JUMPSEC

# ATTACK SURFACE MANAGEMENT IN ACTION ENHANCES NINE CLIENTS SECURITY POSTURE

Company: **Nine local authorities**
Country: **UK**
Industry: **Local Authorities**
Solution: **Attack Surface Management**

## Summary

In March 2023, the group began discussing its unique requirements. The aim was to understand and benchmark the risk of cyber attacks to London local authorities, on both an individual borough level and as a group to reflect the broader status of cyber-threat to all London local authorities.

JUMPSEC designed and delivered a collaborative security project working across nine client organisations in partnership, to collectively enhance their security posture by identifying exploitable vulnerabilities across their shared attack surface.

## The Challenge

JUMPSEC presented an approach that leveraged our experience of attacker simulations to view the participating boroughs' attack surface as an attacker would, and move beyond automated tooling to chain low- and medium-risks together to emulate real-world attacker behaviour. This approach enabled the boroughs to prioritise the risks with the highest return on investment for them, adding context and clarity to the never-ending list of vulnerabilities so many organisations face today.

A concern for many organisations, in both the public and private sectors, is where they sit in relation to their peers. In addition to individual recommendations, JUMPSEC aggregated the findings from all participating boroughs and produced a report that indicated key trends in identified vulnerabilities, whether that be across common technologies or network architecture. This allowed boroughs to contextualise their results alongside their peers and JUMPSEC facilitated conversations between boroughs with shared challenges, enabling knowledge sharing and inter-borough relations.

# Phased Approach

JUMPSEC's approach was tailored to closely meet the borough's needs and was chosen to partner with the nine local authorities for this exciting project. The project was tailored and delivered over the following phases:

**Mapping of the external attack surface** by identifying internet-facing information assets, encompassing infrastructure directly owned and controlled by the clients, third-party suppliers, and information outside the organisation's control which could be leveraged by an attacker (e.g., breach data dumps, information on dark web forums, and typical forms of OSINT (such as unintentionally exposed data by employees and subcontractors).

**Analysis of the issues** identified to create several test cases, determining the likelihood and impact of an attacker leveraging the issue by considering several factors such as the innate risk of the issues identified, compounding factors such as the likelihood of an issue leading to the discovery and exploitation of further vulnerabilities (chaining), and signs of exploitation or exploit code in the wild.

**Execution of a large number of scenario-driven test cases** to validate whether the issues identified present an actual risk in context, based on whether it can be practically leveraged to facilitate the compromise of information or resources, or otherwise breach the perimeter to enable further attacks on the network to take place.

**Internal scenario-driven testing** from an initial foothold on the network (informed by successful test cases from the previous phase) to validate the ability for an attacker with standard levels of user access to move laterally, elevate privileges, and achieve further compromise of information or resources, measuring the efficacy of prevention, detection, and response controls.

## Our approach identified 1400 vulnerabilities yet only 1% were critical

JUMPSEC's approach identified several key improvement areas for the clients whilst ensuring that the scope of recommendations was controlled so as not to overwhelm or create unnecessary overheads with limited security value.

To illustrate this, whilst JUMPSEC identified over 1400 instances of vulnerability, only 3% were found to be leverageable as part of an attack. Further, less than 1% were deemed to be critical. This was valuable feedback for the boroughs who were then able to target their resources to that 1-3% with a verified and evidenced business risk.

## An automated approach would have enrolled 66% of issues lacking context

In contrast, a purely automated approach without context-driven vulnerability classification would have enrolled 66% of the issues into the vulnerability management system for remediation, despite the fact that they posed minimal business risk. This exemplifies the challenge facing so many organisations as tools produce overwhelming vulnerability reporting, resulting in individual burnout and wasted resources as infosec teams struggle to translate automated outputs into a prioritised security roadmap.

## Continuous Attack Surface Management has been implemented

The service has now been implemented as an ongoing managed service to continually monitor the attack surface, probing signs of potential vulnerability to determine exploitability in the context of an attack as the network changes and new adversarial exploits and TTPs emerge over time. This approach significantly reduces the window of opportunity for a threat actor to take advantage of change in an organisation's Attack Surface and removes the burden from InfoSec teams to quickly respond to zero-days and other critical, time-sensitive security alerts.

> We engaged with JUMPSEC in an Attack Surface Management exercise managed by the London Office of Technology and Innovation, we found the exercise to be invaluable JUMPSEC gave us assurance that our organisation was secure and identified areas which needed addressing. The experience with JUMPSECS 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. We will continue to work with JUMPSEC as we feel they're a valuable partner.
>
> Lewisham, Brent,
> Southwark Shared IT Services

## About Attack Surface Management

JUMPSEC Attack Surface Management (ASM) is a human-led technology-enabled service that complements traditional methods of security assurance by providing a balance between 'wide and shallow' vulnerability scanning and 'narrow and deep' penetration testing. ASM enables JUMPSEC clients to think and act like a real-world attacker, probing their network to assess the exploitability of the vulnerabilities present - i.e. whether they can be practically leveraged by an attacker to cause harm. Our service is built around expert advice, delivering positive outcomes to strengthen your organisations attack surface.

> 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

Jumpsec helps leading organisations solve complex cybersecurity problems to enable your organisation to have effective cyber security.

**jumpsec.com**