Service Description

Cyber Attack Assessment

"A lion cub starts to eat meat at three months. They begin to hunt for themselves at one year of age."

Predator Behavior

The cyber-attack assessment analyzes 4 domains of public information to identify behavioral traits that make an organization susceptible 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.

Behavioral Domains

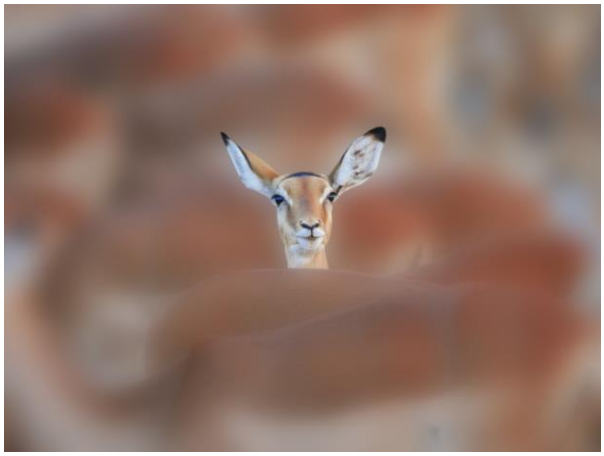
1. Organization Attitude
2. Technology Visibility
3. People Insights
4. Technology Preparedness

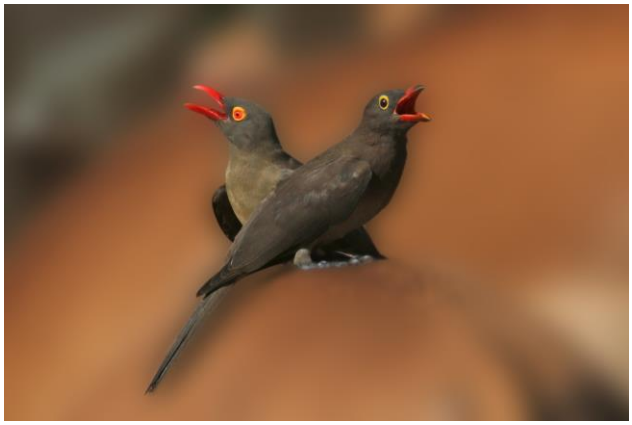
Deep Analytics

We use artificial intelligence to search a huge number of public information sources – billions of records - to identify an organization's behavioral patterns.

Organization Attitude

Deep analytics and advanced pattern matching are used to identify how the organization is perceived. We use our proprietary algorithms to review a large number and variety of public information sources. The same information that a predator would use.



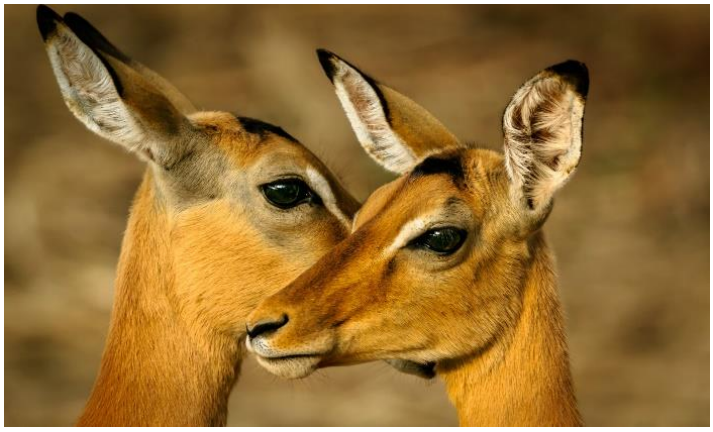


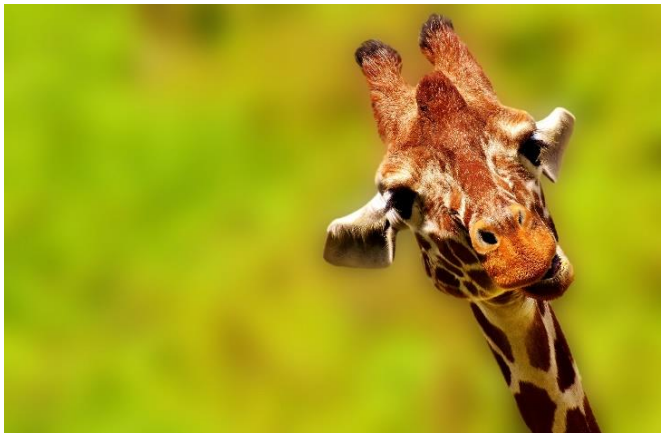
Technology Visibility

How well do you think an adversary understands the technology that you're using? Is it easily identifiable? Our search algorithms are designed to identify the basic building blocks a predator would need to launch a successful attack. If we can do it so can they!

People Insights

How do your people perceive your organization? Both present and past employees? Does your organization suffer from a high number of complaints? The depth and experience of your team? We identify the same weaknesses that a predator would, except we tell you what they are and what can be done to improve.





Technology Preparedness

Is your technology suitable for the current cyber-attack landscape? Is it performant? Dependent on 3rd party software? Legacy or dated approaches? This domain isn't a penetration test but is instead designed to understand where in the technology stack a predator would find it easiest to attack.

The attack assessment is available in basic, standard or advanced options with results made available in 7, 14 and 28 days respectively. Basic is a behavioral snapshot, standard adds in-depth analysis of the four domains and advanced includes behavioral recommendations. All of which are designed to address the question of Why are you a target?

Why are you a target?

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

Features	Basic	Standard	Advanced
Organization Attitude	✓	✓	✓
Technology Visibility	✓	✓	✓
People Insights	✓	✓	✓
Technology Preparedness	✓	✓	✓
Behavioral Snapshot	✓	✓	✓
In-Depth Domain 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		
Attack Assessment		
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.