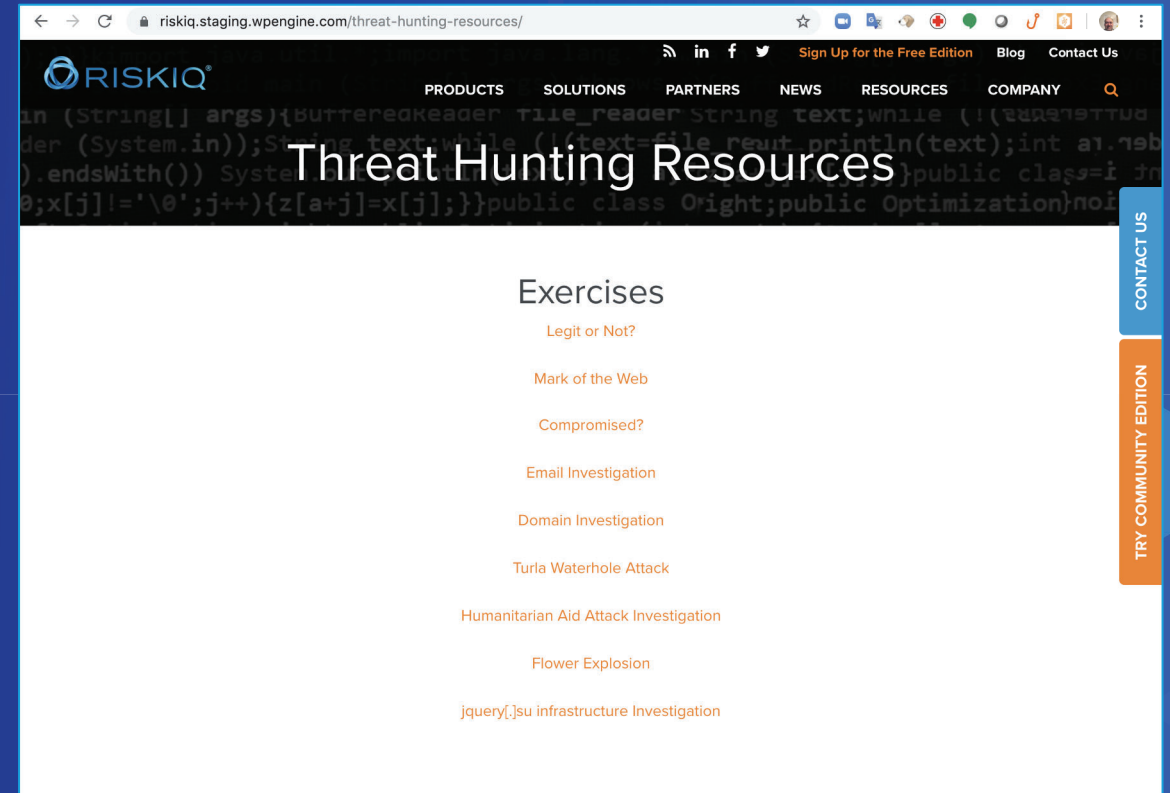
RiskIQ will share online resources (e.g., IP addresses, domain names) that are dangerous and pose a clear and present danger.

We ask our participants to use their best judgment and minimize unnecessary risk while interacting with malicious systems lab exercises.

Poll Questions

RiskIQ Hands-on Training

- How to speed up or guide investigations with Reputation Scores?
 - OSINT investigation of ObliqueRAT
- Question from management about a new vulnerability:
 - Are we at risk, or compromised?
 - What about the partners we depend upon for our business?
 - Are they at risk or compromised?
- How to protect your organization from Threat Actors or the tools and infrastructure they use?



