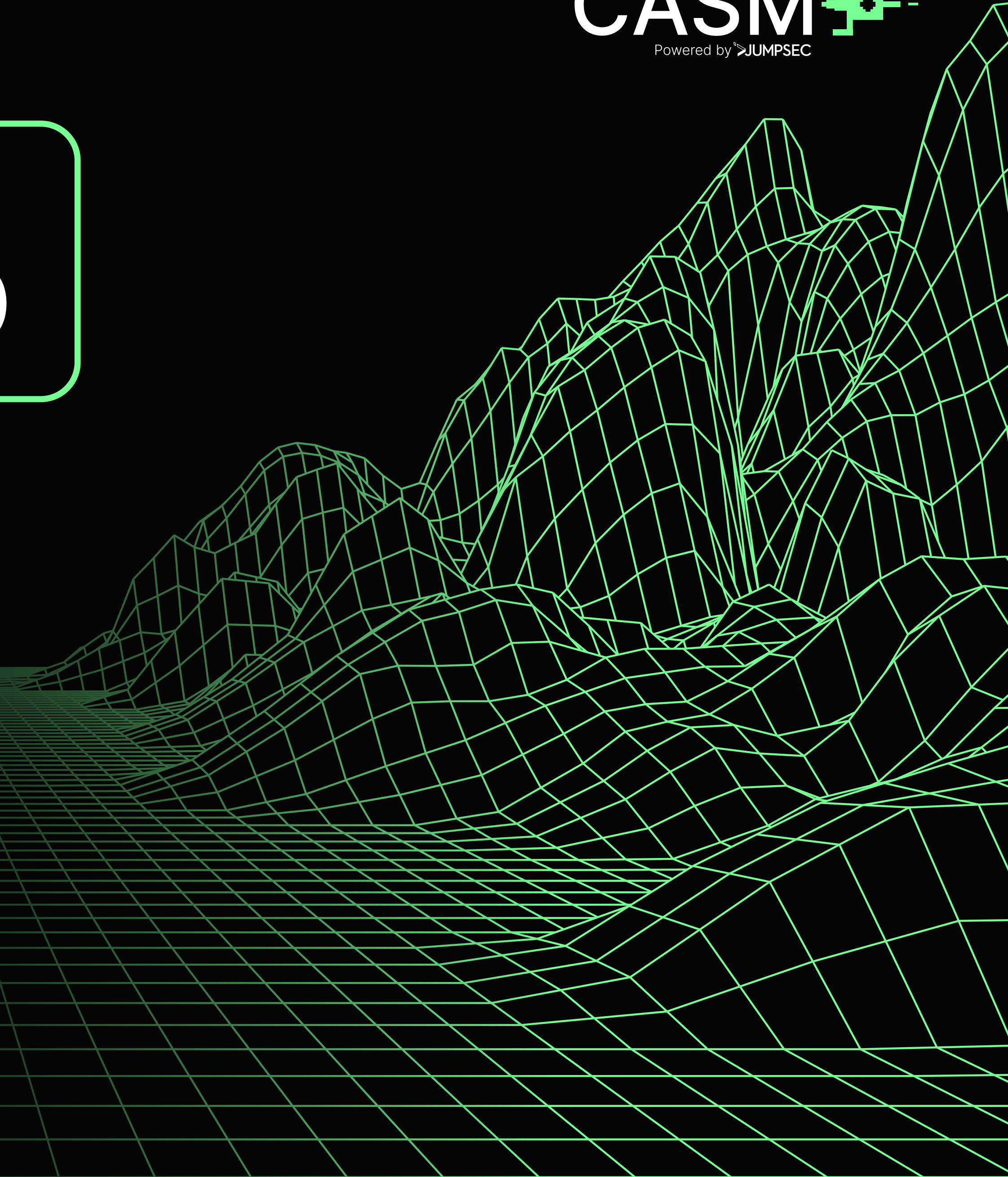CASM

Powered by JUMPSEC

CONTINUOUS ATTACK SURFACE MANAGEMENT (CASM)

UNDERSTAND YOUR ATTACK SURFACE
TO DEFEND YOUR BUSINESS

On average, CASM **alerts clients** to critical vulnerabilities two days ahead of vendor notifications, **enabling faster action**.

Protecting the right assets is becoming more complex as the threat landscape evolves, but with proactive measures, organisations can stay ahead of attackers.

