Executive Protection

5 ways Navigator can safeguard your VIPs

At LifeRaft, we know from talking with customers that executive protection has become a bigger part of their jobs.

Safeguarding VIPs once meant hiring a few burly guys. But in today's landscape, more threats originate online and require a larger security posture. Executive protection now involves preventing doxing and data leaks, combating misinformation and rumors, as well as investigating violent threats on social media. All of which creates a big headache for you.

Security teams spend more time than ever trolling through web pages and social media feeds. It feels impossible to spot one nugget of important data when you're searching across the entire internet.

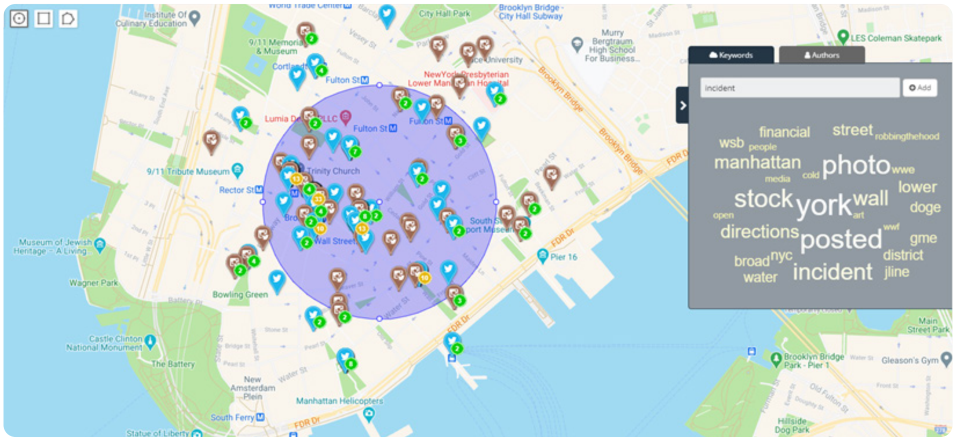
Well, not necessarily impossible. Navigator eliminates the need to manually scroll through feeds to spot threats online. The software monitors the internet 24/7 and sends out automated alerts when triggered. This saves your team time and resources when you need to act fast.

Of course, no single platform offers a total solution. As a best practice, every company should mix and match tools to address their challenges.

But threat intelligence software can represent a valuable addition to your team's toolkit, especially when it comes to executive protection.

We've highlighted five ways Navigator can help protect your organization's VIPs.

1. TRAVEL RISK



Navigator's geofence feature highlighting recent social media activity in Lower Manhattan.

Executives face many threats on the road: natural disasters, terrorist attacks, riots, looting, political turmoil, criminal activity, etc.

Travel advisories, however, often lack context. And events can take time to hit media outlets.

Navigator offers several features to obtain situational awareness with VIPs on the go. Users can watch multiple social media sites for a sense of existing threats. Real-time alerts also allow your team to quickly understand and respond to emerging events.

Navigator's geofencing tool, specifically, represents a useful feature in such situations. Geofencing allows users to draw a virtual border around a location, say a city, travel route, or conference venue. The software will then monitor and report any nearby activity on social media.

Such feeds can present useful intelligence.

Your security team can begin assessing and mitigating risks before your personnel arrive in an area. Alternatively, you could set up a geofence around an executive's position, watching out for emerging threats.

2. VIOLENT THREATS

> Executives have to make important, often controversial decisions. And people out there may not like what they do or who they align with. For that reason, it's not uncommon for high-profile CEOs to receive violent threats online.

Most threats come from individuals simply venting their frustrations. These aptly named "keyboard warriors" don't often present much of a risk.

But other threats made online represent a more serious problem. For example, security teams may uncover a group conversation with details of a planned attack. Alternatively, you may stumble upon individuals with a long history of posting threats against your organization.

In both cases, you can mitigate risk by identifying threats quickly. Any actionable intelligence can allow your team to beef up defensive measures to safeguard your VIP.

Security teams have a number of ways to exploit open-source intelligence tools like Navigator in such situations. One example being targeted queries. For example, you can scan the web for key phrases like 'kill', 'shoot', or 'injure' alongside the names of your organization and executives. Automated alerts can then notify your team by email or desktop almost as soon as threats get posted.

That means a faster response time to credible threats. It also reduces the chances of overlooking real risks altogether.

Secondly, Navigator allows your team to investigate the backgrounds of potential threat actors.

The platform's "People Search" function can return addresses, usernames, social profiles, affiliated organizations, education, websites, and third-party public records. All of which could be valuable intel when trying to determine the severity of a threat.

Finally, you can use Navigator to monitor threat actors and gather valuable intelligence for further investigation.

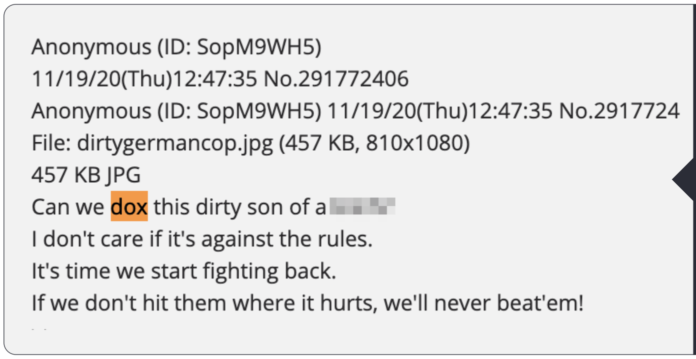
3. DOXING

> Doxing is the practice of revealing an individual's personal information online without their consent.

