

SERVICES TO PROTECT THE PLAYER

ACHILLES RISK PROFILE

We conduct an **"Achilles Risk Profile"** of new recruits and current players to identify any prior social media posting or connections that might raise press or public concern, and hurt the brand of the player, team, or league. We then work with the player, team, or agency to remove it or craft a crisis response program ready to execute if something were to happen.

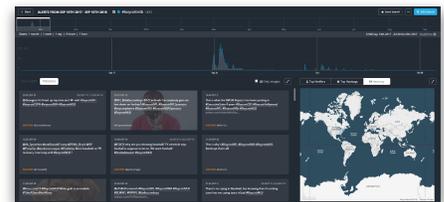
- ◆ Ability to remove all traces from Twitter, Facebook, Google, YouTube, Tumblr, and SnapChat
- ◆ Military trained analysts and insider abuse teams use uniquely tailored tools to identify risk creating content
- ◆ Identify risks within social connections
- ◆ Access to Twitter's "firehose"



ACHILLES AWARENESS MONITORING

Players are increasingly active on social media and we can put a player or recruit on what we call **"Achilles Awareness Monitoring"** to identify postings that may potentially hurt the brand of the player, team, or league. We can monitor in real-time and alert on a need to know basis.

- ◆ Monitoring covers any social media site including Twitter, Facebook, Instagram, YouTube, Tumblr, SnapChat, and the Dark Web
- ◆ Ability to search and analyze Twitter's private "firehose" of Tweets for the past year, so we can find tweets by adversaries as well
- ◆ Geo-fence online monitoring to gain situational awareness of issues
- ◆ Capable of monitoring full rosters of players 24/7/365, based on client needs
- ◆ Collect and decipher 3,200 Tweets per player at any time



SERVICES TO PROTECT THE PLAYER

INVESTIGATIVE INTELLIGENCE & RESPONSE

Players and their families are common targets of cyberstalking, harassment, persistent threats, identity theft, revenge porn, or other crimes. We conduct a full intelligence led investigation to identify the culprits and provide a plan of action that involves our former Navy SEAL team diffusing the issue, or bringing the matter to law enforcement or legal. We can also place the player and family on a 24/7/365 online threat watch to act quickly in case of potential threats even when the player is on the road.

- ◆ Identify perpetrators using highly skilled cyber security experts & ex-military cyber intel analysts
- ◆ Actionable reports for law enforcement or legal teams
- ◆ Direct access to law enforcement officials
- ◆ Threat watch gives us situational awareness to diffuse brewing issues
- ◆ Ability to get exploitative content taken down
- ◆ Ability to deploy former SEAL's to respond to critical threats

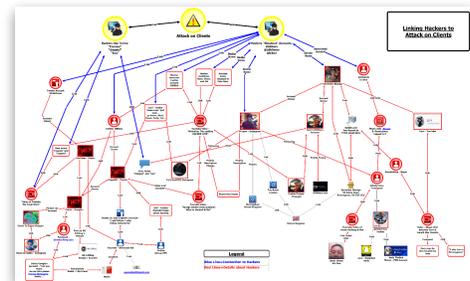


TRAINING & AWARENESS RAISING

Since players are now in the limelight more than ever, we can provide training to players, coaches, and staff on how to safely use social media.

Training and Awareness Raising covers:

- ◆ Training on how to use social media safely
- ◆ Awareness of common scams used by hackers to get access to player's accounts and exploit them
- ◆ Showcasing with examples how trained hackers can put pieces together to attack a player



SSP Blue's team of cyber security experts has worked with the NFL, NBA and high profile talent on investigative intelligence and online protection. Founded by Hemu Nigam, former chief security and privacy officer of News Corporation, Fox, and MySpace, who oversaw globally 40+ digital properties including FoxSports.com, AmericanIdol.com, and MySpace.com, and had teams on the ground in EMEA, APAC, SAPAC, and LatAm. As a former federal prosecutor against online crimes, he knows the ins and outs of how to identify and respond to online threats and brand-impairing posts. Hemu has held top secret clearance in both the public and private sectors. Our team consists of top secret cleared, ex-military online counter-intelligence officers who have served in active combat in several of the armed services, prior to joining us. Our team can engage in threat matrix creation as well as counter-social media strategies to negate the impact of exploitative social media issues. Given this expertise, we have authorized access to specialized investigative intelligence tools that are not available to the general public.