

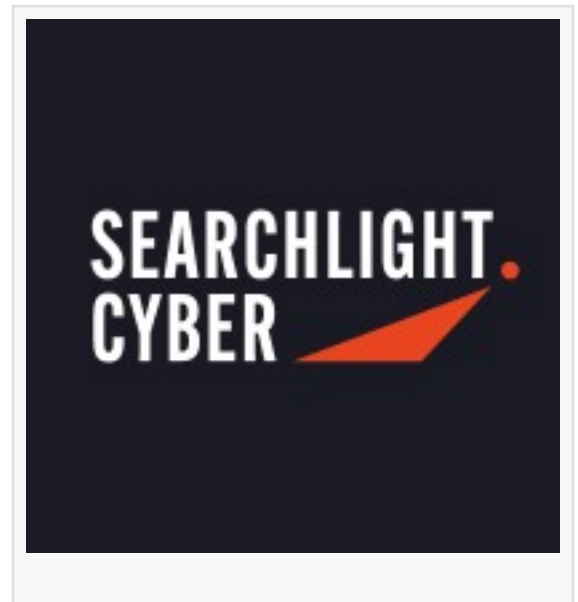
Searchlight Cyber Publishes The Preemptive Cybersecurity Handbook

Book explores the shift to preemptive cybersecurity strategies & provides a practical framework for finding & closing exploitable exposure before attackers act

PORTSMOUTH , UNITED KINGDOM, October 7, 2026
/EINPresswire.com/ --

– [Searchlight Cyber](#) today published [The Preemptive Cybersecurity Handbook](#), a comprehensive resource to help security teams find and fix the exposures that matter before a threat becomes an attack.

The book is available now as a free PDF and EPUB for e-readers, with a physical edition to follow.



The Case for Preemptive Cybersecurity

The window organizations have to act on vulnerabilities is shrinking. Attackers are finding and exploiting vulnerabilities faster, while organizations are managing increasingly complex and constantly changing attack surfaces.

The handbook explores how AI-assisted vulnerability discovery is accelerating this problem, in the hands of both attackers and defenders. By the time a vulnerability is publicly disclosed and enters the conventional vulnerability management process, attackers may already have had a significant head start.

With no time to react, security teams need to focus on reducing the exposure window: the time between an exposure existing and that exposure being closed or exploited, earlier in the attack lifecycle.

From Reactive Security to Preemptive Defense

The Preemptive Cybersecurity Handbook helps security leaders translate preemptive cybersecurity into an operating approach they can apply within their own organizations. It outlines the foundational capabilities of understanding the organization's true attack surface and applying real-world attacker context, with practical guidance on how teams prioritize risk, take

action and verify that exposure has been reduced.

At its core is Preemptive Threat Exposure Management (PTEM), Searchlight Cyber's operating model that brings together continuous exposure discovery, exploitability validation and real-world attacker intelligence. The shift also requires changes beyond technology: how teams measure progress, make decisions and organize around reducing exposure.

"Finding an exposure is only useful if you can do something about it" said Michael Gianarakis, CEO of Searchlight Cyber. "Security teams need to know whether it is exploitable, what attackers could do with it, and how to fix it before exploitation. The time available to act is shrinking, so organizations need to be able to focus on the threats that matter and rapidly remediate with confidence. This handbook sets out how organizations can put that into practice, from identifying and validating exposure to prioritizing action and confirming that the exposure window is closed" he continued.

The Core Pillars of Preemptive Cybersecurity

Readers will gain an understanding of the key capabilities and practices that underpin a successful preemptive security posture:

Exposure Visibility: Knowing the organization's true external attack surface and continuously identifying assets and exposures that could provide attackers with an entry point.

Attacker Reality: Understanding what attackers are actually doing, including activity across criminal forums, marketplaces, credential exposure, targeting behavior, and exploitation activity.

Preemptive Action: Combining exposure visibility with attacker intelligence to determine which risks demand action, and rapidly remediating exposures before attackers can take advantage of them.

Inside the Book

The book combines the central ideas of preemptive cybersecurity with original research, case studies and practical resources designed to be useful long after the first read.

The new zero-day race: Searchlight Cyber Chief Security Research Officer Shubham Shah examines how frontier AI models are changing vulnerability research. The cPanel case study shows the implications in practice: AI helps defenders accelerate research, but threat actors are able to utilize the same capabilities and fewer constraints. The chapter explores how the traditional lifecycle of vulnerability discovery, disclosure and exploitation is being compressed, and what that means for defenders.

The Practitioner's Guide to the Dark Web: Building on the success of Searchlight Cyber's 2023

and 2024 editions, the book includes a guide to the cybercriminal ecosystem, covering hacking forums, dark web marketplaces, ransomware infrastructure and the signals they can provide about attacker activity.

The Preemptive Cybersecurity Maturity Model: A practical framework for assessing an organization's current capabilities across ten dimensions, from discovery and validation to attacker awareness, speed of action, metrics and organizational integration. Five stages map the journey from reactive security through to preemption.

The Preemptive Security Buyer's Guide: Practical guidance for evaluating the capabilities and technologies needed to build a preemptive security program.

Additional chapters turn to the role of security leaders in building a preemptive organization; from changing how teams prioritize and measure risk to creating the culture, processes and accountability needed to act on threats before they become incidents.

"The threat environment is changing faster than traditional security processes can keep up. Preemptive security is about utilizing what little time organizations have to act before an attacker does." Gianarakis concluded.

The Preemptive Cybersecurity Handbook is available now as a free PDF and EPUB download for e-readers. A physical edition will follow.

[Read The Preemptive Cybersecurity Handbook](#)

About Searchlight:

Searchlight Cyber is a preemptive cybersecurity company helping organizations reduce exploitable exposure before attackers act. Its Preemptive Threat Exposure Management (PTeM) platform combines continuous attack surface visibility, exploitability validation, pre-disclosure security research, and real-world attacker intelligence, enabling security teams to identify and prioritize the threats that matter most. Founded in 2017 with a mission to stop criminals acting with impunity, Searchlight is used by some of the world's largest enterprises, government and law enforcement agencies, and managed security service providers.

Find out more at www.slcyber.io or follow Searchlight Cyber on LinkedIn and X.

Tom Duncan
Searchlight Cyber
t.duncan@slcyber.io
Visit us on social media:

[LinkedIn](#)

[X](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/947964959>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.