<https://www.riskiq.com/threat-hunting-resources/>

Security intelligence challenges in real life

Real life challenges



Digital, cloud-centric transformation

Nearly infinite attacker targets, diverse assets, continuous expansion

VISIBILITY



Find and prioritize what matters

Partial collection, generic threat indicators, complex and contextual attack surface

INSIGHTS



Precise action, meaningful outcomes

Non-standard response, legacy ecosystems, workflows, processes, and technologies

OUTCOMES



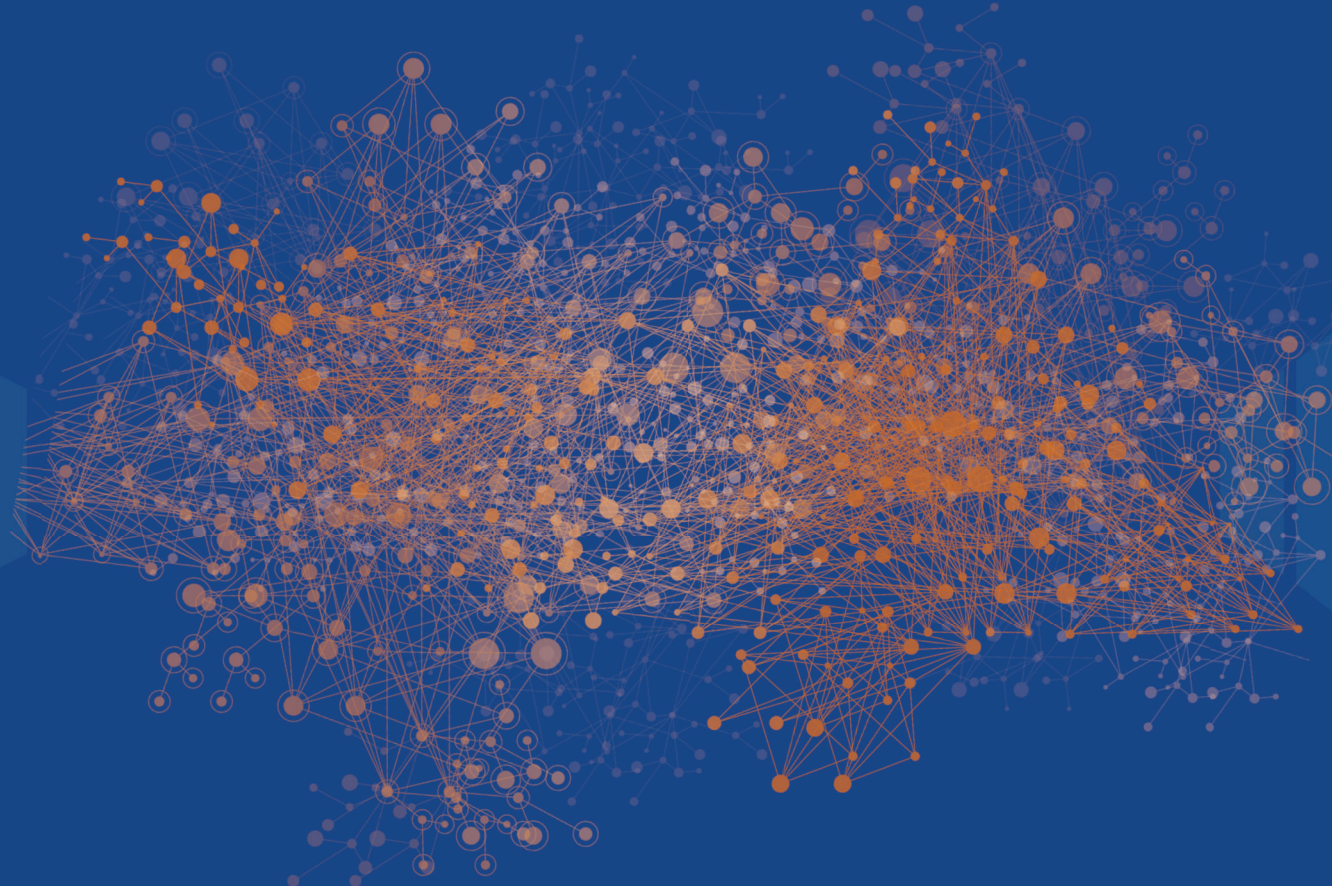
Defense at global scale

All leading to incomplete protection, limited security for the worldwide digital footprint

DEFENSE

RiskIQ Illuminate

Internet Intelligence Platform



Unified Global
Attack Surface

Tailored Attack
Surface Intelligence

Adversary-Threat
Infrastructure

Adaptive Defense At
Global Scale



Automated Discovery
and Continuous Mapping



Machine Learning and
Artificial Intelligence



Threat Research and
Security Expertise

4 Key Benefits



One Platform: Multiple Solutions

Cyber Threat Intelligence

relevant security intelligence,
via adversary infrastructure fingerprinting
for scaled defense