CASM's human expert-in-the-loop service delivers the critical context and protection needed to outpace hackers. Powered by advanced technology and driven by world-class penetration testers, red teamers, threat hunters, defenders, and intelligence experts, CASM combines the best tools and data sets to keep your organisation ahead in the evolving cyber battle.
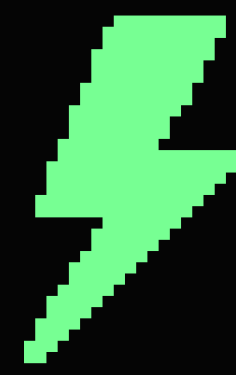
Key Outcomes

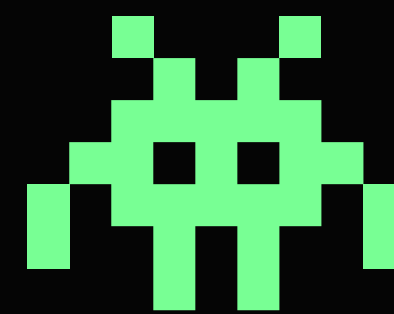**With CASM, you'll know who is targeting your business, why, and how.**

Our team of experts will help you build and implement defensive strategies tailored to your business' unique needs. From proactive remediation plans to immediate takedowns of sensitive data found online:
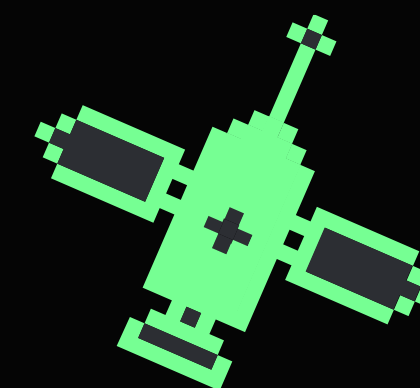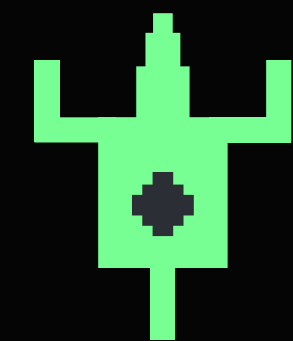
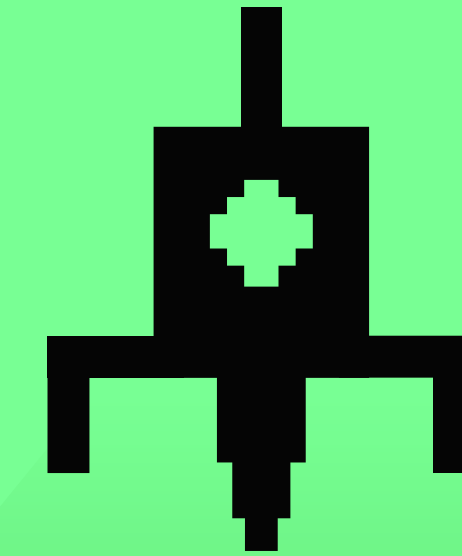**IMPROVED SECURITY POSTURE**

