ADVANCED CYBER DEFENCE SYSTEMS

A CISO’s Guide to ASM

Elliott Wilkes and Paige Mullen

Table of Contents

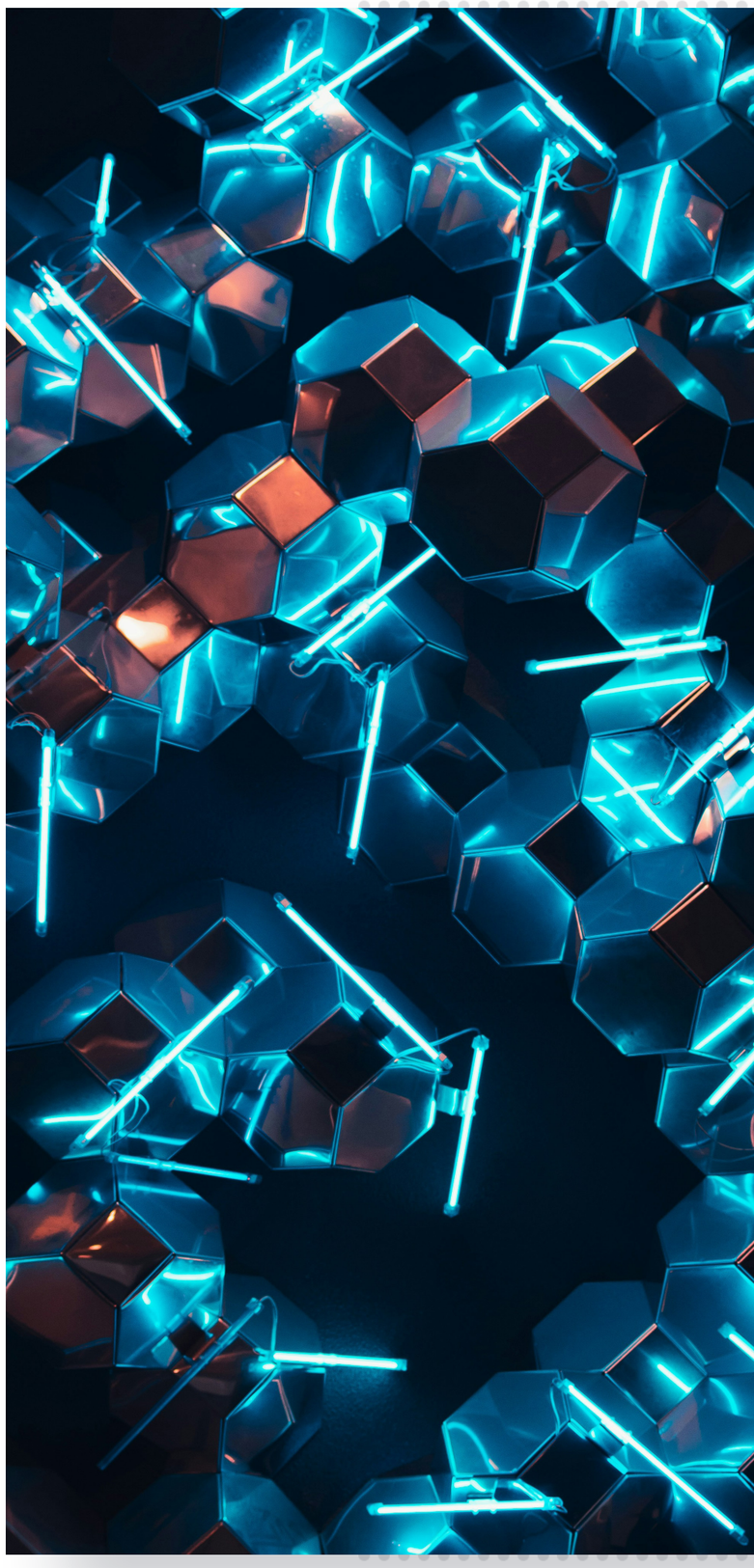
What is attack surface management?

Attack surfaces are evolving.

In simple terms, an attack surface refers to all the entry points and internet-facing assets of an organisation’s IT infrastructure that can be vulnerable to an attack. It is the areas of an organisation that can be compromised. From an attacker’s viewpoint, they will try to discover any weaknesses and vulnerabilities across your organisation. Once they identify any flaws that can be exploited, they will use them to gain unauthorised access to your business and cause harm. It is crucial to be aware of your attack surface so that you can take necessary measures to reduce the risk of an attack and safeguard your business.