Security Operation Intelligence

easy-to-integrate apps and simple
APIs for SIEM, SOAR, XDR, EDR,
IPS, and other security tools

Third-Party Intelligence

identify relevant risks and exposures
across partners, eComm, digital supply
chain and dependencies

Attack Surface Intelligence

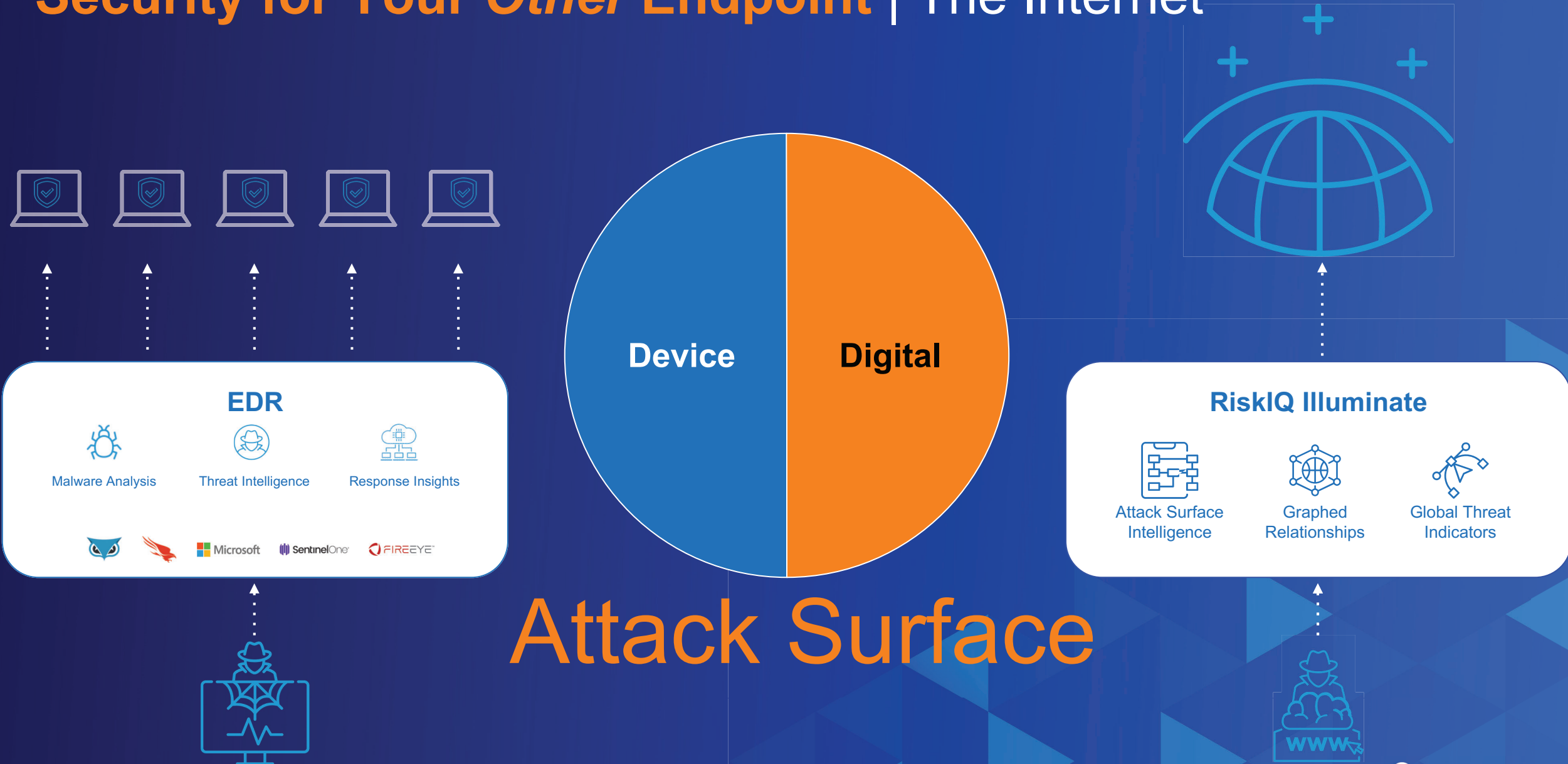
attack surface discovery to uncover
threat intelligence mapped to the
worldwide digital footprint

Vulnerability Intelligence

discover attacker-exposed assets and
targets—prioritize what matters for
faster mitigation and protection



Security for Your *Other* Endpoint | The Internet



How to speed up or guide investigations with Reputation Scores?