REDUCED RISK OF CYBER ATTACKS

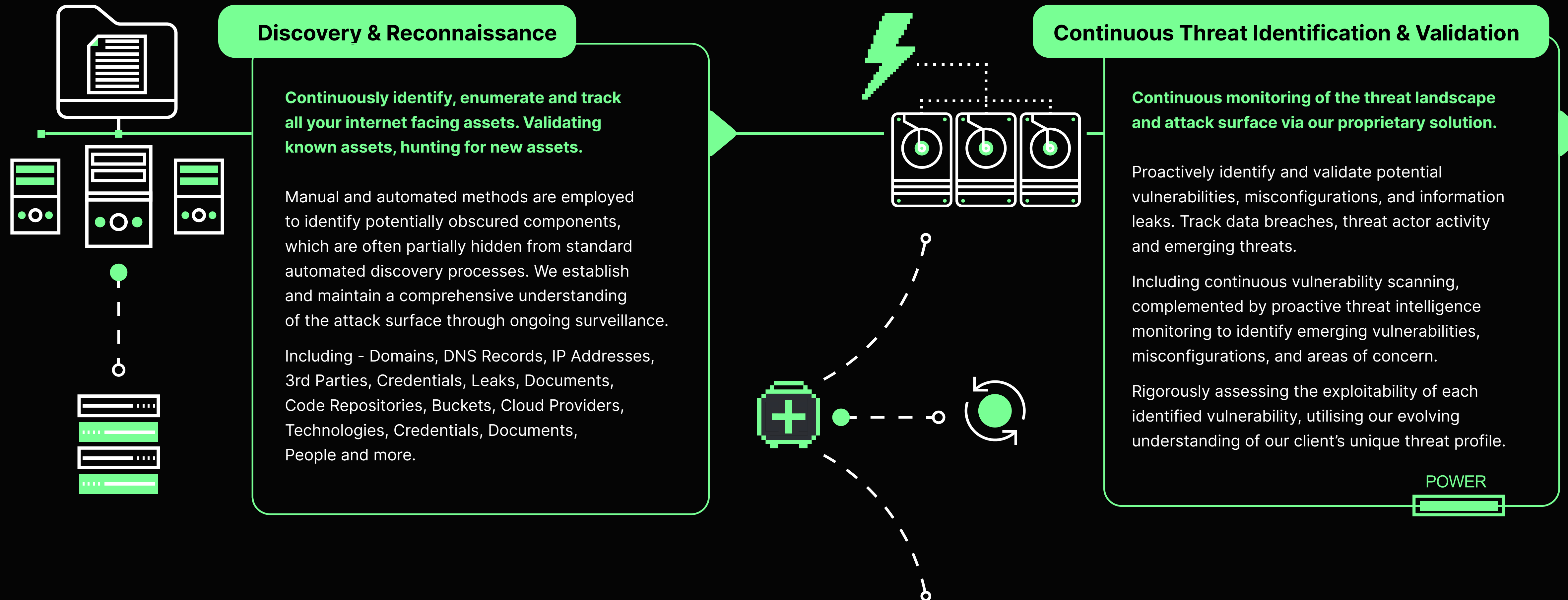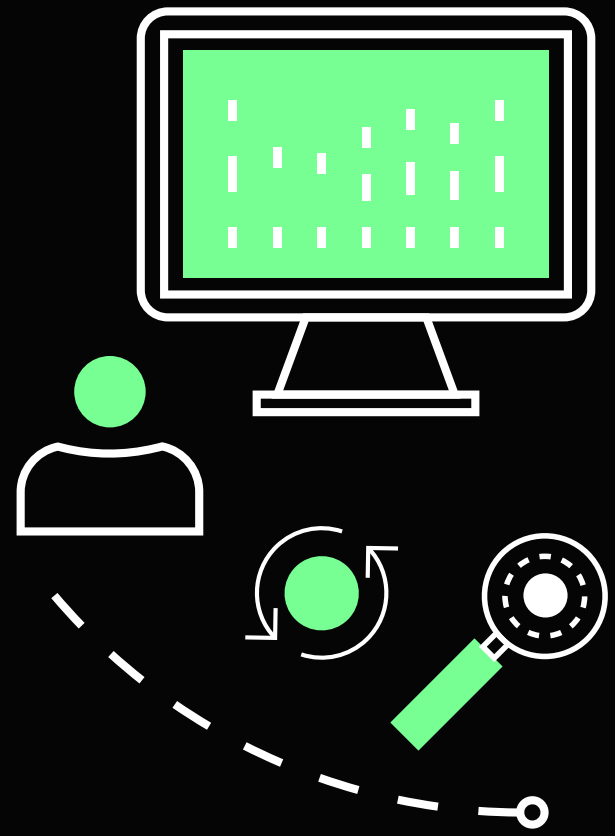**ENHANCED EFFICIENCY**

IMPROVED CONTROL

CONFIDENCE TO THRIVE

How does CASM work?

Modern continuous attack surface management in action - actionable insights to empower security teams.

Discovery & Reconnaissance

Continuously identify, enumerate and track all your internet facing assets. Validating known assets, hunting for new assets.

Manual and automated methods are employed to identify potentially obscured components, which are often partially hidden from standard automated discovery processes. We establish and maintain a comprehensive understanding of the attack surface through ongoing surveillance.

Including - Domains, DNS Records, IP Addresses, 3rd Parties, Credentials, Leaks, Documents, Code Repositories, Buckets, Cloud Providers, Technologies, Credentials, Documents, People and more.

Continuous Threat Identification & Validation

Continuous monitoring of the threat landscape and attack surface via our proprietary solution.

Proactively identify and validate potential vulnerabilities, misconfigurations, and information leaks. Track data breaches, threat actor activity and emerging threats.

