

The CyberMenas Special Intelligence Unit (SIU) provides a highly skilled, experienced team which can conduct web-based searches, investigations and analysis quickly, efficiently and with the highest level of discretion.

Our Special Intelligence Unit works in conjunction with your own security and investigative staff to expand the breadth and depth of any assessment using our vast database of open source intelligence and threat actors, along with customized research and in-depth analysis from our team of security experts.

Our analysts are experts in the fields of cyber intelligence, intelligence studies and behavioral science, and they apply their cultural and foreign language skills to help you understand threats across the globe.

**Features and Benefits**

- **Expert Analysts** – Our staff has experience handling a wide array of security issues, including physical and digital threats.
- **Investigative Specialists** – We know how to find information quickly and efficiently.
- **Depth and Breadth of Coverage** – We provide broader, deeper visibility into potential threats and deep-dive analysis of threat actors.
- **Cost-Effective Services** – Eliminate the need for in-house staff to spend valuable time on manual reviews of thousands of websites and social media platforms.
- **Better Information** – Identify potential vulnerabilities found online in order to help internal stakeholders better understand potential dangers facing executives and their families.
- **Focus on the Core Business** – Our clients can focus on their core business processes while delegating time-consuming processes to experienced SIU analysts.

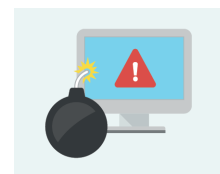
Our analysts apply their cultural and foreign language skills to help you understand threats across the globe.



We monitor for any disruptive activities - such as demonstrations and protests – that may be planned for a specific event.



Our staff has experience handling a wide array of security issues, including physical and digital threats.



**External Threats**

Event Monitoring –

We monitor for any disruptive activities - such as demonstrations and protests – that may be planned for a specific event.

These events may be as small as a shareholders’ meeting or as large as the Olympics or the UN General Assembly.

**Adversarial Groups** - We can focus on a specific adversary, such as a particular activist group and provide a report about the group, their targets, previous activities and preferred attack methods.

**Threat Actors** - We assist in collecting and reporting information on alleged fraudsters, hackers, credit card/identity thieves or other criminals you may be building a case against.

**Adversarial Groups** - Our Executive Threat Assessments provide an in-depth review of how vulnerable executives are based on their exposure on the Internet. We can also provide this service for an organization.

**Internal Threats**

**Threats against Executives or Employees** - When a company’s security team is alerted to threats – such as death threats or a suspicious package – the SIU team delivers an intelligence profile about the possible sender.

**Insider Threats** - We search for information regarding violence in the workplace, alleged corporate espionage, violations and other insider threats.

**Post-incident Monitoring** - After a negative event or incident has occurred, we can monitor for any lingering effects or issues. Incidents may include layoffs or other internal changes within a company, or an event such as a bomb threat.

**Fraud and Legal Issues**

**Due Diligence on Potential Mergers and Acquisitions** - For potential mergers and acquisitions, we look for any legal actions, criminal actions, accusations of fraud, affiliations with vendors, investors and related issues for the target company, its executives and board.

**Black Market or Grey Market Products** - We can report on a particular product or class of products that are being sold on the black market or that may be counterfeit goods.

**Lawsuits** - If you are being sued by either another company or an individual, we can collect information on the opposition.

**Geopolitical Intelligence Country Assessments** - If you are planning or evaluating whether to open an office in a new location, we can assess the target geographic area. Intelligence collected may include which other businesses operate in that country, crime rates, political issues, potential threats to employees and more.

L'Unité d'Intelligence Spéciale CyberMenas (SIU) dispose d'une équipe hautement qualifiée et expérimentée qui peut mener des recherches, des enquêtes et des analyses sur le Web rapidement, efficacement et avec le plus haut niveau de discrétion.

Notre unité de renseignement spécial travaille en collaboration avec votre propre équipe de sécurité et d'enquête pour élargir et approfondir votre évaluation en utilisant notre vaste base de données d'acteurs de menace, ainsi que des analyses personnalisées et approfondies de notre équipe d'experts en sécurité.

Nos analystes sont des experts dans les domaines de l'intelligence informatique, des études de renseignement et des sciences du comportement, et ils appliquent leurs compétences linguistiques et culturelles pour vous aider à comprendre les menaces à travers le monde.