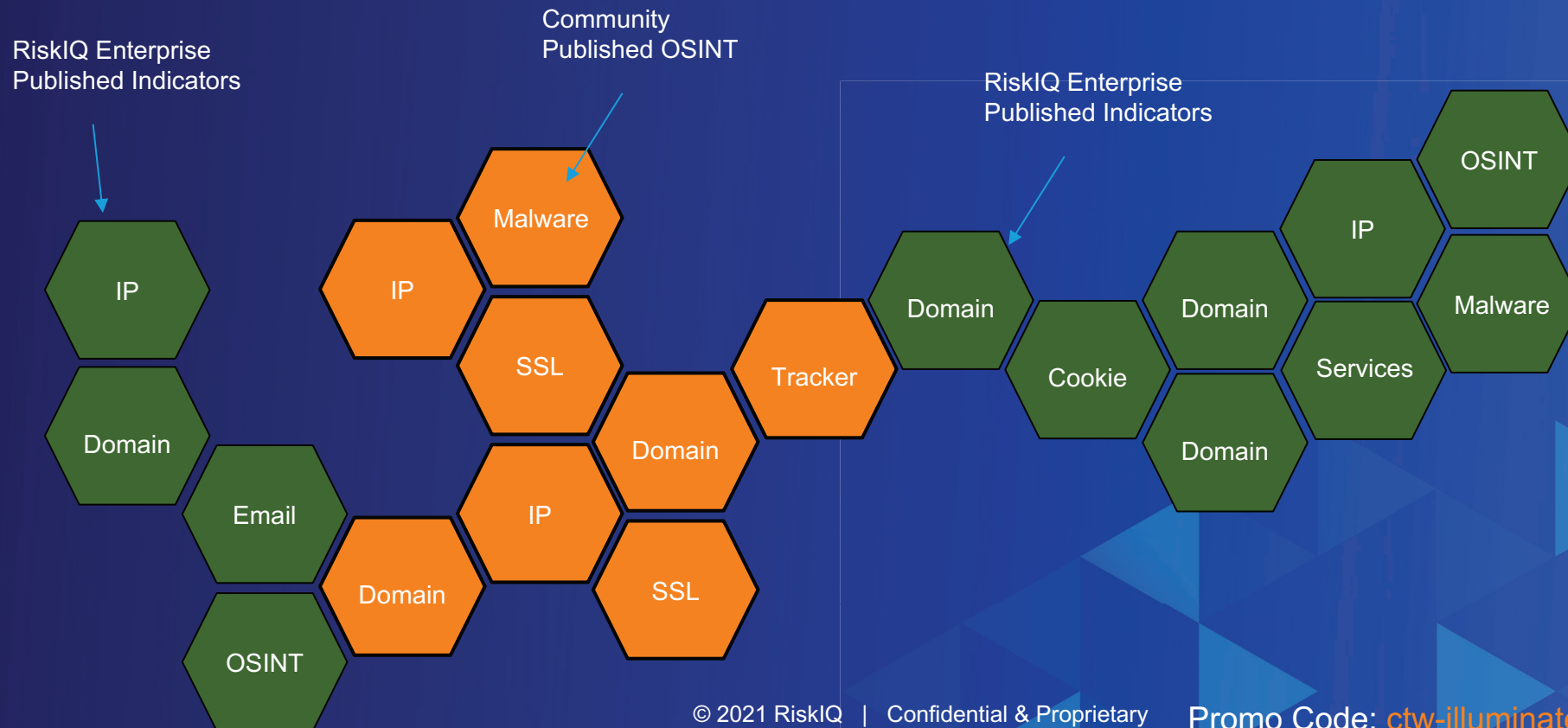
OSINT Investigation

ObliqueRAT



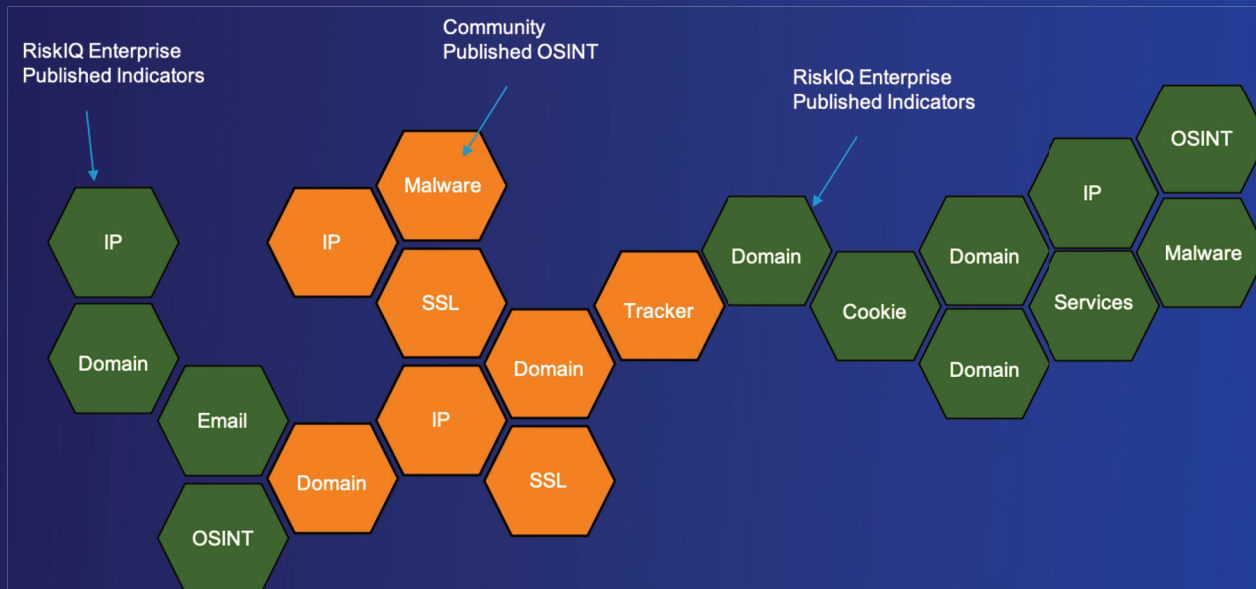
Smarter, Faster Incident Response

Jumpstart Your Investigations & Threat Hunting



Smarter, Faster Incident Response

Jumpstart Your Investigations & Threat Hunting



RISKIQ Illuminate

Search: 185.183.98.182 Search Options

PassiveTotal Intelligence

185.183.98.182 [Details](#)

First Seen	-	NetBlock	185.183.98.0/24	OS	Windows
Last Seen	-	ASN	AS60117 - HS	Hosting Provider	-
Country	NL	Organization	Host Sailor Ltd		

Reputation Malicious (Score: 100)

Severity	Rule	Description
●	RiskIQ Intel Article	ObliqueRAT returns with new campaign using hijacked websites
●	ASN	Infrastructure hosted by this ASN are more likely to be malicious
●	SSL certificate self-signed	Self-signed certificates may indicate malicious behavior
●	Country	Infrastructure hosted in this country are more likely to be malicious

ObliqueRAT OSINT Investigation

With the rise of remote workforces, digital supply chains, and global networks, the time could not be more advantageous for threat actors to create and distribute remote access trojan (RAT) malware.

Scenario:

- A computer in your organization was infected with ObliqueRat malware.
- You are asked to investigate ObliqueRAT OSINT and determine if there is any infrastructure to block or other indicators to help determine find other infected systems.




Initial Query

- <https://community.riskiq.com/article/f6ee031b>

ObliqueRAT OSINT

[Threat Intel Portal](#) / ObliqueRAT returns with new campaign using hijacked websites

- Created about 2 months ago



ObliqueRAT returns with new campaign using hijacked websites

RAT

APT

ObliqueRAT

SecureX

Malware

Talos

Description

Public Indicators (29)

Description

Cisco Talos recently discovered another new campaign distributing the malicious remote access trojan (RAT) ObliqueRAT. In the past, Talos connected ObliqueRAT and another campaign from December 2019 distributing CrimsonRAT. These two malware families share similar maldocs and macros. This new campaign, however, utilizes completely different macro code to download and deploy the ObliqueRAT payload. The attackers have also updated the infection chain to deliver ObliqueRAT via adversary-controlled websites.

