BULLET PROOF

BULLETPROOF S.W.A.T. DEFENCE®

NEXT-GENERATION CYBER THREAT PROTECTION

CONTENTS

S.W.A.T. DEFENCE® | OVERVIEW

REAL-TIME PROTECTION FOR TOMORROW'S THREATS

Bulletproof S.W.A.T. Defence® is a multi-layered threat protection suite that combines a feature-rich managed SIEM with military-grade intelligent cyber protection modules. Built with advanced machine learning and integrated threat intelligence, S.W.A.T. Defence® is engineered with innovation at its core to meet the security challenges of tomorrow.

Bulletproof believe human expertise, insight and ingenuity are fundamental to keeping ahead of the modern dynamic threat landscape. That's why Bulletproof puts experienced security analysts at the core of our service. By escalating outcomes and actions, not floods of alerts, S.W.A.T. Defence® delivers credible security improvements to your organisation. Combining this ethos with our world-leading suite of SIEM tools and 'as a Service' delivery model, makes S.W.A.T. Defence® a powerful solution to solve the security challenges of today and beyond.

"SpecialOps® drives the continuous improvement of S.W.A.T. Defence®, meaning we're always able to detect and counter the latest cyber threats."

BULLETPROOF SPECIALOPS® ENHANCED INTELLIGENCE

Bulletproof SpecialOps® is the home of our research and intelligence division. It's a unique development lab, staffed by an elite team and drives innovation across our entire product suite.

Anonymised data from our entire range of security products is analysed in conjunction with internal and commercial intelligence, in order to significantly enhance our services.

SpecialOps® drives the continuous improvement of S.W.A.T. Defence®, meaning we're always able to detect and counter the latest cyber threats.

S.W.A.T. DEFENCE® | KEY FEATURES

FEATURE-RICH PROTECTION

S.W.A.T. Defence® delivers comprehensive security thanks to its full list of protection features, including:

- 24/7 protection
- Proactive threat hunting
- Network & host IDS/IPS
- File integrity monitoring
- Web application firewall
- Flexible VA scans
- System hardening

SAAS DELIVERY

Thanks to our continuously updated SaaS platform, you're always protected against the latest cyber vulnerabilities and exploits. SaaS delivery also means S.W.A.T. Defence® offers extremely rapid set-up and on-boarding, with a 10-minute deployment process.

CLOUD READY

S.W.A.T. Defence® has been built for native integration with public cloud (Azure, AWS, Google), container and serverless deployments, as well as traditional on-premises infrastructure.
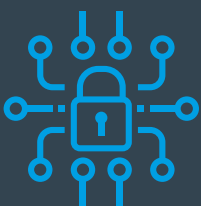
BUILT TO BE BULLETPROOF

Bulletproof retain full ownership of our service design and delivery. This includes engineering our powerful, innovative SIEM platform and its scalable cloud underpinning, as well as running our 24/7 in-house Security Operations Centre.

S.W.A.T. DEFENCE® | CAPABILITY

The challenge for many organisations is finding trained, experienced security experts to deploy, manage and monitor a traditional SIEM. By choosing the Bulletproof managed option, you're protected 24/7 by a team of dedicated security analysts who filter out noise to target genuine security threats. Backed by research from Bulletproof's SpecialOps® division, S.W.A.T. Defence® turns your raw logs into actionable intelligence, enabling our analysts to proactively prevent cyber attacks.

THE WORLD'S MOST POWERFUL SIEM

Our in-house engineered SIEM can search millions of logs in milliseconds and ingest thousands of logs per second, from virtually any source. Advanced parsing allows S.W.A.T. Defence® to cut through the noise and quickly establish a baseline, meaning our skilled security analysts escalate outcomes and actions to you, not alerts.
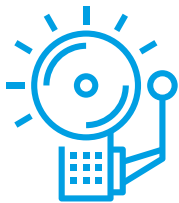
NETWORK & HOST INTRUSION DETECTION (IDS)

Detect and even proactively block malicious traffic and behaviour. Our IDS modules can be host or network based, with our security analysts' expert configuration knowledge and machine learning components combining to deliver a low number of false positives.

FILE INTEGRITY MONITORING (FIM)

FIM is a high-value cyber defence but can easily lead to alert fatigue if not implemented correctly. S.W.A.T. Defence® takes an intelligent approach to FIM, with our experienced SOC analysts fine-tuning the configuration to deliver useful alerts on your critical files.