Including continuous vulnerability scanning, complemented by proactive threat intelligence monitoring to identify emerging vulnerabilities, misconfigurations, and areas of concern.

Rigorously assessing the exploitability of each identified vulnerability, utilising our evolving understanding of our client's unique threat profile.

POWER

Regular Threat Hunting

Manual hunts, tool enabled hunts, testing hypotheses looking for unknown threats.

Leveraging latest threat intelligence to uncover developing issues before they escalate into active attacks. The CASM team continuously gathers intelligence to assess vulnerability to emerging threats.

Our deep dives into attacker behaviour include monitoring across various platforms, such as social media, the dark web (forums, telegram/private chats, breach data), adversary monitoring, industry and country monitoring, cyber community news, public news monitoring, vendor news allowing us to proactively identify attack vector threats.
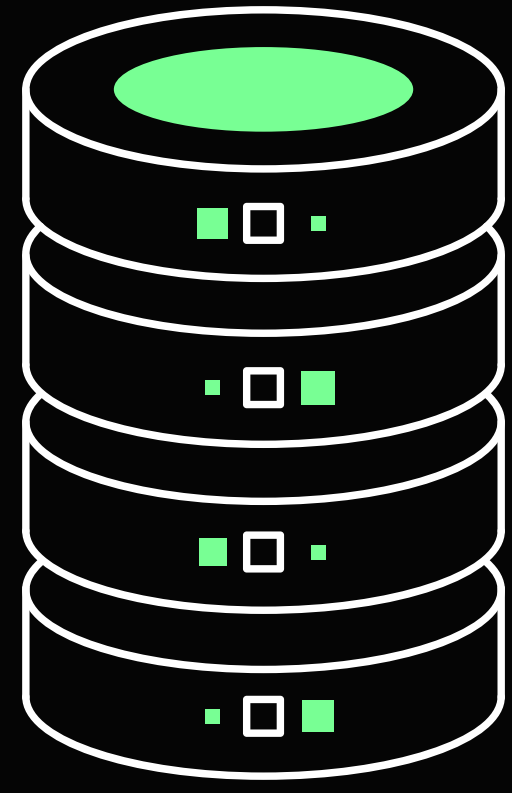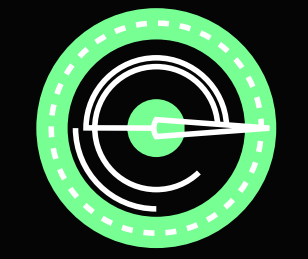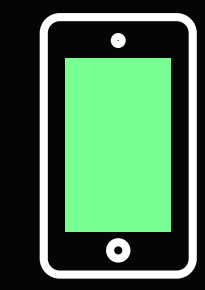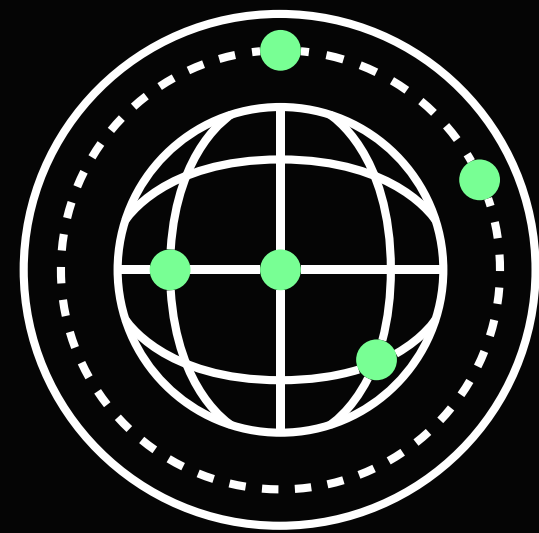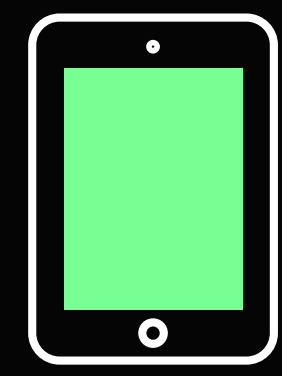
Contextualised reporting

Receive ongoing updates and actionable reports on vulnerabilities by exploitability and threat level, rapid critical alerting and two-way dialogue with our experts.

Remediation and expert support

Managed takedowns and supported recommendations with workarounds provided where global patches or fixes are not available.

