Service Description

Cyber Threat Analysis

"The Philippine Eagle feeds on flying lemurs, squirrels, civets, snakes, hornbills, bats and monkeys. It was previously known as the Monkey-Eating Eagle."

Predator Behavior

The cyber-threat analysis assesses 6 threat actors and their associated motives and behavioral traits so that we can identify the probability of them targeting your organization - Who is going to attack?

The assessment can be integrated with our predator-prey platform and the resultant dashboard succinctly identifies an organization's high-risk behavior. Platform outputs can be used to influence and inform Enterprise Risk Management, Budget and Strategy.

Threat Actors

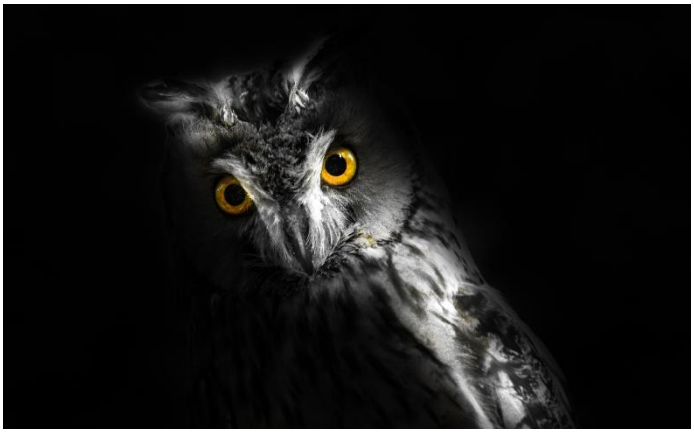
1. Opportunists
2. Nation States
3. Organized Criminal Groups
4. Corporate Competitors
5. Company Insiders
6. Hacktivists

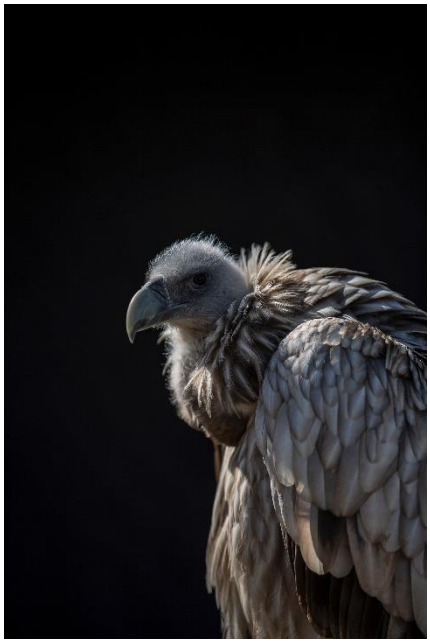
Deep Analytics

We use artificial intelligence to identify current and evolving actor motivations and attack techniques – searching billions of records - to understand who will target individual organizations.

Opportunists

Usually amateur hackers and often seeking notoriety. They will use widely available attack techniques. Our algorithms review a large number and variety of public and private information sources to understand their motivations for attacking individual organizations. Not an advanced adversary but troublesome if you're their target – something we'll advise on.





Nation States

Sophisticated, targeted attacks and deep financial resources. Motivations can be fluid in alignment with political, economic, technological or military agendas. That combined with industrial espionage and business destruction make this an adversary to be dissuaded at the earliest opportunity.

Organized Criminal Groups

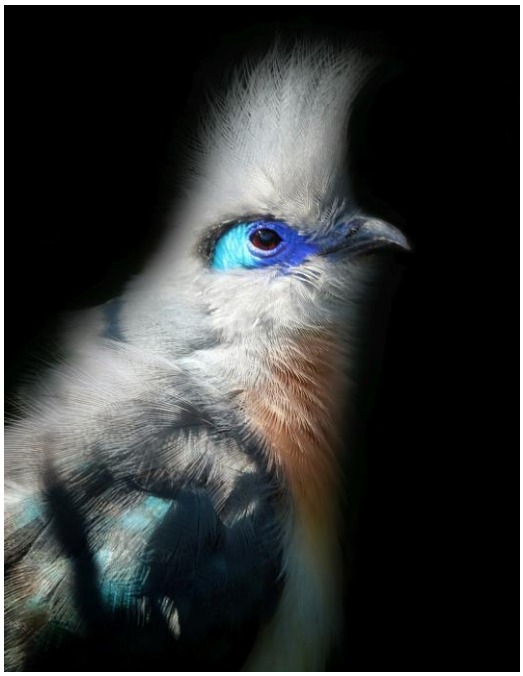
Sometimes individual but often a collective. Motivated to conduct targeted attacks for financial gain. They could sell stolen information or cause disruption and seek ransom. An intermediate adversary. Our algorithms identify counterbalancing behavior.

Corporate Competitors

Competitor organizations many of which are backed by nation states! Their goal is to obtain intellectual property including financial, strategic and workforce information. A sophisticated adversary performing highly targeted attacks. Forewarned is forearmed!

Company Insiders

Usually disgruntled or ex-employees motivated by revenge or financial gain. A difficult adversary when working with external actors as they can bypass the most robust defenses. Our algorithms identify their motivations, attack techniques and behavioral patterns!



Hacktivists

Can be individuals or organized groups around the World. They will normally use widely available attack techniques. Their aim is often a high-profile attack to damage the reputation and credibility of their opponents for ideological reasons. Our proprietary algorithms are designed to identify if an individual organization is one of their current or emergent targets.

The cyber-threat analysis is available in basic, standard or advanced options with results made available in 7, 14 and 28 days respectively. Basic is a threat-actor behavioral snapshot, standard adds in-depth analysis of the six actors and advanced includes behavioral recommendations.

Who is going to attack?

Identifying an organization's high-risk behavior relative to the threat actors is a key element to understanding risk.

Features	Basic	Standard	Advanced
Opportunists Nation States Organized Criminal Groups Corporate Competitors Company Insiders Hacktivists	✓	✓	✓
Threat Actor Behavioral Snapshot	✓	✓	✓
In-Depth Threat Actor Analysis	X	✓	✓
Behavioral Recommendations	X	X	✓

Each assessment includes a summary rating within the scale of 1 to 5 and a red-amber-green dashboard display.

Defense		
Threat Analysis		
1	3	5

Predator-Prey Platform

The resultant summary rating can be used within the predator-prey platform to influence and inform Enterprise Risk Management, Budget and Strategy.