

Threat intelligence provides enterprise defenders advantages against adversaries through actionable intelligence on current threats, vulnerabilities, and security trends. This intelligence allows for the development or implementation of proactive defensive measures and improved response actions to enhance security posture.

OUR OFFERINGS

DISCOVER

Deep/ Dark Web Recon

Conduct threat reconnaissance within a rich set of deep/ dark web content to include:

- Assets for sale (e.g., fraud)
- Leaked sensitive data
- Soliciting insiders

Threat Landscape

Analyze and synthesize intelligence for your threat landscape to include:

- Relevant threat actor profiles
- Trending tools and Tactics, Techniques, & Procedures (TTP)
- Notable industry attacks and lessons

Open Source Intelligence Exposure

Scour the open web for relevant threats including:

- Credentials and other sensitive data leaks
- Negative/ unauthorized commentary

BUILD

Intelligence Program

- Design and build based on desired end-state objectives to include human and machine-readable intelligence
- Lead workshop sessions for tactical, operational, and strategic audiences

Intelligence Tools

- Support the selection of technologies based on use cases and functional requirements
- Strategically plan and operationally design the deployment of new technologies
- Architect the integration and/ or the automation of current technologies
- Execute deployment, integration and/ or automation

ASSESS

Intelligence Program

- Assess current state capacity aligned to the intelligence lifecycle with a focus on human and machine-readable intelligence
- Create recommendations roadmap to achieve higher levels of desired capability

Intelligence Tools

- Assess current effectiveness to include breadth and depth of deployment and employment of relevant features
- Recommend features, settings, and workflows to achieve maximum value

MANAGE

Intelligence Program

Conduct routine intelligence support based on intelligence requirements to include:

- Collections of intelligence
- Routine intelligence digests
- Temporary staff augmentation
- Reach back support

Tailored Intelligence

Conduct specific and custom intelligence analysis and production to include:

- Requests for information (RFI)
- Supply chain risks
- Merger & acquisition risks
- Discover LinkedIn imposters targeting employees