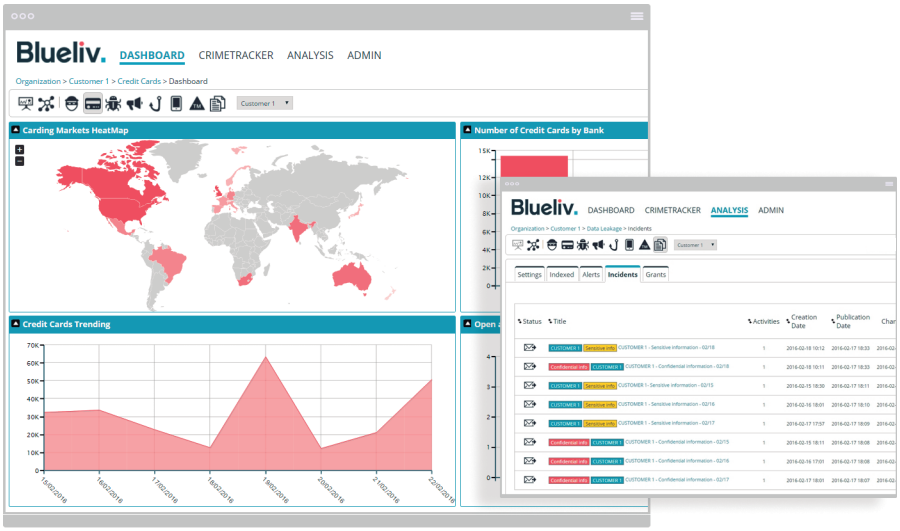
ADVANCED ACQUISITION THREAT INTELLIGENCE PLATFORM

Cyber threats are increasing almost exponentially, they are becoming more complex, and new threat actors are emerging from the dark web. Their targets? Primarily financial services, telecommunications, utilities, government agencies, and retailers. Today, static or reactive defenses against general threats are not enough.

Blueliv takes a proactive approach to deliver targeted, actionable threat intelligence. The Blueliv platform actively hunts down threats that exist outside of your corporate network, identifying and tracking malicious events and actors before they cause harm inside your network. Blueliv automatically collects, analyzes, correlates, categorizes, and presents threat data across critical threat categories: botnets and command & control; targeted malware; credit card theft; rogue mobile apps; hacktivism; data leakage; phishing and cybersquatting; and brand abuse.



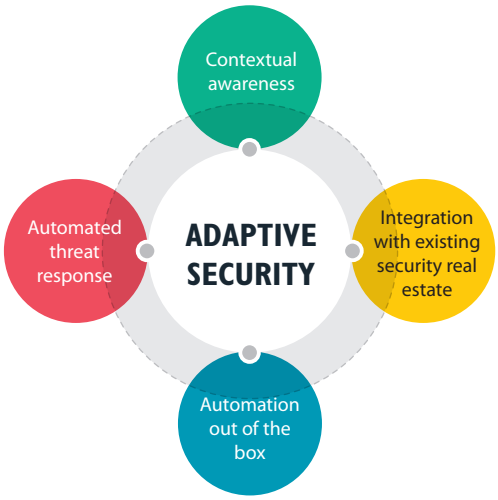
Powerful dashboard delivers critical data to inform threat defense decision-making

With Blueliv, targeted threat intelligence is immediately available to your security analysts and your other security systems. You gain valuable situational awareness with the ability to quickly remediate threats before they cause substantial harm. As a strategic part of your security defenses, Blueliv also enables you to easily add third-party security vendor feeds and RSS, new websites, forums, and other sources to continually improve your organization's adaptive threat response.

Blueliv triages incident responses, enabling your team to quickly stop threats, remediate damage, and implement a strategic solution that makes it extremely difficult for a similar attack vector to succeed. Targeted, triaged threat intelligence saves time and maximizes your security resources while accelerating accurate response.

BLUELIV DELIVERS SPECIFIC ANSWERS TO SPECIFIC QUESTIONS:

- Where specifically has your corporate network been compromised?
- Which IP addresses have been compromised?
- Which users have been compromised?
- What is the specific nature of the compromise?
- What malicious IP addresses are actually infected machines connecting to the network?
- Who is targeting your organization?
- Where in your global URL list are you being targeted?



COMPREHENSIVE PROTECTION

The Blueliv modular delivery platform protects enterprises from a wide range of threats, including:

BOTNETS AND COMMAND & CONTROL

The Blueliv platform can recover credentials from a diverse range of sources to identify internal and external infections. It helps protect your business and users from potential damage, such as becoming part of a botnet network, data theft, or other cyber threats.