Reference URL(s)

1. <http://blog.talosintelligence.com/2021/02/obliquerat-new-campaign.html>

Publication Date




March 02, 2021

Author(s)

Asheer Malhotra

[Threat Intel Portal](#) / ObliqueRAT returns with new campaign using hijacked websites

- Created about 2 months ago



ObliqueRAT returns with new campaign using hijacked websites

RAT

APT

ObliqueRAT

SecureX

Malware

Talos

Description

Public Indicators (29)

URLs (11)

<http://drivestransfer.com/myfiles/dinner%20invitation.doc/win10/dinner%20invitation.doc>
<http://liaonline.in/111.jpg>
<http://liaonline.in/111.png>
<http://liaonline.in/9999.jpg>
<http://liaonline.in/camela.bmp>

[Show 6 more](#)

IP Port Combinations (1)

[185.183.98.182:4701](#)

SHA-256 Hashes (13)

[0196bc9ac3db6f02cfa97323c8fce6cc7318b8f8adb3e73bdf7971b3c541964](#)
[VirusTotal, ANY.RUN, Hybrid Analysis](#)
[0ade4e834f34ed7693ebbe0354c668a6cb9821de581beaf1f3faae08150bd60d](#)
[VirusTotal, ANY.RUN, Hybrid Analysis](#)
[23577ceb59f606ae17d9bdabaccefcb53dc2bac19619ce8a2d3d18ecb84bcad](#)
[VirusTotal, ANY.RUN, Hybrid Analysis](#)
[2ad362e25989b0b1911310345da90473df9053190737c456494b0c26613c8d1f](#)
[VirusTotal, ANY.RUN, Hybrid Analysis](#)
[47bed59051a727911b050c2922874ae817e05860e4eee83b323f9feab710bf5c](#)
[VirusTotal, ANY.RUN, Hybrid Analysis](#)

[Show 8 more](#)

Domains (3)

[larsentobro.com](#)
[microsoft.ddns.net](#)
[yepp.ddns.net](#)

IPs (1)

[185.183.98.182](#)

<https://community.riskiq.com/article/f6ee031b>

Scaling Investigations with RiskIQ API and Reputation Scoring

- Now that you have determined a way to find additional related infrastructure.
- You can now create a script to utilize a repeatable way to perform the investigation at scale.
- From a single indicator 185.183.98[.]12 how many IP addresses and domains can you we find together?
- How do you determine good from bad?

ObliqueRAT Script to find additional Infrastructure

1 IP address



90

IP addresses

3 Domains



583

Domains

Jupyter ObliqueRat-Reputation Last Checkpoint: 03/09/2021 (unsaved changes) Logout

File Edit View Insert Cell Kernel Widgets Help Trusted Python 3

OBLIQUERAT Cisco OSINT Article
<https://community.riskiq.com/article/6ee031b/indicators>

Cisco Talos recently discovered another new campaign distributing the malicious remote access trojan (RAT) ObliqueRAT. In the past, Talos connected ObliqueRAT and another campaign from December 2019 distributing CrimsonRAT. These two malware families share similar maldocs and macros. This new campaign, however, utilizes completely different macro code to download and deploy the ObliqueRAT payload. The attackers have also updated the infection chain to deliver ObliqueRAT via adversary-controlled websites.