"You're protected 24/7 by a team of dedicated security analysts who filter out noise to target genuine security threats."
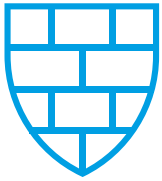
WEB APPLICATION FIREWALL (WAF)

Stay protected against common web exploits with our WAF module. By filtering HTTP traffic and watching for potential threats, S.W.A.T. Defence® secures your application against attacks like XSS and SQL injections.

FLEXIBLE VULNERABILITY SCANS (VA)

Developed with intelligence from Bulletproof's SpecialOps® research division, our integrated scanning platform features commercial and in-house built scanning engines. Our VA scans are detailed and methodical. They've even been PCI DSS ASV certified.
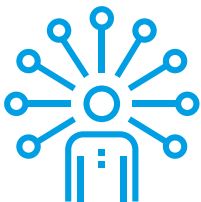
PROACTIVE SYSTEM HARDENING

Daily security audits automatically check system configurations against best-practice CIS benchmarks, giving a quick outline of systems and applications that are susceptible to exploitation. This enables proactive system hardening, where your infrastructure is fine-tuned based on your specific attack surface.
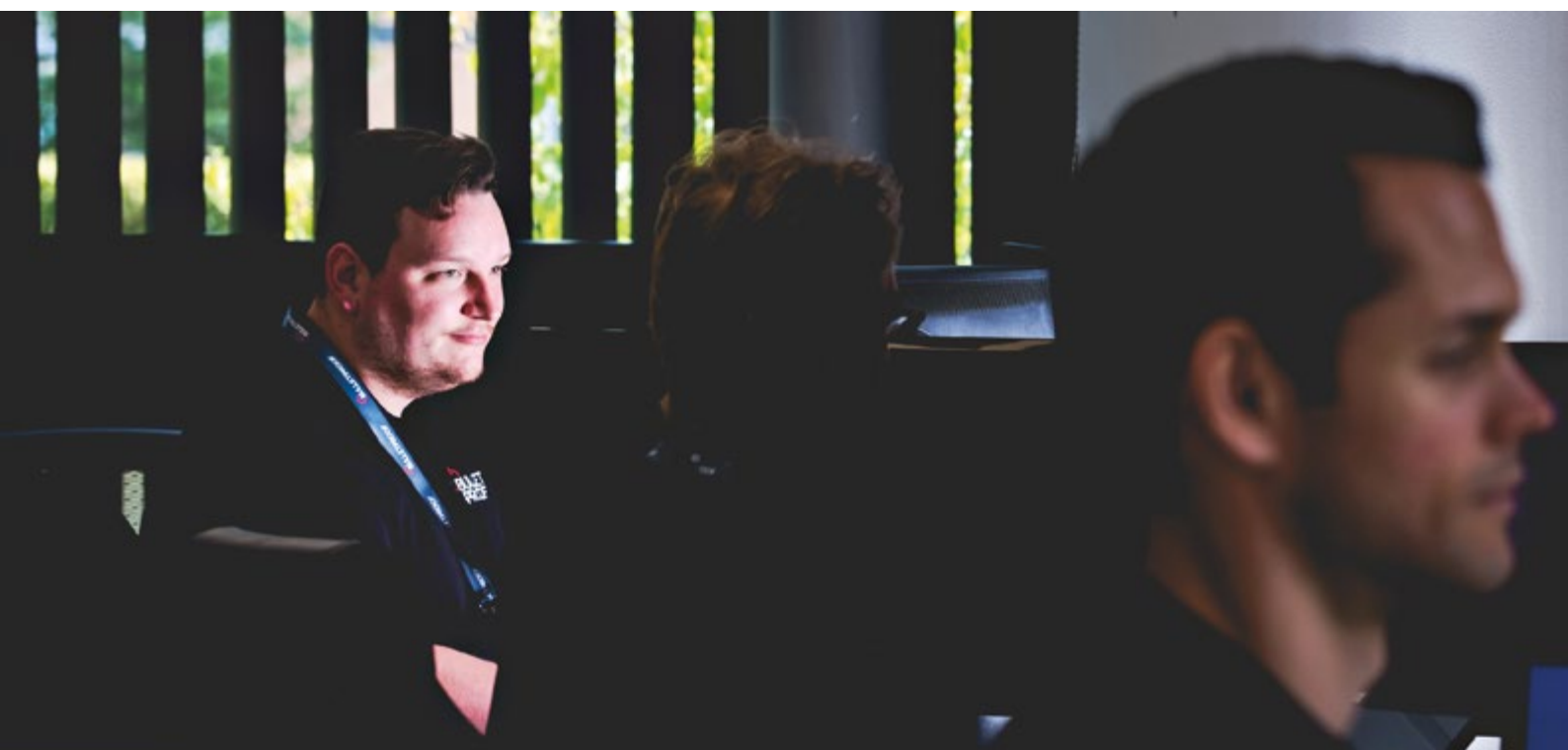
S.W.A.T. DEFENCE® | DRIVEN BY INNOVATION

