eventus

eventussecurity.com

CYBER THREAT INTELLIGENCE SERVICE

Stay informed, Stay Secure: Harness the Power of Cyber Threat Intelligence and Protect Your Digital Landscape

EVENTUS CYBER THREAT INTELLIGENCE SERVICE

The challenges of optimizing your infrastructure to fend off cyber threats can be significant at times. Eventus offers Cyber Threat Intelligence Services that enable you to proactively prevent attacks and optimize your security. Our proven services provide deep support to help you combat threats, whether you need to augment a larger team or force multiply a small one.

Leveraging our industry-leading collections, technology, and human expertise, we help you stay ahead of emerging threats while saving time and money. With Eventus Threat Labs Intelligence, you can confidently protect your organization from potential attacks and optimize your security posture.

BENEFITS

- **Early Detection and Response:** Threat intelligence provides early detection of emerging threats and helps organizations respond quickly to prevent attacks or minimize their impact.
- **Proactive Defense:** Threat intelligence enables proactive defense by identifying potential threats and vulnerabilities before they are exploited.
- **Improved Decision Making:** Threat intelligence provides valuable insights into the tactics, techniques, and procedures (TTPs) used by attackers. This information can be used to inform decision making around security strategy, policy, and operations.
- **Increased Efficiency:** Threat intelligence automates the process of gathering and analyzing threat data, reducing the time and effort required to identify and respond to threats.
- **Enhanced Situational Awareness:** Threat intelligence provides a comprehensive view of the threat landscape, including the types of attacks, the industries being targeted, and the motivations of attackers. This information can help organizations develop a more effective security posture.
- **Collaborative Defense:** Threat intelligence can be shared among organizations to improve their collective defense against common threats. This allows organizations to benefit from the knowledge and expertise of others in the security community.

THREAT INTEL TYPES

1. Strategic Threat Intelligence

Focussed on understanding high level trends and adversarial motives, and then leveraging that understanding to engage in strategic security and business decision making.

Stakeholders:
- CISO
- CIO
- CTO
- Executive Board

2. Operational Threat Intelligence

Focused on understanding adversarial capabilities, infrastructure and TTPs, and then leveraging that understanding to conduct more targeted and prioritized cybersecurity operations.

Stakeholders:
- Threat Hunter
- SOC Analyst
- Vulnerability Management
- Incident Response