75% of employees will acquire, modify, or create tech outside of IT teams’ visibility by 2027. (Gartner)

With the rapid proliferation of cloud providers, software, web properties, remote devices, and more, it is becoming incredibly challenging for security teams to identify risks and take action. As an organisation’s attack surface is constantly evolving, its security team needs access to a comprehensive and highly contextualised data feed for security analysis at scale.



CISO concerns with their attack surface

The expanding attack surface is a worry for CISOs; in combination with advancing threats, readily available tools and artificial intelligence are creating more opportunities to exploit vulnerabilities within an organisation’s attack surface.

There can be a lot of unnecessary time manually spent tracking inventory assets and evaluating their risks; this is incredibly time-consuming for SOC teams and can often be inaccurate. Statistics show that there is a high percentage of assets that are unknown within an organisation; therefore, an automation process is required for optimum security.

30% of assets are unknown or unmanaged because of fast digital transformation. (Forrester)

CISOs are more concerned about their attack surface due to the Covid-19 pandemic and the increase in remote work, which they believe, has significantly increased their risk of attack. Alongside increased digitalisation, attack surfaces continue to expand, leaving those in charge of cybersecurity struggling to keep up with the constant evolution.

CISOs need to be proactive, rather than reactive, which will not only aim to prevent cyber attacks but also save time and money. For a CISO, one of the most negative impacts of a cyber attack is the downtime and remediation associated with the attack; therefore, proactive methods to protect their attack surface are vital.

What are the dangers of shadow IT and rogue assets?

Shadow IT

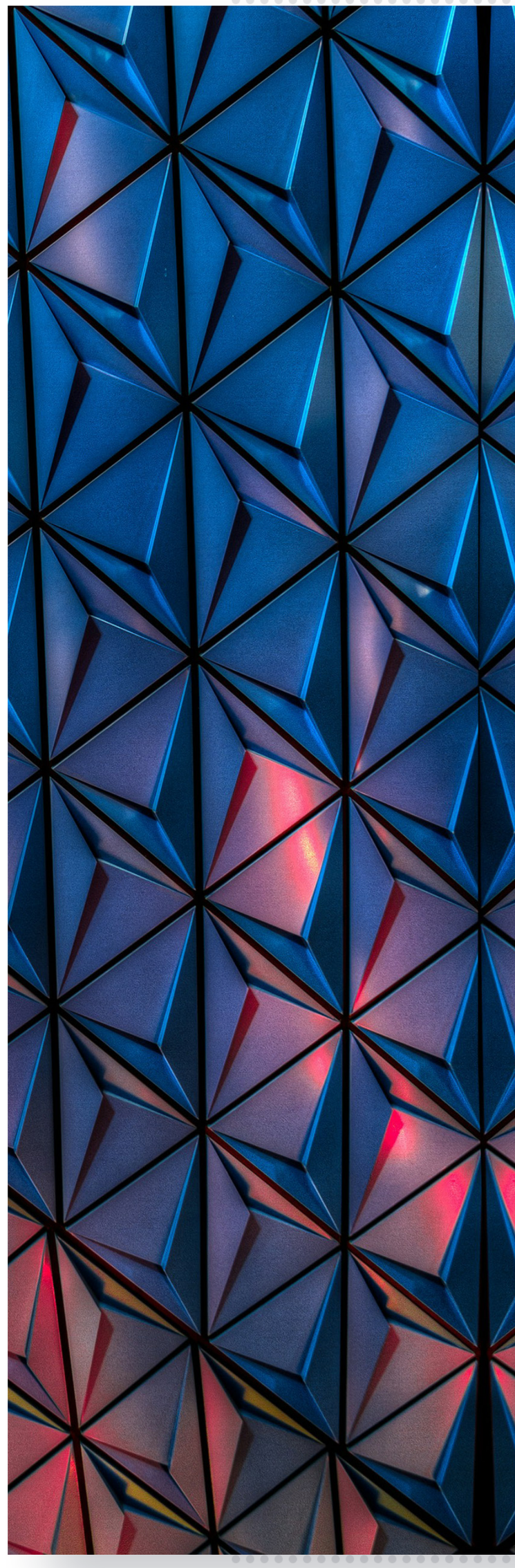
Shadow IT, otherwise known as ‘unknown assets’, refers to the systems, software, or applications that are not supervised by the IT security team. It can also include any assets that the security team is unaware of or failed to secure. These types of assets can pose a severe threat to an organisation as they can be exploited by attackers to gain unauthorised access to sensitive information.