S.W.A.T. Defence® is delivered from Bulletproof's in-house Security Operations Centre (SOC). The Bulletproof SOC is the command centre of all our cyber security operations and is home to our experienced security analysts and SpecialOps® researchers. Staffed round the clock by qualified, dedicated security professionals, our teams' expertise and experience safeguards your data, every day and every night.

INTEGRATED MACHINE LEARNING

We've engineered our machine learning platform to work smarter, detecting and analysing suspicious behaviour patterns and automatically creating security events within the SIEM. It also feeds actionable intelligence to our security analysts, enabling them to take quick and decisive action.

ROBUST RUNBOOKS

Bulletproof's tailored runbooks build a profile of what normal behaviour looks like for your business, cutting through noise and reducing false positives. Strong security is not one-size-fits-all, so S.W.A.T. Defence® offers customised runbooks on all service tiers.

PROACTIVE THREAT HUNTING

Modern cyber defences must keep pace with an ever-evolving threat landscape and combat new attack vectors. S.W.A.T. Defence® achieves this with a team of specially-trained security analysts who proactively hunt for unknown threats that would otherwise go undetected.

COMPLIANCE SUPPORT

Managing and maintaining compliance with security standards can be a burden, so why not get a helping hand? S.W.A.T. Defence® can implement standard-specific security controls as well as produce custom reports to demonstrate your compliance, including GDPR, PCI DSS, ISO 27001 and more.

24/7 SECURITY EXPERTISE

The Bulletproof Security Operations Centre is staffed round the clock by trained security experts who are on-hand for all security queries. So from simple questions through to incident response and even malware reverse engineering, your Bulletproof team is standing by.

FEATURE SPOTLIGHT: WORKING SMARTER WITH SAAS

ALWAYS THE LATEST PROTECTION

Product innovation is one of our core strengths, with regular enhancements and updates being part of the package. To enable this continuous improvement our cyber protection is delivered on a SaaS model, giving you instant access to new security features as they're released.

SIMPLE PRICING

SaaS delivery means no hardware is required, enabling us to offer a simple node-based pricing structure with no upfront fees. This makes it easy to deploy and scale-up without the need for any CAPEX outlay. S.W.A.T. Defence® is 100% free from restrictive licenses and costly support contracts.

EASY TO MANAGE

Quickly and securely manage your S.W.A.T. Defence® protection, administrate users and generate custom reports through the easy-to-use Bulletproof portal. Or why not build your own reports and dashboards with our handy API?