TARGETED MALWARE

Blueliv enables users to track and hunt malware that is specifically targeting an organization. Upload a malware sample, have it analyzed, and help keep dangerous or infected files out of your websites and servers.

CREDIT CARD THEFT

This module helps you detect credit card information that has been stolen so that you can protect customers or employees from becoming victims of fraud. Retrieve compromised credit cards when they are published and sold on black markets.

HACKTIVISM

Defend against targeted social-borne cyber attacks as well as track and monitor global social hacktivism operations. Detect cyber threats against your organization, pinpoint information leaks after an attack, and monitor global social Hacktivism Ops.

DATA LEAKAGE

Discover whether or not your organization's sensitive documents or data have become publicly available on the Internet and peer-to peer networks. Detect and identify data that could represent leaked information across multiple file-sharing platforms.

PHISHING AND CYBERSQUATTING

Combat both types of attacks at once. Blueliv detects attempts to acquire sensitive information by actors masquerading as trusted entities or by detecting similar domains that can potentially be used to replace your company's original domains.

MALICIOUS MOBILE APPLICATIONS

Identify false, infected, modified, or copied apps, as well as apps performing brand abuse activities. Detect rogue applications that bear your name when they are uploaded to a market place, as well as illegal mobile apps that are being publicly published.

BRAND ABUSE

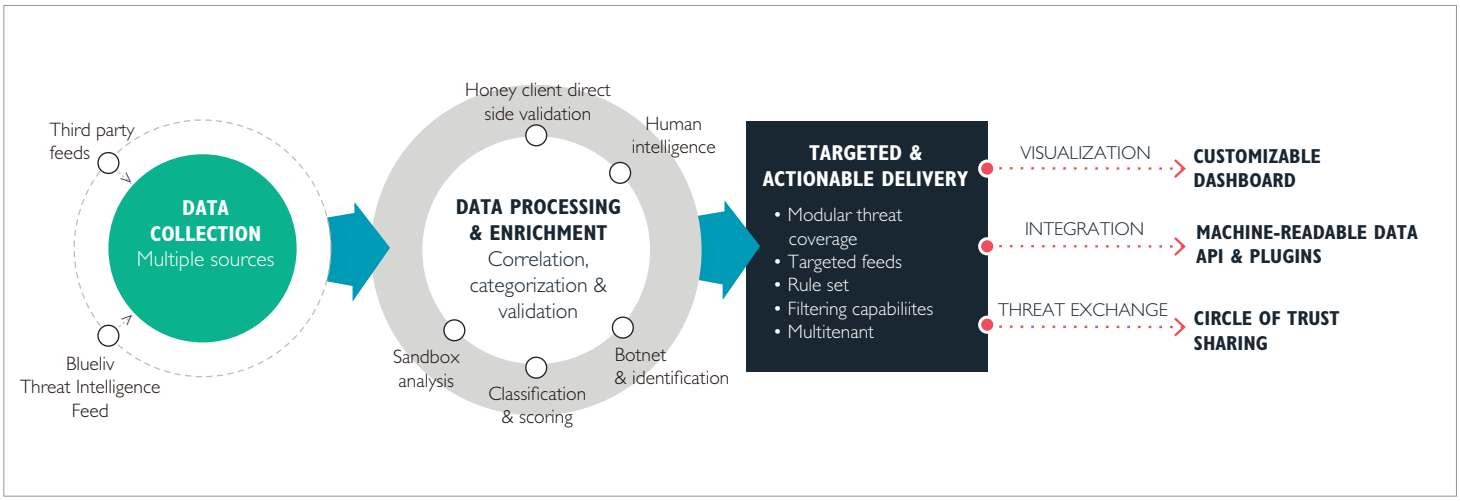
Identify and shut down site impersonations and claimed affiliations sites. Track and monitor user sentiment, as well as potentially brand-damaging stories that identify security weaknesses on an entity's online sites. This module pinpoints and prioritizes abuse incidents, enabling stronger brand protection.

NEWS

The "NEWS" scans and retrieves - in REAL TIME - relevant news from thousands of newspapers around the globe in multiple languages.

SINGLE POINT FOR AUTOMATED, TARGETED INTELLIGENCE

Built on documented, proven intelligence analysis methodology, Blueliv provides a central point of control for automated operational, tactical, and strategic threat intelligence. It includes five functionalities.