IOC IP 185.183.98.182
Notebook created by Benjamin Powell and Mark Kendrick

1. Setup Python Environment

```
In [1]: import requests
import auth

creds = (auth.API_USERNAME, auth.API_KEY)
other_requests_args = {
    'verify': True,
    'proxies': [],
}
```

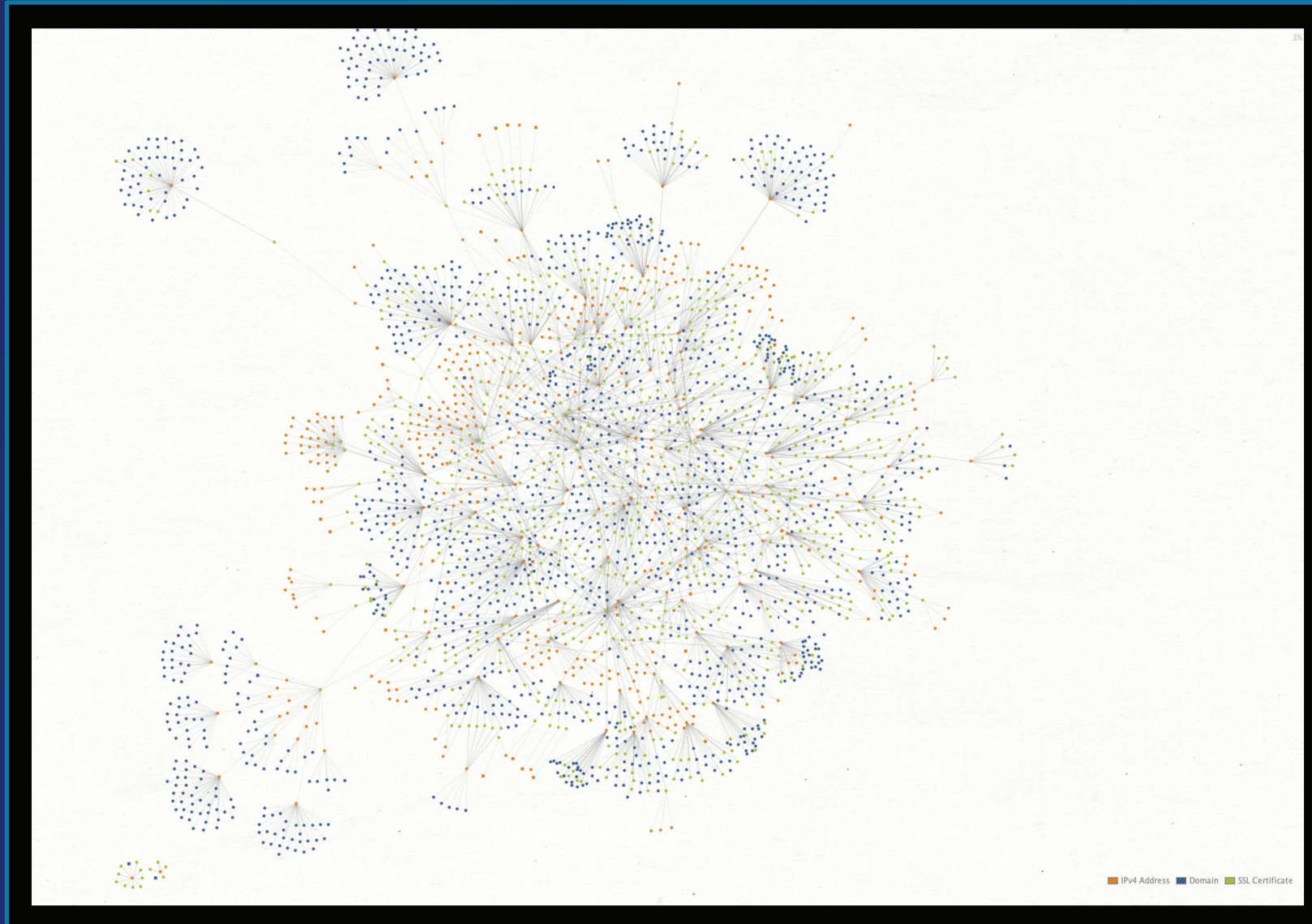
2. Talos OSINT Article initial IP address

```
In [2]: anchorip = '185.183.98.182'
date_start = '2020-11-16'
```

3. Find all SSL certs on single IP

```
In [3]: ip_query = {
    'query': anchorip,
    'start': date_start,
}
ip_response = requests.get(
    'https://api.passivetotal.org/v2/ssl-certificate/history',
    auth=creds,
    params=ip_query,
    **other_requests_args
)
ips = ip_response.json()
ips
```

Map of ObliqueRAT from our example



Always Anticipating Question from the CISO'S

- Are we at risk, or compromised?
- What about the partners we depend upon for our business?
 - Are they at risk or compromised?
- How can we be proactive to stop threat actors their infrastructure and tools?