ENGINEERED IN-HOUSE

Our resilient high-performance SIEM platform was developed in-house and tailored to our customers. With its scalable cloud underpinning, our SIEM can ingest millions of logs per second, return complex searches in milliseconds, and provides powerful dashboarding for our skilled security analysts.
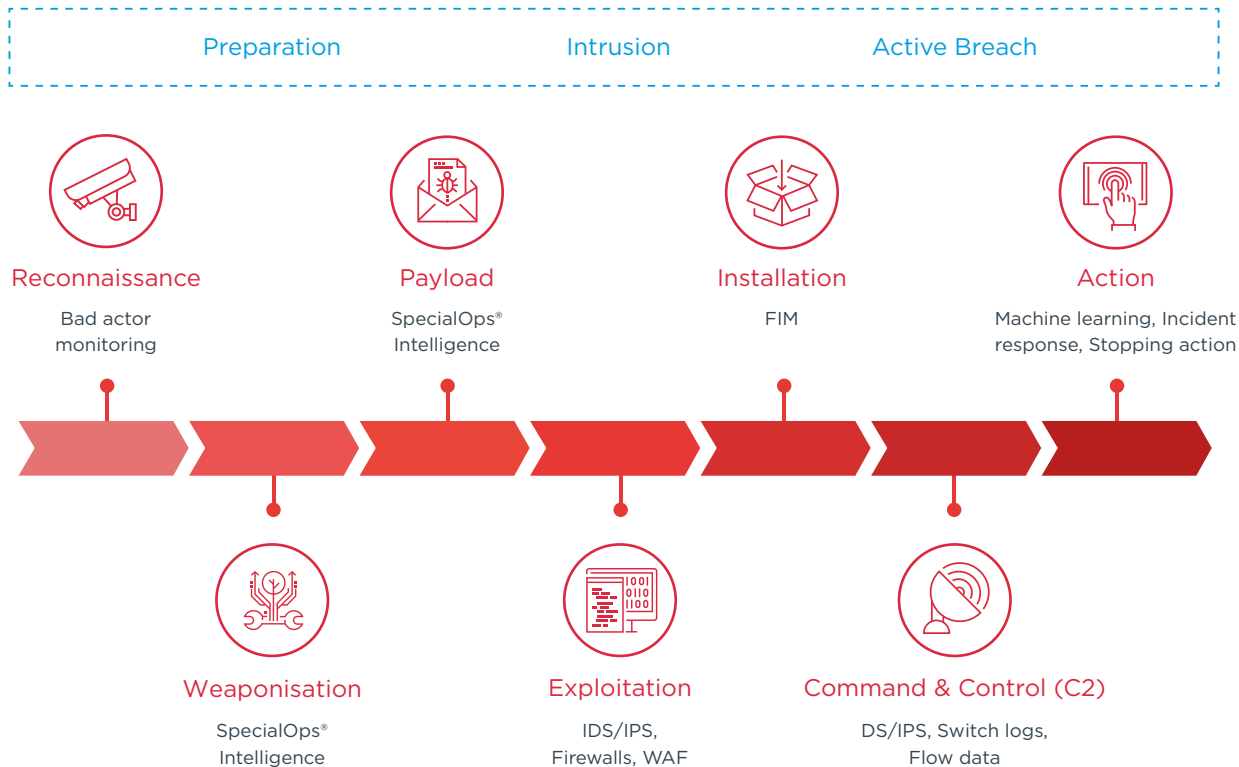
GROWS WITH YOU

With no hardware or licensing limitations, S.W.A.T. Defence® cyber protection scales effortlessly with your business. Bulletproof continuously upgrade the underlying cloud-based infrastructure to ensure cutting-edge performance and security.

COMPLETE KILL CHAIN PROTECTION

Thanks to the versatility of S.W.A.T Defence®, Bulletproof can secure every type of environment by acting at all stages of the cyber kill chain.

Preparation	Intrusion	Active Breach

Reconnaissance
Bad actor monitoring

Payload
SpecialOps® Intelligence

Installation
FIM

Action
Machine learning, Incident response, Stopping action

Weaponisation
SpecialOps® Intelligence

Exploitation
IDS/IPS, Firewalls, WAF

Command & Control (C2)
DS/IPS, Switch logs, Flow data

DEPLOY ANYWHERE, ANYTIME

Bulletproof S.W.A.T. Defence® has been engineered for fast, seamless integration with your infrastructure. Combining our SaaS delivery with a highly automated deployment process leads to a rapid, low-touch setup for both traditional on-premises infrastructure and modern cloud environments. It features native support for public cloud providers including Azure, AWS and Google and is even designed to work effortlessly with container and serverless technologies.

"A highly automated deployment process leads to a rapid, low-touch setup... and is even designed to work effortlessly with container and serverless technologies."

GET IN TOUCH TO BOOK YOUR FREE DEMO

See the power of S.W.A.T. Defence® for yourself with a free demo.
Book your slot today to find out how Bulletproof's next-generation
cyber threat protection delivers real security improvements.

📞 01438 532 900

✉ contact@bulletproof.co.uk

💻 www.bulletproof.co.uk

YOUR BEST DEFENCE AGAINST CYBER THREATS.