Blueliv
AN OUTPOST24 COMPANY

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, Threat hunting, compliance and Threat Intelligence teams with continuously updated and intuitive information around threat actors, campaigns, IOCs, attack patterns, tools, signatures, CVEs, malware analysis and the relations between them.

Using Blueliv's ever-expanding database of 180+ million items, the easy-to-use module offers pivoting capabilities, so analysts can rapidly gather enriched, contextualized information to enhance cybersecurity processes before, during and after an attack.

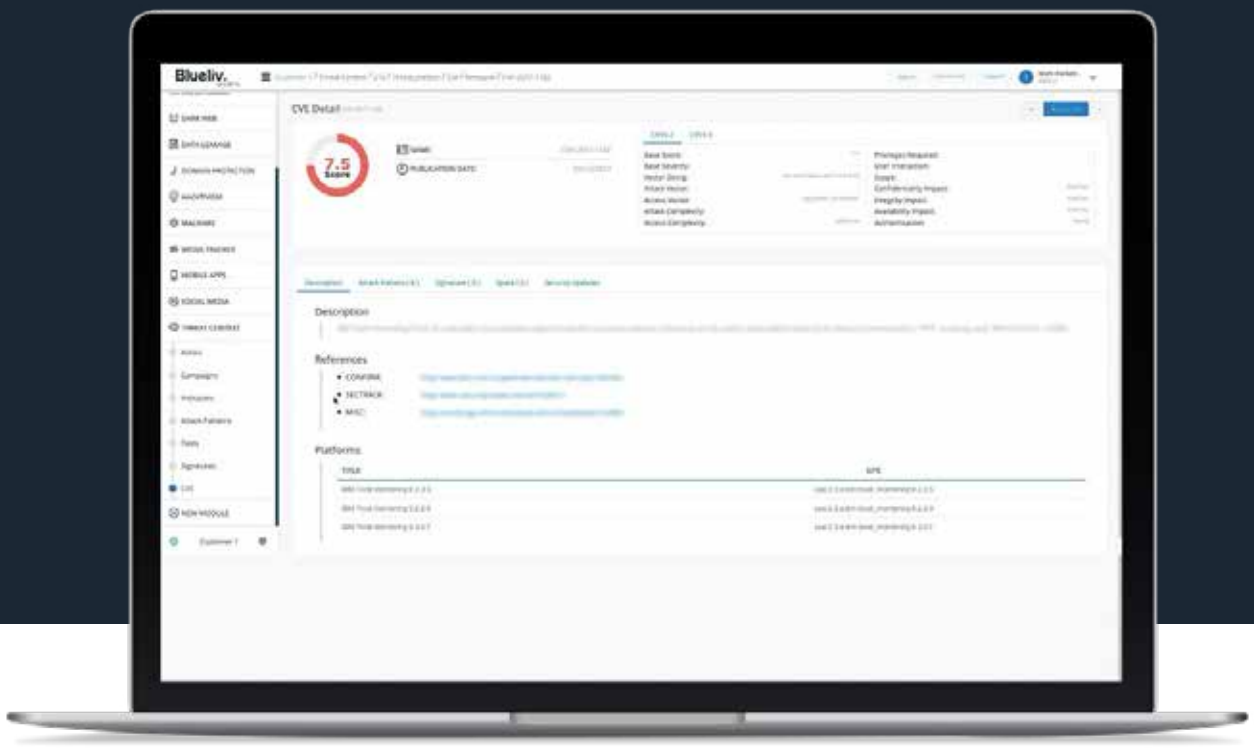
What business benefits does it deliver?

1. Improves team productivity using verified information delivered by our proprietary automated engine and human intelligence
2. Reduces information overload and shortens incident response times, empowering your security team with powerful threat management detail
3. Prepares and protects 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?

1. Facilitates analysis of actors and campaigns affecting your organization or sector
2. Helps red teams execute highly realistic attack simulations
3. Speeds up triage processes and incident response using qualified information to help orchestration systems prioritize relevant IOCs and detail required for forensics
4. Achieves effective Vulnerability Management with contextual Threat Intelligence and scoring for CVE
5. Accelerates Threat hunt with in-depth intelligence against Blueliv malware database
6. Initiates the most rapid and effective attack response and contributes to adopt a solid security posture to optimize your post-breach compliance process

Blueliv.
AN OUTPOST24 COMPANY



Contact sales@blueliv.com for a demonstration.

computing Security Excellence Awards 2018
Winner
Enterprise Threat Detection Award

computing Security Excellence Awards 2018
Winner
Enterprise Security Award

CYBERSECURITY BREAKTHROUGH AWARD 2018

Blueliv is Europe's leading cyberthreat intelligence provider, headquartered in Barcelona, Spain. We look beyond your perimeter, scouring the open, deep and dark web to deliver fresh, automated and actionable threat intelligence to protect the enterprise and manage your digital risk. Covering the broadest range of threats on the market, a pay-as-you-need modular architecture means customers receive streamlined, cost-effective intelligence delivered in real-time, backed by our world-class in-house analyst team. Intelligence modules are scalable, easy to deploy and easy to use, maximizing security resource while accelerating threat detection, incident response performance and forensic investigations. Blueliv is recognized across the industry by analysts including Gartner and Forrester, and has earned multiple awards for its technology and services including 'Security Company of the Year 2019' by Red Seguridad, Enterprise Security and Enterprise Threat Detection 2018 category winners by Computing.co.uk, in addition to holding affiliate membership of FS-ISAC for several years.

blueliv.com info@blueliv.com twitter.com/blueliv linkedin.com/company/blueliv