THREAT DATA COLLECTION

Blueliv automates threat data collection from multiple sources, whether closed, private, or open—and in multiple formats. Adding a new source is as easy as adding a new Java or Python plugin into the Blueliv administrative panel. As data comes into the Blueliv platform, we cloak it and provide it to you. The platform includes Blueliv's own Data Feed which provides unique intelligence about verified online crime servers conducting malicious activity, infected bot IPs, malware hashes, attacking IPs and hacktivism activities

THREAT DATA CORRELATION & ENRICHMENT

The Blueliv platform performs powerful information categorization, honey client direct side validation, and sandbox analysis and scoring. It combines data correlation with Big-Data storage for delivering ongoing analysis combined with human intelligence. Blueliv also connects and correlates data collected from across third-party feeds to identify common attack vectors and actors. You receive machine-readable, actionable intelligence.

ACTIONABLE INTELLIGENCE

Blueliv's powerful visualization tools represent targeted threat intelligence intuitively, making it easy to focus on actionable information. Use the information to create your own YARA rules, gain a tactical advantage, and create strategic cyber threat response capabilities. Blueliv generates its own targeted threat intelligence, and we also enable you to generate your own actionable intelligence and feeds by creating rules, labels, and classification with tags, alerts, and incident notifications.

THREAT DATA INTEGRATION

Add other vendors' data feeds into your Blueliv solution and use targeted threat intelligence to complement internal firewalls, SIEMS, IDS/IPS, and monitoring capabilities. Plugins are available for Splunk, AlienVault, ArcSight, and Elastic-ELK. Blueliv also offers APIs and a powerful SDK for integration with third-party security platforms, internal security operations centers (SOCs), or computer emergency response teams (CERTs). Blueliv supports STIX/TAXII enabling easy information sharing between different data formats. This makes fast and easy to inject data into your traditional security elements.

EXCHANGING THREAT INTELLIGENCE

Blueliv targeted threat intelligence can be shared across your internal groups and with trusted third parties. Enable a single user to collect threat data of specific interest and easily find and sort it using tags. Quickly and easily share relevant, timely, accurate Indicators of Compromise (IOCs) about new or ongoing cyber attacks and threats to avoid breaches or minimize damage from an attack.

BENEFITS

BLUELIV ACCELERATES ACCURATE, ADAPTIVE RESPONSES

By automating targeted threat intelligence collection and presentation, you gain new visibility into threats and reduce incident response times. Targeted intelligence significantly reduces business disruption and reduces windows of opportunity for threat actors. Blueliv's Big-Data analytics capabilities quickly deliver actionable information with minimal false positives in a single view—with context and underlying detail—for better decision-making.

ENHANCE YOUR SECURITY TEAM'S EFFICIENCY

The Blueliv platform enables your security team to enhance their capabilities and create responses that keep away threat actors—without having to add staff. Eliminate the need to sort through thousands of alerts, and let your team focus on targeted threat intelligence with sophisticated analysis capabilities. The Blueliv multitenant platform provides role-based access control and is delivered through the cloud, enabling you to easily manage threats across business units, organizations or departments.

BUILD STRATEGIC RESPONSES

Blueliv lets you build a list of malicious IP addresses, which can be added into internal and perimeter security control devices. It identifies compromised accounts being used to access corporate resources, and it ensures greater scrutiny and control over mobile applications and claimed associations. With Blueliv, you can create a strategic set of responses to specific threats, understand the kill chain and maximize the effectiveness of your valuable security team.

EASE OF USE IMPROVES YOUR SECURITY POSTURE

Because Blueliv delivers targeted and automated threat intelligence with flexibility, your team can quickly enhance the security posture of your organization. Customizable dashboards enable staff to easily set rules and define filters to tailor capabilities to your organization's needs. Add new sources to monitor, and automatically receive data in machine-readable formats to improve the accuracy and effectiveness of other security measures. You also can automate global threat response for added peace of mind.

EASY TO DEPLOY

Blueliv is easy to buy and provides high-impact results immediately. As a cloud-based solution, the platform eliminates the need to install hardware or software. Flexible licensing options make it easy to provide adaptive protection across the enterprise to operations located anywhere. Deploy correct, compliant controls exactly where they're needed, and see results in minutes or hours.

START TODAY

Don't wait for cyber threats to find you. Learn more about how Blueliv can help protect your enterprise. Request a demo and test the cyber threat intelligence solution at:

www.blueliv.com/arrange-a-demo

ABOUT BLUELIV

Blueliv is a leading provider of targeted cyber threat information and analysis intelligence for large enterprises, service providers, and security vendors. Blueliv's clients include leading bank, insurance, telecom, utility, and retail enterprises in Europe, and the company has alliances with leading security vendors and other organizations to share cyber intelligence. Blueliv was named Gartner 2015 Cool Vendor.

NetSec Chile

www.blueliv.com

info@blueliv.com

twitter.com/blueliv

linkedin.com/company/blueliv

plus.google.com/+Blueliv