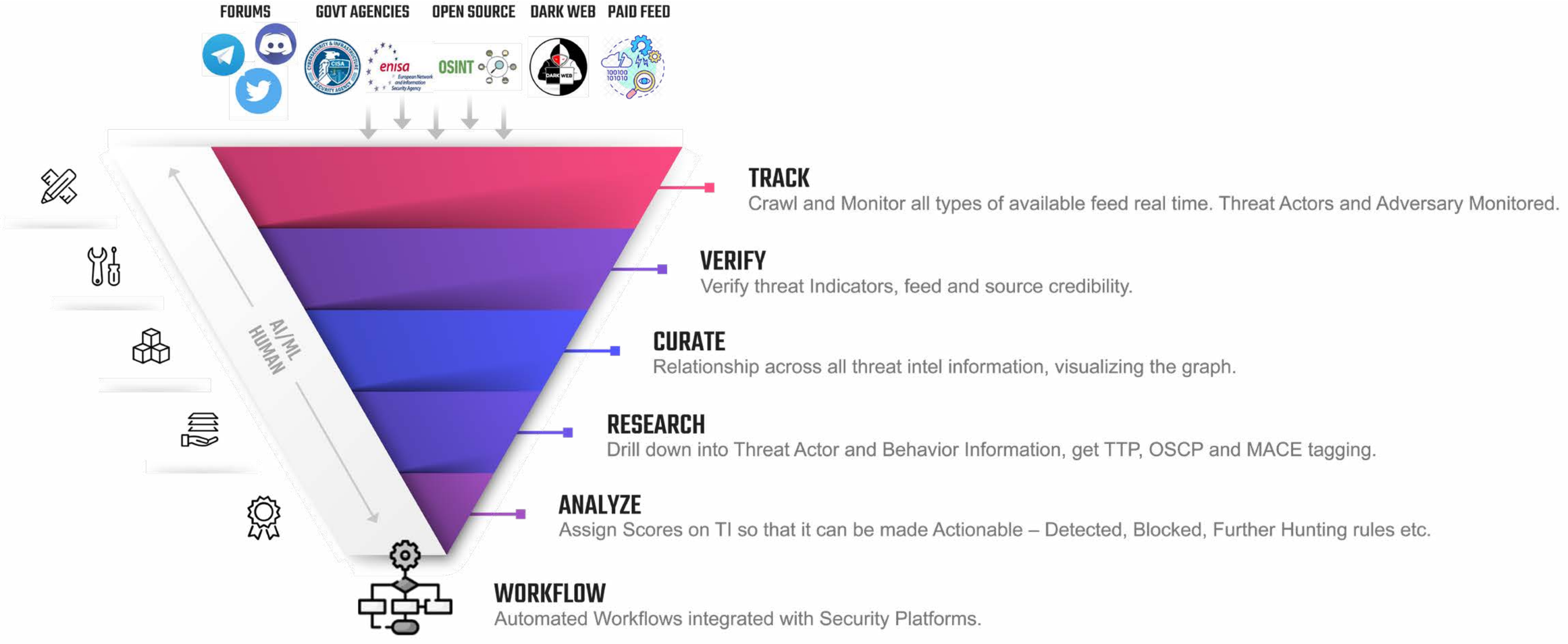
3. Tactical Threat Intelligence

Focused on performing Malware analysis and Enrichment, as well as ingest atomic, static and behavioural threat indicators into defensive cybersecurity systems.

Stakeholders:
- SOC Analyst
- SIEM and Datalakes
- Endpoints and Servers
- Network Security

HOW WE DELIVER?

- **Track** - Govt Agencies, Open Intel, Vendor Provided, Exploit repos, OSINT Feeds, Social Media, Twitter
- **Analyze** - Malware Reverse Engineering, Static and Dynamic analysis, Sandbox Analysis, MACE Mapping
- **Research** - Dark Web, Malware Sites, Yara Analysis, TTP Profiling, Adversary Mapping
- **Curate** - AI Driven, Relationship added on all TI received, Automated, Prioritized and Confidence score added, Threat Rule (Mitre/Behavior Based)
- **Verify** - Automated, Human Verified, Continuous Strategic- Nation State, Threat Actor, Industry Mapping



IMPORTANCE OF DARK WEB MONITORING

Proactive protection is important, and Threat Intel plays a vital role in identifying potential risks. But have you considered the possibility of planned attacks on your organization? Are there any mentions of your organization in the dark web? Could there be a breach happening without your knowledge? Is your organization's sensitive information being sold by threat actors?

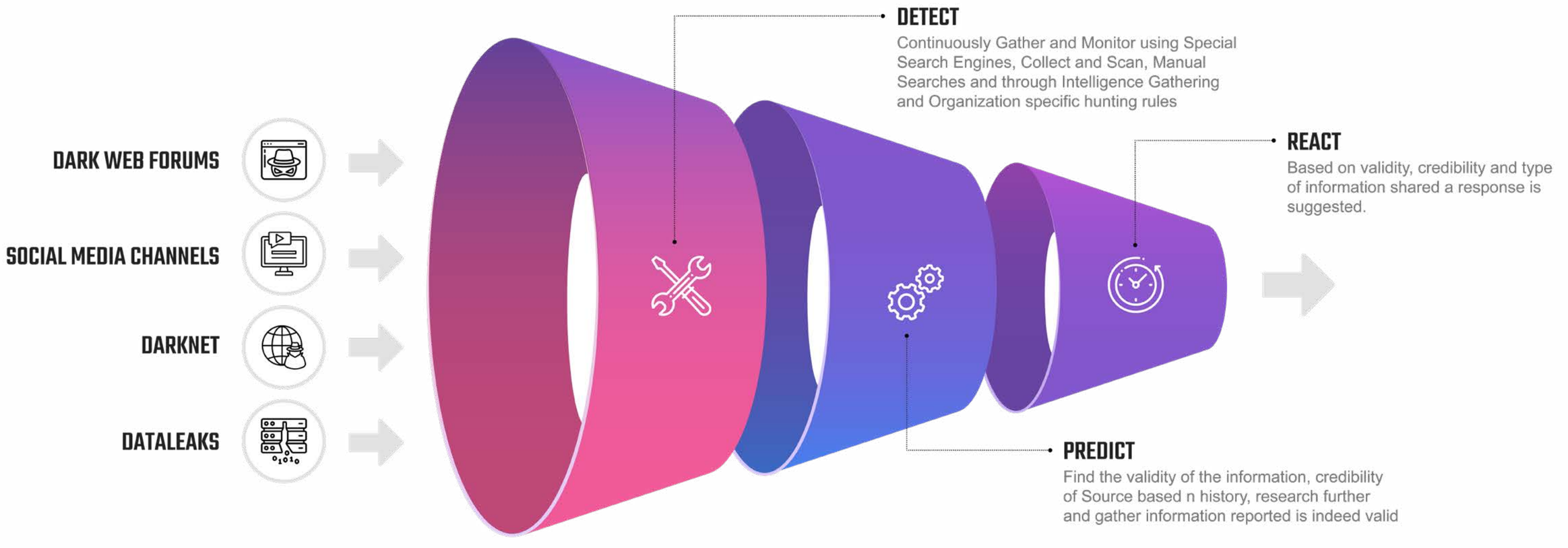
With deep-dive investigative capabilities, Eventus Threat Labs helps threat hunting teams seek the highest priority potential cyberthreats. With our in-house researchers, AI platform, and partnership with GroupIB's Unified Risk Platform, which has the industry's largest dark web database, we have access to valuable intelligence. Our Threat Intelligence service allows us to uncover illegal activities and monitor whether your organization is mentioned on the dark web.

