ONTIC + TORCHSTONE

The Role of Baseline Threat Assessments in Protective Intelligence

Fred Burton - Executive Director, Center for Protective Intelligence, Ontic
Scott Stewart - Vice President, TorchStone Global

As their name suggests, baseline threat assessments are foundational tools protective intelligence teams use to establish the threat posed to a specific person, company, event or facility. Baseline threat assessments are conducted to create as complete a picture as possible of the existing threat level, and will typically examine factors that could bring hostile attention to the subject, any currently known threats, the universe of potential threats and threat actors, as well as the subject's general threat environment.

By identifying, analyzing and describing the existing threat level, baseline threat assessments are useful tools for determining what security measures are appropriate to protect against the identified or potential threats. Any security measures must also be implemented in accordance with corporate or personal risk tolerance as well as lifestyle, corporate culture, business operations and budgetary considerations.

It is important to recognize that while baseline threat assessments provide a foundational understanding of the threat, they are not static. Baseline assessments must be responsive, living documents that reflect changes in the potential target's situation and environment. In the absence of major incidents that would trigger a re-assessment, we suggest scheduled periodic reviews and re-assessments that can account for smaller cumulative changes that happen over time. Based on our experiences, a good rule-of-thumb has been that baseline updates should be conducted quarterly, with full, ground-up re-assessments annually.

Another caveat is that baseline assessments are not just useful to gauge the threats facing CEOs and other top-level leadership; they are also useful to assess the threat posed to a country manager in a dangerous location, or even a lower level employee who has been threatened.

Baseline assessments must be responsive, living documents that reflect changes in the potential target's situation and environment.

Elements of a Baseline Threat Assessment

Now that we've defined the baseline threat assessment, let's examine the elements that go into it. We are going to frame our discussion of the elements with a person as the subject, but these same criteria can also be applied to a company, event or facility.

Subject Profile

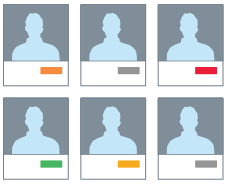
The first element to examine is the subject's public profile. High profile personalities are far more likely to attract the attention of threat actors and are more easily recognized as they proceed through their normal daily activities. Large numbers of fans and admirers increase the probability of unstable individuals developing an unhealthy focus of interest in the subject. Obviously large numbers of detractors and critics also increase the possibility of negative attention and hostile action being directed toward the subject, especially if the subject is featured in conspiracy theories or portrayed negatively in social media.

The subject's business dealings can also draw untoward attention, especially if they work for or are on the board of a company or in an industry that is controversial. Investments in contentious companies or technologies can also trigger such activity, as can the acquisition of a company that is a lightning rod attracting negative attention.

Social activities such as providing support to controversial organizations or even participating in high-profile meetings such as Bilderburg or the World Economic Forum can also be expected to draw adverse interest.

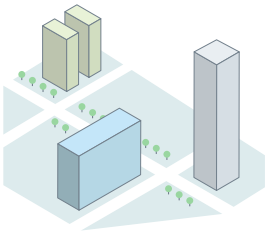
While examining the subject's profile, it is also helpful to conduct a thorough cyber survey to determine what open-source information is available about the subject. If such a study is conducted from the perspective of a potential attacker, it can allow the assessment team to determine what information is available that could be useful in planning an attack. But more importantly it can also be used to identify information gaps. These gaps are missing items of information that would be required to plan an attack and that a potential attacker would have to obtain physically through surveillance. These information gaps can then be used to help direct surveillance detection efforts. Suggestions on how to remove sensitive information from the Internet and to limit such future postings may also be provided.

The profiles of various family members should also be considered as part of the baseline, as they can reveal vulnerabilities or draw unwarranted attention to the subject through controversial activities or by releasing private information such as vacation pictures, residences or private aircraft on social media platforms.



Documented and Potential Threats

Known and documented threats also play an important role in the baseline threat assessment. Such threats should include persons of interest (POIs) such as abnormally angry customers, disgruntled former employees, unstable individuals who have an abnormal focus of interest in the subject, etc. The communications of such individuals should be monitored and databased for future reference. When we talk about the need for the baseline assessment to be a living document, one of the factors that can drive the need for a re-assessment is when a POI provides indications in their correspondence that they are moving along a pathway to violence. Such indicators may include grievances against a subject for not acknowledging or returning affection or when a person with a grievance begins to exhibit violent ideation. Other threats could include mentions of the subject in terrorist propaganda or on social media forums frequented by extremists or activist groups as well as activist campaigns targeting the subject, the subject's company, or against other companies in the same sector.



Physical Environment

It is also important to assess the subject's work and home environment, where the company operates, and areas that must be regularly traversed to get from home to work or are otherwise frequented. It is important to gain an understanding of the criminal, civil and natural disaster threats and vulnerabilities associated with those locations. In some cities, employees may live in relatively safe residential neighborhoods, but then work in facilities in more dangerous parts of the city, or must pass through more dangerous neighborhoods to get from the residence to an office in the city center.

In addition to analyzing the overall environment it is also useful to conduct a detailed analysis of the routes that are taken at predictable times to predictable places, where it is possible for a threat actor to establish the subject's behavior patterns that could allow them to identify and select an attack site. One of the most frequently exploited patterns has been the morning home to work commute since it tends to be the most predictable daily move for most potential targets. However, any regularly scheduled movement to or from religious services or gyms or other known locations can be exploited and should therefore be analyzed. Chokepoints, and possible attack sites should be identified, and extra security attention can be placed on those spots to look for hostile surveillance operating in there.

Current Security Measures

Current security programs and measures should also be part of the baseline assessment. This would include security training provided to the subject, a driver or a protective detail. This should also account for residential security, estate staff and physical security measures in place at the office. The security measures in place can then be weighed against the assessed threat level to determine if they are sufficient and appropriate.

About Us

Ontic is the first protective intelligence software company to digitally transform how Fortune 500 and emerging enterprises proactively address physical threat management to protect employees, customers and assets. Ontic's SaaS-based platform collects and connects threat indicators to provide a comprehensive view of potential threats while surfacing critical knowledge to maintain business continuity and reduce financial impact.

Learn more about the platform here:
www.ontic.co/product

ONTIC

TorchStone is in the Business of Before. We have assembled a team of world-class, highly experienced protective intelligence practitioners that includes investigators, analysts and psychologists.

We can either serve as your organization's PI team or come alongside to support and supplement the efforts of your existing PI team.

Please contact us for more information about our PI practice at: www.torchstoneglobal.com

TORCHSTONE