Rogue Assets

These assets are malicious infrastructure, such as malware. They’re assets that are connected to a network with no authorisation, but they differ from unknown assets as they are known to the organisation. As they are not included in the company’s inventory list, they are difficult to detect and manage, posing a significant security risk.

What does an effective attack surface management tool look like?

When looking for an effective Attack Surface Management (ASM) tool, keep an eye out for these features and functions.



ASSET DISCOVERY

The tool should enable you to view your entire external attack surface, keeping your asset inventory up-to-date. A continuous whole-internet scanning engine will regularly scan thousands of ports, with the top ports most likely to be used for nefarious purposes scanned with more detail and frequency. This massive scanning apparatus and intelligence engine gives you an unparalleled advantage over cyber criminals, ensuring you can spot and manage rogue assets and shadow IT when they emerge, stay on top of misconfigurations and better protect your ever-evolving attack surface.

COMMON VULNERABILITIES & EXPOSURES (CVE) FLAGGING

An ASM tool that flags CVEs is important for mitigating risks of attack proactively.

Why is this important?

Cisco disclosed two CVEs (CVE-2023-20198 and CVE-2023-20273), which impacted the Cisco IOS XE User Web Management Interface. The vulnerabilities enabled malicious actors to gain control of the affected system by creating an account with privilege level 15 access and installing a malicious implant to the disk of a device.

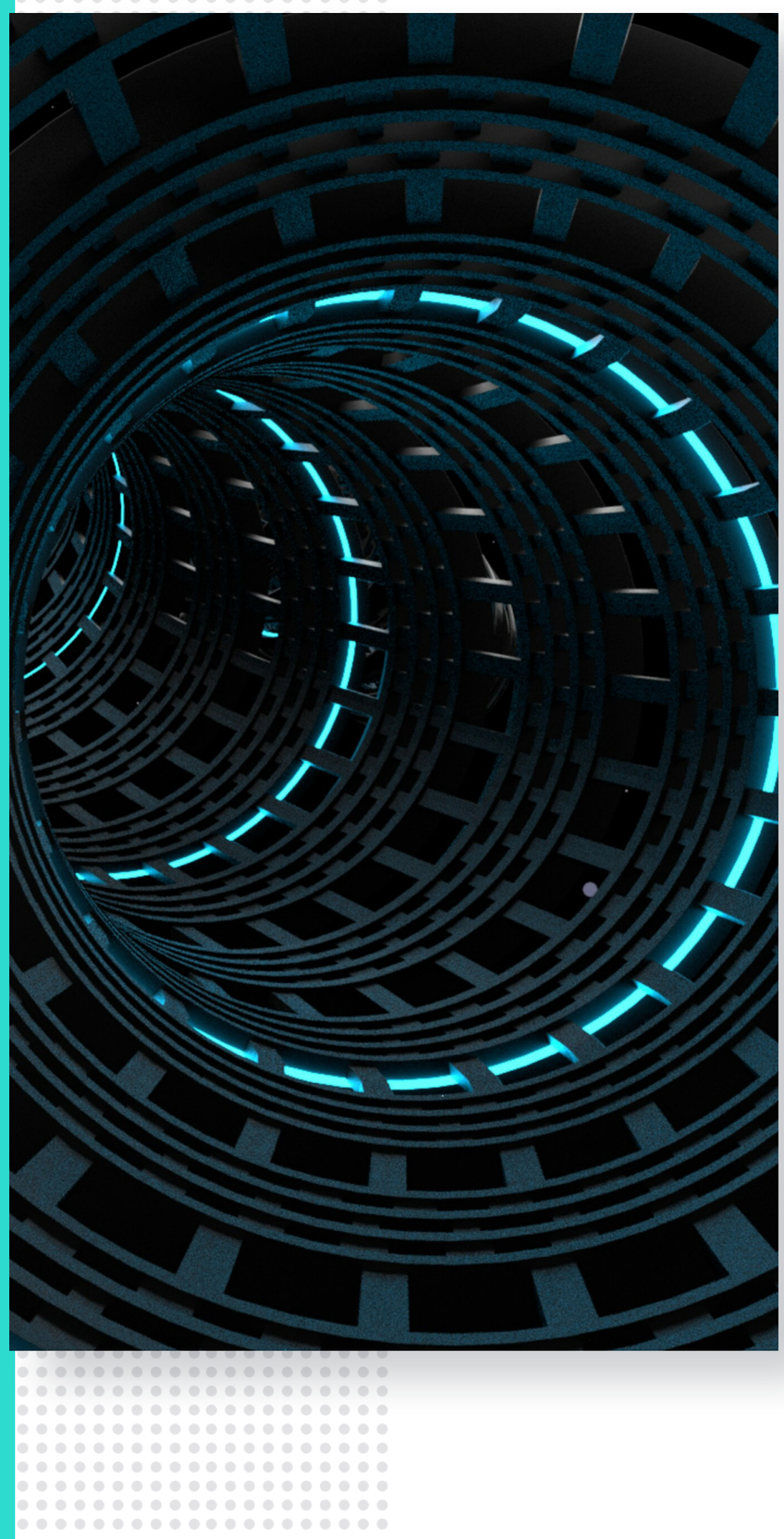
An Attack Surface Management tool that flags CVEs will enable a security team to rapidly discover and remediate any assets that have been compromised.

