Threat Context

Deeper defense, richer investigation.

Accelerate your cybersecurity processes before, during and after an attack

Improve team productivity with qualified, easy-to-use interrelated threat intelligence.

Threat Context provides SOC, Incident Response and Threat Intelligence teams with continuously updated and intuitive information around threat actors, campaigns, malware indicators, attack patterns, tools, signatures and CVEs.

Using Blueliv's ever-expanding database of over 70 million items, the easy-to-use module offers pivoting capabilities similar to Wikipedia, so analysts can rapidly gather enriched, contextualized information to enhance cybersecurity processes before, during and after an attack.

What business benefits does it deliver?

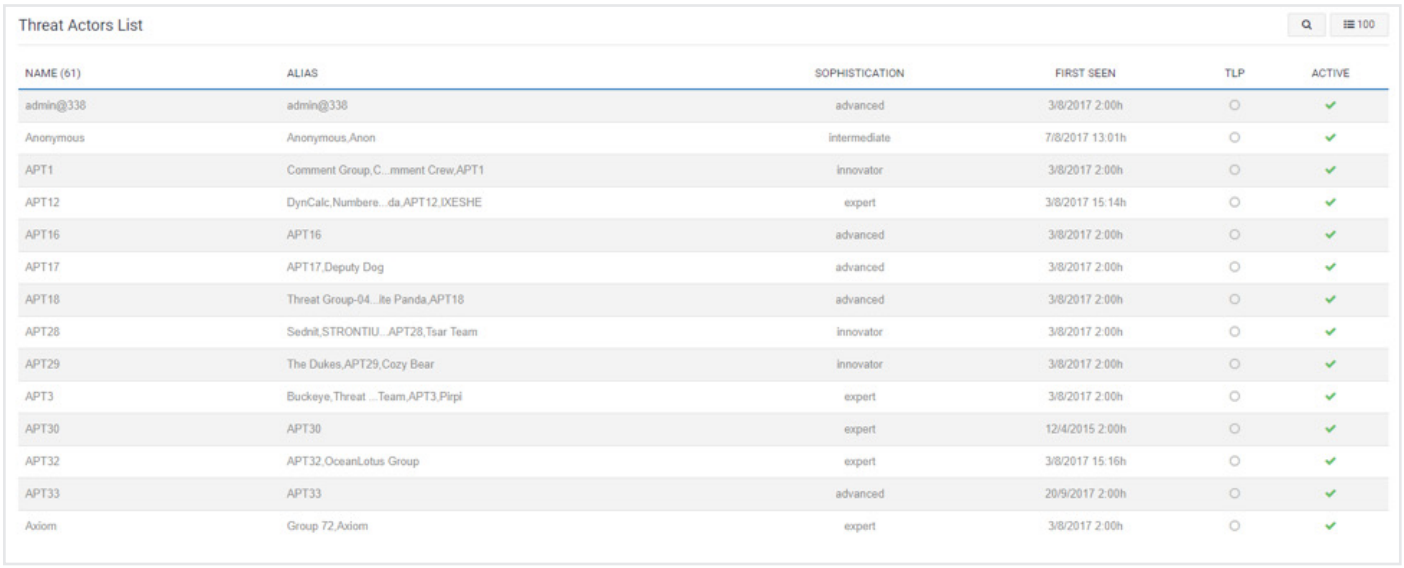
1. Improve team productivity using verified information delivered by our proprietary automated engine and human intelligence

2. Reduce information overload and shorten incident response times, empowering your security team with powerful threat management detail

3. Prepare and protect your perimeter against malicious actors before they strike, with specific detail around campaigns and attack vectors based on trends and factual threat information

What does it do?

- Facilitates analysis of actors and campaigns affecting your organization or sector, using information that can also help red teams execute highly realistic attack simulations
- Speeds up triage processes and incident response using qualified information to help orchestration systems prioritize relevant IOCs and detail required for forensics
- Charts and plots the threat landscape for you to follow through an intuitive, multifaceted interface



Threat Actors List

NAME (61)	ALIAS	SOPHISTICATION	FIRST SEEN	TLP	ACTIVE
admin@338	admin@338	advanced	3/8/2017 2:00h		✔
Anonymous	Anonymous,Anon	intermediate	7/8/2017 13:01h		✔
APT1	Comment Group,C...mment Crew,APT1	innovator	3/8/2017 2:00h		✔
APT12	DynCalc,Numbere...da,APT12,IXESHE	expert	3/8/2017 15:14h		✔
APT16	APT16	advanced	3/8/2017 2:00h		✔
APT17	APT17,Deputy Dog	advanced	3/8/2017 2:00h		✔
APT18	Threat Group-04...ite Panda,APT18	advanced	3/8/2017 2:00h		✔
APT28	Sednit,STRONTIU...APT28,Tsar Team	innovator	3/8/2017 2:00h		✔
APT29	The Dukes,APT29,Cozy Bear	innovator	3/8/2017 2:00h		✔
APT3	Buckeye,Threat ...Team,APT3,Pirpi	expert	3/8/2017 2:00h		✔
APT30	APT30	expert	12/4/2015 2:00h		✔
APT32	APT32,OceanLotus Group	expert	3/8/2017 15:16h		✔
APT33	APT33	advanced	20/9/2017 2:00h		✔
Axiom	Group 72,Axiom	expert	3/8/2017 2:00h		✔

About Blueliv

Blueliv is a leading cyberthreat intelligence provider, headquartered from Barcelona, Spain. We scour the open, deep and dark web to deliver fresh, automated and actionable threat intelligence to organizations, helping protect their networks from the outside in. Blueliv's scalable cloud-based technology turns global threat data into sophisticated, relevant intelligence. We enable organizations to save time and resource by accelerating incident response performance, providing user-friendly evidence accessible to all levels within cybersecurity operations teams. Our pay-as-you-need solution delivers an accelerated, predictive view of the threat landscape in real-time. We do not believe in a one-size-fits-all approach, and work together to configure a modular solution bespoke to your needs using separate intelligence modules, all backed up by our world-class in-house analyst team. Blueliv has been named 'Threat Intelligence Company of the Year' by Cybersecurity Breakthrough Awards, a Gartner 'Cool Vendor,' and Go-Ignite winner, in addition to holding affiliate membership of FS-ISAC for several years.

blueliv.com

info@blueliv.com

twitter.com/blueliv

linkedin.com/company/blueliv

CYBERSECURITY BREAKTHROUGH AWARD 2018

GO IGNITE 2016

Gartner 2015 CoolVendor