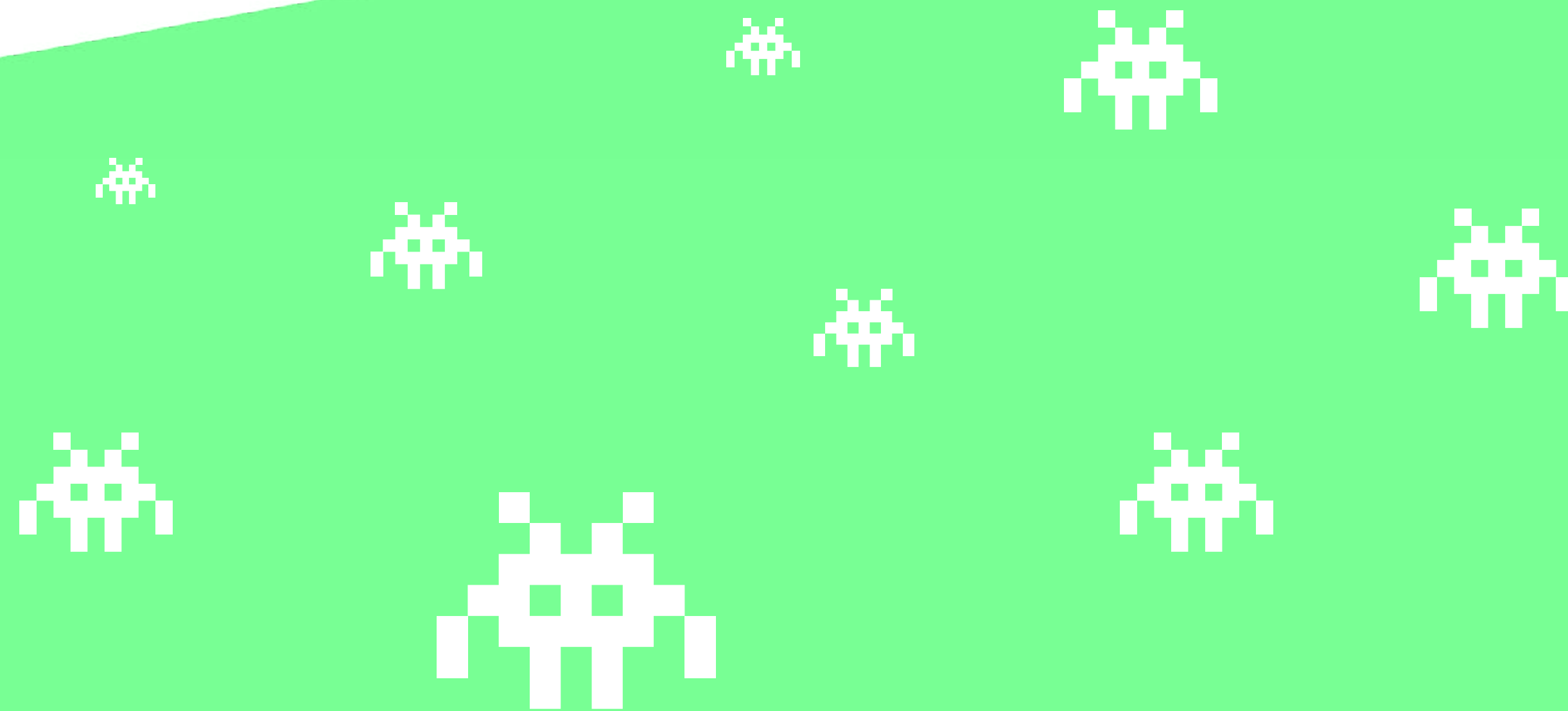# Driven by CASM specialists applying the mindset of attackers.

CASM is driven by world-class penetration testers, red teamers, threat hunters, defenders and intelligence experts.