RISK SCORING

Risk scoring of vulnerabilities, weaknesses, and anomalies for rapid triage, combining industry-standard scoring with new predictive scoring methods (CVSS, EPSS).

What is a CVSS score? CVSS stands for the Common Vulnerability Scoring System. CVSS generates a score from 0 to 10 based on the severity of the vulnerability. A score of 0 is less significant than the highest score of 10.

What is an EPSS score? EPSS (Exploit Prediction Scoring System) measures how likely a particular vulnerability is to be exploited in the wild. A score of 0% is the lowest probability score, and a score of 100% is the highest probability that a vulnerability will be exploited.



RISK PRIORITISATION

An effective Attack Surface Management tool will prioritise vulnerable assets to ensure that security teams focus on the vulnerabilities most critical to their organisation.

Using a combination of CVSS and EPSS scores, an ASM tool should flag critical CVEs and prioritise the CVEs that are most likely to be exploited in the wild.

Security teams may not have the time to fix all vulnerabilities in a timely manner; therefore, knowing which ones are most likely to be exploited in a prioritised list reduces an organisation’s risk in the most efficient way.

ADVANCED SOFTWARE AND DEVICE FINGERPRINTING

For maximum device identification, we incorporate the industry-standard Open Source nmap and recog CPE fingerprinting databases, supplemented with proprietary methods for specific configuration searches.

Recog is a framework for identifying products, services, operating systems, and hardware by matching fingerprints against data returned from various networks.

EASY-TO-USE USER INTERFACE

A user interface that is simple and easy to use for the end-user is essential when it comes to choosing an ASM tool. The user interface should display professional and streamlined business reporting that is intuitive.

Why should businesses prioritise attack surface management (ASM)?

Cyber attack threats are constantly growing, and businesses must prioritise Attack Surface Management to mitigate this risk. By monitoring and reducing the attack surface, attackers will have fewer opportunities to find vulnerabilities and weaknesses to exploit, reducing the likelihood of an attack.

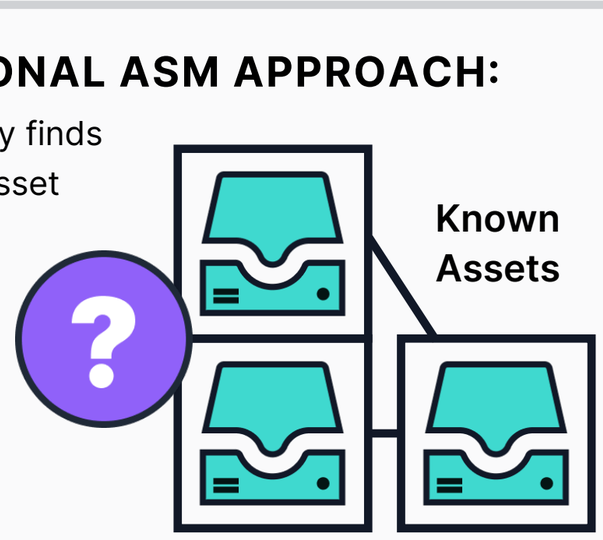
The cyber threat landscape is continuously evolving and will continue to do so. An emerging trend we began seeing in 2023 was the rise of edge security. As organisations expand their digital presence, the number of internet-facing assets also increases. These edge devices are difficult to track and secure, thus making it challenging to protect the organisation’s attack surface. Malicious actors are finding edge devices an attractive target to break into organisations.