**Caractéristiques et avantages**

- **Analystes experts** - Notre personnel a de l'expérience dans la gestion d'un large éventail de problèmes de sécurité, y compris les menaces physiques et numériques.
- **Spécialistes d'enquête** - Nous savons comment trouver l'information rapidement et efficacement.
- **Profondeur et étendue de la couverture** - Nous fournissons une visibilité plus large et plus profonde sur les menaces potentielles et l'analyse approfondie des acteurs de menace.
- **Services rentables** - Éliminez le besoin pour le personnel interne de passer un temps précieux sur les examens manuels de milliers de sites Web et de plateformes de réseaux sociaux.
- **Meilleure information** - Identifier les vulnérabilités potentielles trouvées en ligne afin d'aider les parties prenantes internes à mieux comprendre les dangers potentiels auxquels sont confrontés les cadres et leurs familles.
- **Se concentrer sur votre business** - Nos clients peuvent se concentrer sur leurs processus interne tout en déléguant des processus fastidieux à des SIU analystes expérimentés.

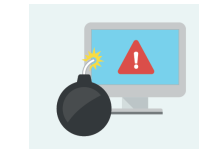
Nos analystes appliquent leurs compétences linguistiques et culturelles pour vous aider à comprendre les menaces à travers le monde.



Nous surveillons les activités perturbatrices telles que les manifestations et les protestations qui peuvent être planifiées pour un événement spécifique



Notre personnel a de l'expérience dans la gestion d'un large éventail de problèmes de sécurité, y compris les menaces physiques et numériques.



**Menaces externes**

Surveillance des événements -

Nous surveillons les activités perturbatrices - telles que les manifestations et les protestations qui peuvent être planifiées pour un événement spécifique. Ces événements peuvent être aussi petits qu'une réunion des actionnaires ou aussi importants que les Jeux olympiques ou l'Assemblée générale des Nations Unies.

**Groupes adverses** – Nous pouvons nous concentrer sur un adversaire spécifique, tel qu'un groupe d'activistes particulier, et fournir un rapport sur le groupe, ses cibles, ses activités précédentes et ses méthodes d'attaque préférées.

**Acteurs de menace** - Nous aidons à recueillir et rapporter des informations sur les présumés fraudeurs, les pirates informatiques, les voleurs de cartes de crédit / d'identité ou d'autres criminels contre lesquels vous pourriez constituer un cas judiciaire.

**Groupes d'adversaires** - Nos rapports de menaces sur les officielles fournissent un examen approfondi de la vulnérabilité des officielles en fonction de leur exposition sur l' Internet. Nous pouvons également fournir ce service pour une organisation.

**Menaces internes**

**Menaces contre des cadres ou des employés** - Lorsque l'équipe de sécurité d'une entreprise est alertée de menaces - telles que des menaces de mort ou un colis suspect - l'équipe du SIU délivre un profil de renseignement sur l'expéditeur éventuel.

**Menaces en Interne** - Nous recherchons des informations concernant la violence sur le lieu de travail, l'espionnage présumé d'entreprise, les violations et d'autres menaces internes.

**Surveillance post-incident** - Après un événement ou un incident négatif s'est produite, nous pouvons surveiller tout effet ou problème persistant. Les incidents peuvent inclure des licenciements ou d'autres changements internes au sein d'une entreprise, ou un événement tel qu'une alerte à la bombe.

**Fraude et questions juridiques**

**Due Diligence sur les Fusions et Acquisitions potentielles** - Pour les fusions et acquisitions potentielles, nous recherchons toute action en justice, action pénale, accusation de fraude, affiliation avec des fournisseurs, investisseurs et questions complexe pour la société cible, ses dirigeants et son conseil d'administration.

**Produits du marché noir ou du marché gris** - Nous pouvons établir un rapport sur un produit ou une catégorie particulière de produits qui sont vendus sur le marché noir et qui peuvent être des produits contrefaits.

**Procès** - Si vous êtes poursuivi par une autre société ou un individu, nous pouvons collecter des informations sur l'opposition.

**Évaluations géopolitiques par pays** - Si vous planifiez ou évaluez l'ouverture d'un bureau dans un nouvel emplacement, nous pouvons évaluer la zone géographique cible. Les renseignements collectés peuvent inclure les autres entreprises présentes dans ce pays, les taux de criminalité, les problèmes politiques, les menaces potentielles pour les employés et plus encore.