Eventus Threat Labs offers a comprehensive solution by combining threat intelligence and dark web monitoring into an Essential Package. This package includes continuous monitoring and the creation of custom rules to keep you informed when any topics of interest arise.

BENEFITS

Adding dark web monitoring to your threat intelligence program can provide several key benefits, including:

- **Early detection of potential threats:** Monitor underground forums, marketplaces, and other criminal networks for signs of potential threats. To provides early warning of emerging threats and enable organizations to become proactive.
- **Protection against data breaches:** Detect data breaches and prevent the exposure of sensitive data, such as user credentials or confidential information. Also, avoid reputational damage and potential legal consequences.
- **Improved incident response:** Providing valuable information during incident response activities, such as identifying the source of an attack, or the methods used by attackers. Organizations can respond quickly and effectively to minimize the impact of an attack.
- **Competitive advantage:** By monitoring the dark web, organizations can gain insights into emerging threats and stay ahead of their competitors. Organizations can also identify new business opportunities or avoid potential risks.
- **Comprehensive threat intelligence:** Dark web monitoring provides a more comprehensive view of the threat landscape, including both publicly available and underground sources. Better understand the motivations and methods of attackers.



PACKAGES

ESSENTIALS

Tactical Threat Intel
- IOC's

Operational Threat Intel
- Threat
- Adversary and OCSF Mapping
- Malware Reverse Engg
- MACE Layout

Strategic Threat Intel
- Adversary mapping with industry
- Industry specific advisory

Enrichment & Curation
- Analysis
- Verification and Confidence Score

Dark Web Monitoring
- Public leaks
- Git leads
- Breached DB
- Darkweb Forums
- Instant Messengers
- Underground shops
- Ransomware DLS & Cyber Criminals

ADVANCED

Tactical Threat Intel
- IOC's

Operational Threat Intel
- Threat
- Adversary and OCSF Mapping
- Malware Reverse Engg
- MACE Layout

Strategic Threat Intel
- Adversary mapping with industry
- Industry specific advisory

Enrichment & Curation
- Analysis
- Verification and Confidence Score

Dark Web Monitoring
- Public leaks
- Git leads
- Breached DB
- Darkweb Forums
- Instant Messengers
- Underground shops
- Ransomware DLS & Cyber Criminals
- Compromised Credential
- Nation State Actors

BRAND MONITORING AND TAKE DOWN

DRP and Phishing Malicious URL's – Per Brand
- Phishing and Malicious URL's

DRP Scams and Trademark Abuse – Per Brand
- Social Media
- Web
- Instant Messengers
- Advertisement
- Mobile App Stores

Takedown Services - 1
- 10 Takedowns Per Month

Takedown Services - 2
- 25 Takedowns Per Month

Takedown Services - 3
- Unlimited

Contact us at

sales@eventussecurity.com

www.eventussecurity.com