Identifying and minimising the attack surface can help reduce the overall risk of cyber threats. Understanding these potential entry points from an attacker’s perspective is a proactive way to reduce risk. An ASM tool can help manage resources more efficiently, allowing the security team to focus on the most critical vulnerabilities and avoid wasting time on unnecessary areas. Ultimately, an attack surface management solution will reduce the likelihood of a cyber attack, which, in turn, will increase brand and reputation protection, and organisations won’t have to face the financial loss of an attack.

Why choose ACDS’ solution to manage your attack surface?

CONVENTIONAL ASM APPROACH:

Limited view only finds **one** additional asset



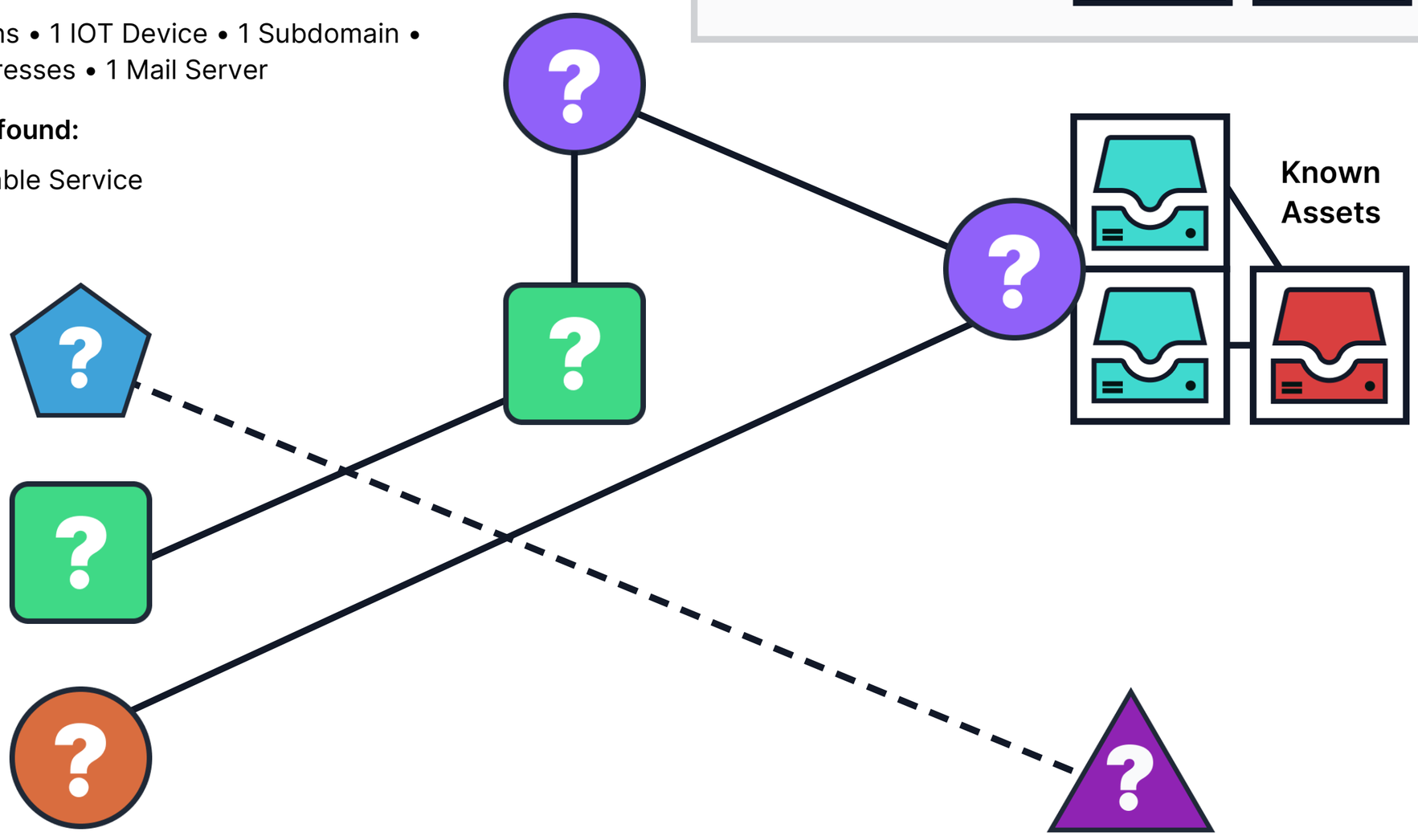
ACDS ASSET DISCOVERY:

Adds seven assets to your baseline:

2 Domains • 1 IOT Device • 1 Subdomain • 2 IP Addresses • 1 Mail Server

We also found:

1 Vulnerable Service



ACDS combines multiple massive data sources to feed its powerful anomaly detection engine, picking up configuration errors and vulnerabilities that often go undetected by others. Regular monitoring of an organisation’s external attack surfaces for changes and new assets will alert of any weaknesses or vulnerabilities that might be exploited.

Our advanced detection model helps to discover, identify and monitor the entirety of your attack surface. Combining the power of data science and analytics, we deliver a highly vetted list of vulnerabilities and their critical risk factor to ensure prompt action and tracking.

Organisations can see results instantly after deploying ACDS’ Attack Surface Management tool.

Compared to conventional ASM tools that have a limited view of an organisation’s assets, ACDS’ asset discovery is incredibly advanced, providing a number of additional assets to your baseline.

You can see from the above diagram that a conventional ASM approach is likely to only find one additional asset during the discovery phase, compared to ACDS’ ASM tool, which has such rich metadata that a web of related assets can be discovered in this same phase.

ASM Case Study

How ACDS identified an unknown vulnerability for a global financial services company with its ASM solution.

AT A GLANCE

Challenges

- Discovering unknown assets
- Keeping full attack surface in view
- Finding actionable insights amongst vast sea of data

The Solution

- Continuous review of the attack surface using extensive data discovery tools
- Highly tuned Risk Prioritisation
- Ongoing attack surface monitoring

The Results

- Team alerted of unknown assets as soon as they are discovered
- Decrease in attack surface
- Analytics to show progress

THE COMPANY

A large global financial services company.

THE CHALLENGE

The company was only alerted to a potential vulnerability after ACDS conducted an analysis of their external attack surface. An old office network device that had been sold on to a third party was still beaconing to the old network and so could be identified as an ‘open door’ to a potential cyber-attack.

Financial services are attractive targets for cybercriminals due to the possibility of high financial rewards. Large organisations struggle to keep track of all assets and require a solution to detect known and unknown assets, keeping their full attack surface in view.

There is a vast sea of data available, but it is essential to find actionable insights among this data to effectively protect the organisation from an attack.

THE SOLUTION

Extensive data set

Our experienced data analysts flagged this vulnerability after reviewing multiple internet-scale data sources.

Risk Prioritisation

With a combination of in-house expertise and ML algorithms, we identified a highly vetted list of vulnerabilities to flag as top priorities to the customer.

Attack surface monitoring

Focused on a highly-tuned, human-trained detection system for lower false positives, giving higher confidence in deploying staff for remediation.

ASM Case Study

THE RESULTS

The organisation could see immediate results after selecting key seed data.

In this case, the quick action enabled the customer to shut down the asset immediately, preventing a potential data breach or other malicious attacks.

The time lag between asset discovery and risk assessment was minimised to hours, compared to days or weeks, from other solutions.

Now, with careful ongoing monitoring, the customer can decrease the vulnerabilities exposed in its external attack surface by removing assets not in use, or not required.

Using analytics provided by the tool, customers are able to monitor progress and present a decrease in potential vulnerabilities that could be exploited, to various stakeholders throughout the organisation.

> The underlying technology in our products is infused with the same design and engineering and code that underpins critical security systems in use across the UK government.
>
> We are confident that our ASM solution, with access to more and different data sets, is making our solution uniquely powerful amongst ASM competition.

Elliott Wilkes
CTO, Advanced Cyber Defence Systems

Conclusion

In conclusion, Attack Surface Management is something that should be prioritised by all organisations. It is a crucial tool in the ever-evolving landscape of cybersecurity, and with increased digitalisation continuously expanding the attack surface, organisations need to do their utmost to stay one step ahead of the attackers.

By introducing this type of automation to discover assets, an ASM solution allows an organisation to find unknown assets that they likely would not be able to find when manually creating an inventory list. Discovering and monitoring these unknown assets gives an organisation a hacker’s view of their attack surface, allowing them to remediate vulnerabilities before they are exploited.