The kind of information revealed could include passwords, addresses, passport details, medical information, bank records, and social insurance numbers. And it represents an effective way to intimidate or humiliate victims.

Doxings also expose an executive to other threats.

For instance, bad actors could use information gleaned from a leak to harass family members. Alternatively, criminals might exploit clues from a doxing for spear-phishing campaigns or hack other accounts owned by the executive.



Anonymous (ID: SopM9WH5)
11/19/20(Thu)12:47:35 No.291772406
Anonymous (ID: SopM9WH5) 11/19/20(Thu)12:47:35 No.2917724
File: dirtygermancop.jpg (457 KB, 810x1080)
457 KB JPG
Can we dox this dirty son of a [redacted]
I don't care if it's against the rules.
It's time we start fighting back.
If we don't hit them where it hurts, we'll never beat'em!

An example of a doxing request discovered using Navigator on the dark web

In such situations, speed plays a crucial factor. Unfortunately, doxed content rarely shows up in a Google search. So security teams must monitor a wide variety of websites — sometimes on parts of the internet you'd rather not visit.

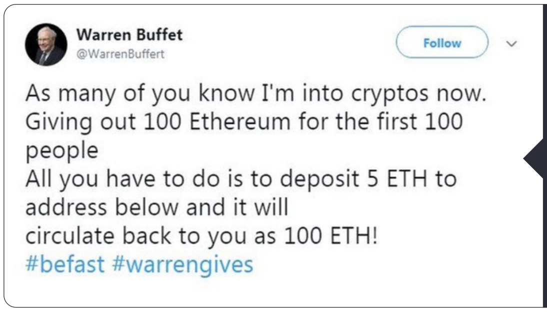
Navigator's Deep and Dark Web search function can be quite helpful for such situations.

You can enter in the names of your company's executives, board members, or other VIPs. Navigator will then scan online pages, specifically those that are usually poorly indexed by traditional search engines like forums, paste sites, darknet web rings, etc.

If attackers have leaked any personal information online, it will likely get picked up in query results.

4. MISINFORMATION

Malicious individuals have many reasons for spreading fake or misleading information online.



Warren Buffet
@WarrenBuffert

As many of you know I'm into cryptos now.
Giving out 100 Ethereum for the first 100 people
All you have to do is to deposit 5 ETH to address below and it will
circulate back to you as 100 ETH!
#befast #warrengives

Cybercriminals impersonating a high-profile executive on Twitter. Note the username: @WarrenBuffert

It could be to forward a political agenda. Criminals may borrow on an executive's reputation to scam unsuspecting members of the public.

State governments could see undermining western businesses, and the executives that work for them, as part of a broader plan to promote their national interests.

Furthermore, disinformation attacks are relatively cheap. In some cases, a well-orchestrated campaign can cost less than a few hundred dollars. Yet threat actors, if successful, can inflict tremendous damage on their targets.

Of course, misinformation can circulate online as part of normal gossip. Most people connected to the internet. So it doesn't take long for a false rumor to spread.

Regardless of why misinformation proliferates, the results are the same. Rumors, if left unchecked, can damage an executive's reputation. It can also impair your organization's credibility.

Navigator allows security teams to monitor the web for misleading content.

The platform aggregates dozens of social media feeds. Analysts can also collect data from poorly indexed deep web sources, like forums and paste sites.

This minimizes the chances of overlooking critical information and reduces the time spent manually searching for content.

Email alerts also give your team a chance to take down or respond to misinformation before it goes viral. An early heads up could provide valuable hours or days for your communications group to plot a public relations strategy.

5. DISRUPTIVE EVENTS

Disruptive events often present a safety problem for your executives and other employees. This could include an unsanctioned event planned at a company office, factory, or worksite.

Alternatively, nearby civil unrest, criminal activity, natural disasters, or other events could jeopardize the safety of personnel.

This has become an even bigger headache during COVID-19. More employees now work from home. Security teams may now need to monitor, not only a company office or worksite, but also an executive's home residence.

Any information regarding individuals or groups looking to cause problems can pay dividends in such situations. Investigation tools like Navigator allow you to take appropriate precautions and better deploy defensive measures.

That could prevent a threat from escalating. Or in the best-case scenario, allow your team to sidestep a bad situation altogether.

> VIPs today face a growing number of threats — both physical and virtual. For that reason, we can't ignore the digital side of physical security. And given the sheer volume of content online, corporate security teams can also no longer rely solely on manual searches through Google, media outlets, and other websites.

VISIT OUR WEBSITE
LIFERAFTINC.COM

WATCH OUR VIDEO
LIFERAFTINC.COM/VIDEO

GET IN TOUCH
INFO@LIFERAFTINC.COM