Querypack[.]com Remote Connection To Internal System

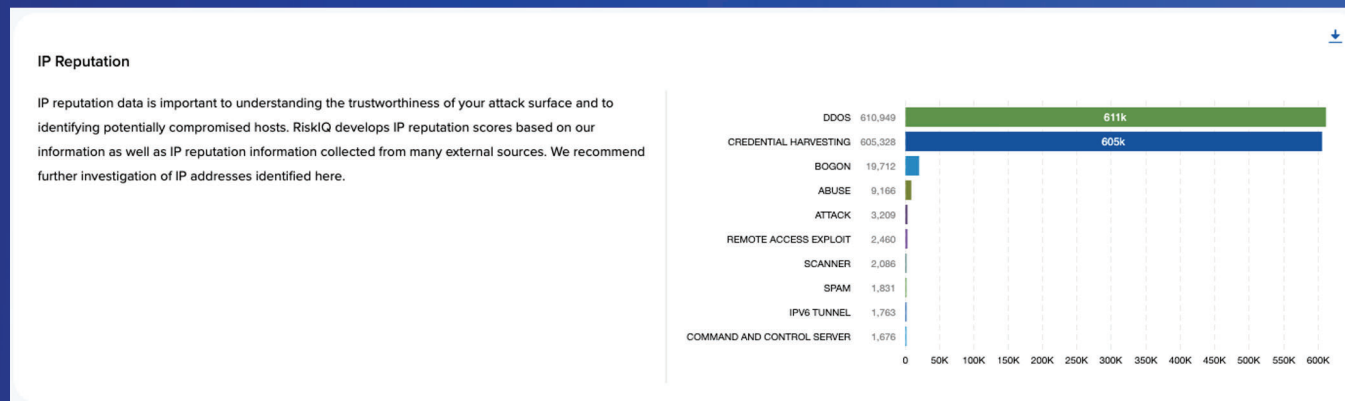
Scenario

- Windows Computer was remotely connected to a system outside the USA where you do not do business
- You have been asked to investigate and determine if that connection was legitimate or a potential compromise.

Initial Query:

- <https://transparencyreport.google.com/safe-browsing/search?hl=en>
- <https://community.riskiq.com/research?query=querypack.com>

Querypack[.]com Summary



- Domain is malicious
- IP address had Port 3389 open for Windows Remote Access
- The Self signed SSL certificate created by windows computer WIN-OQJUIMC71B6
- The unique SSL Certificate was found on 100 different IP addresses
- The domain has been identified with the Threat Actor APT33
- Threat Infrastructure was connected to Teleperformace SE attack surface in Germany
 - <https://community.riskiq.com/attack-surfaces/46004>

RiskIQ Illuminate Start Your Trial Today

The screenshot shows the RiskIQ Illuminate landing page. At the top, the RiskIQ logo is on the left, and navigation links for 'Illuminate', a gear icon, a shield icon, and a user icon are on the right. Below the header, a breadcrumb trail reads 'Home / Learn More'. The main heading is 'INTRODUCING RiskIQ Illuminate', followed by the tagline 'Intelligent, quick, and actionable Attack Surface Management built on top of our premiere Threat Investigation platform.' A horizontal menu contains 'Enterprise', 'Illuminate' (which is underlined), 'CTI', 'SecOps', and 'Third-Party'. The 'Illuminate Overview' section is highlighted in the left sidebar. The main content area describes RiskIQ Illuminate as a security intelligence platform that combines attack surface insights with adversary indicators. To the right, under the 'Try It' heading, are three buttons: 'Activate Illuminate Trial' (orange), 'Workshops' (grey), and 'Talk to an Expert' (grey). Below this is a video player titled 'RiskIQ Illuminate Threat Intelligence...' with 'Watch later' and 'Share' buttons. The video thumbnail shows the RiskIQ logo and the word 'Illuminate' with a play button. At the bottom right of the page is a blue chat bubble icon.

<https://community.riskiq.com/learn-more/illuminate>

RiskIQ Illuminate® Internet Intelligence Platform



RISKIQ®

Security Intelligence for Your Interconnected World

<https://community.riskiq.com/learn-more/illuminate>