"

Only experts can connect the dots and decide if findings are significant in the context of the current world of cyber security. Effective use of Threat Intelligence and threat hunting and contextualisation are essential components of a modern attack surface management solution.
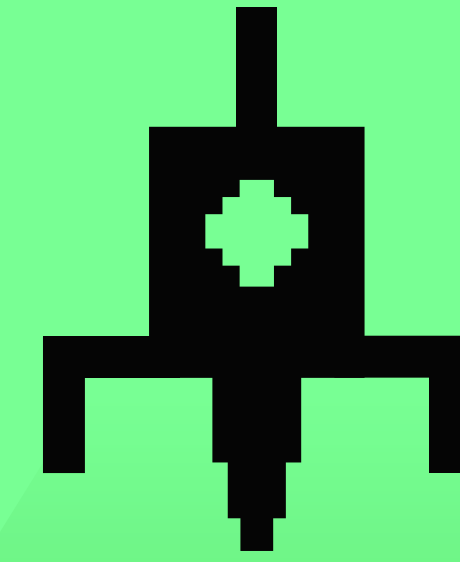
BJOERN SCHWABE, CTO

"

CASM versus the Competition

Monitored Assets	Tenable EASM	Microsoft EASM	Qualys EASM	JUMPSEC CASM	
	Domains	Domains	Domains	**Domains**	**Ports**
	IP Address	IP Blocks	IP Blocks	**IP Blocks**	**DNS Records**
	ASN	Hosts	Hosts	**Hosts**	**SSL Certificates**
	DNS	Email Contacts	ASN	**Email**	**Cloud Buckets**
	Vulnerabilities	ASN	Ports	**ASN**	**Azure Tenants**
		WHOIS Organizations	Technologies	**WHOIS**	**Documents**
			Vulnerabilities	**Credentials**	**Code & Container Repositories**
				Technologies	
				Vulnerabilities	
Uptime Monitoring	Yes	Yes	Yes	**Yes**	
Vulnerability Scanning Included	Yes	No	Yes	**Yes**	
Cyber Threat Intelligence	No	No	No	**Yes**	
Threat Hunts	No	No	No	**Yes**	
Dark Web Monitoring	No	No	No	**Yes**	

Testimonials

"

We engaged with JUMPSEC in an Attack Surface Mapping exercise managed by the **London Office of Technology and Innovation, and found the exercise to be invaluable**. JUMPSEC's CASM team gave us assurance that our organisation was secure and identified areas which needed addressing. The experience with JUMPSEC was excellent.

They were incredibly collaborative in their approach and responsive to our needs, **regular check-ins allowed us to be a part of the exercise**, not just having it delivered to us.

Shared Technology Services will continue to work with JUMPSEC as we feel they're a valuable partner.

**LONDON BOROUGHS OF LEWISHAM,
BRENT AND SOUTHWARK SHARED IT SERVICE**

We work very hard to keep our systems secure, but we also know that **cyber threats are increasing rapidly**.

While we need to defend all of our systems all of the time, the attackers only need to find one gap to be successful.

We need to keep one step ahead of the cyber criminals and **our work with JUMPSEC has shown that this can give us a valuable extra layer of defence**, working proactively to find any potential vulnerabilities quickly and take prompt corrective action.

LOCAL GOVERNMENT CLIENT

As we service our existing customers, and grow to add new customers around the world, **it is critical that our cyber security posture is continuously being monitored** and that it constantly adapts to new and emerging threats.

Having JUMPSEC on-board means we can do this proactively, ensuring we have a real-time view of our attack surface, so that we can instantly respond to any issues that arise.

EAGLE EYE SOLUTIONS

"

CASM
Powered by >JUMPSEC
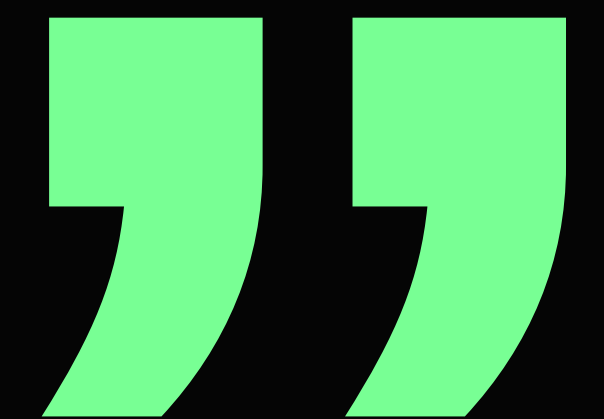
CASM is brought to you by JUMPSEC, the leading UK specialist in both offensive and defensive cyber security.

Over the past 12 years, JUMPSEC has built a reputation for excellence and dedication to service having significantly improved security for hundreds of clients.

JUMPSEC's research is widely recognised and cited in the media, and it has contributed to shaping the UK's national security strategy, particularly in addressing the ransomware threat.

Talk to the CASM team to help safeguard your business
Contact casm@jumpsec.com

casm.jumpsec.com