

A Journey into the Smart Vulnerability Management War Room



Introduction – A Peak Inside the War Room

Throughout the Edgescan Thought Leadership series, we have been looking at innovative ways for the Enterprise to exercise “Smart” approaches to managing their Vulnerability Management (VM) and Attack Surface Management (ASM) programs. We have seen the benefits of a full Stack VM program leveraging a hybrid model with human validation and remediation expertise all integrated into one single platform – and communicated on only one single touchstone of truth. In this paper, we turn our focus inwardly - specifically to the Edgescan Platform itself and environment of the Expert Security Consultants and take a virtual tour through the optimal “War Room”. We lead with a provocative question – what if you, the CISO, had the ability to create the ideal war room to make your enterprise secure? Well as we shall see – the founders of Edgescan not only poised to answer this provocative question – they actually built the solution. Let’s take a dive into their war room and learn from their example.

Back to the Future – 2014

The initial idea and start of the prototype started in 2014 and the first viable version was created a year and half later in 2016 and the first enterprise-ready version was launched in 2017. And so while it took three years to build the solution, it was over 30 years of combined in-the-trenches Enterprise security consulting of both founders that fueled the entire approach.



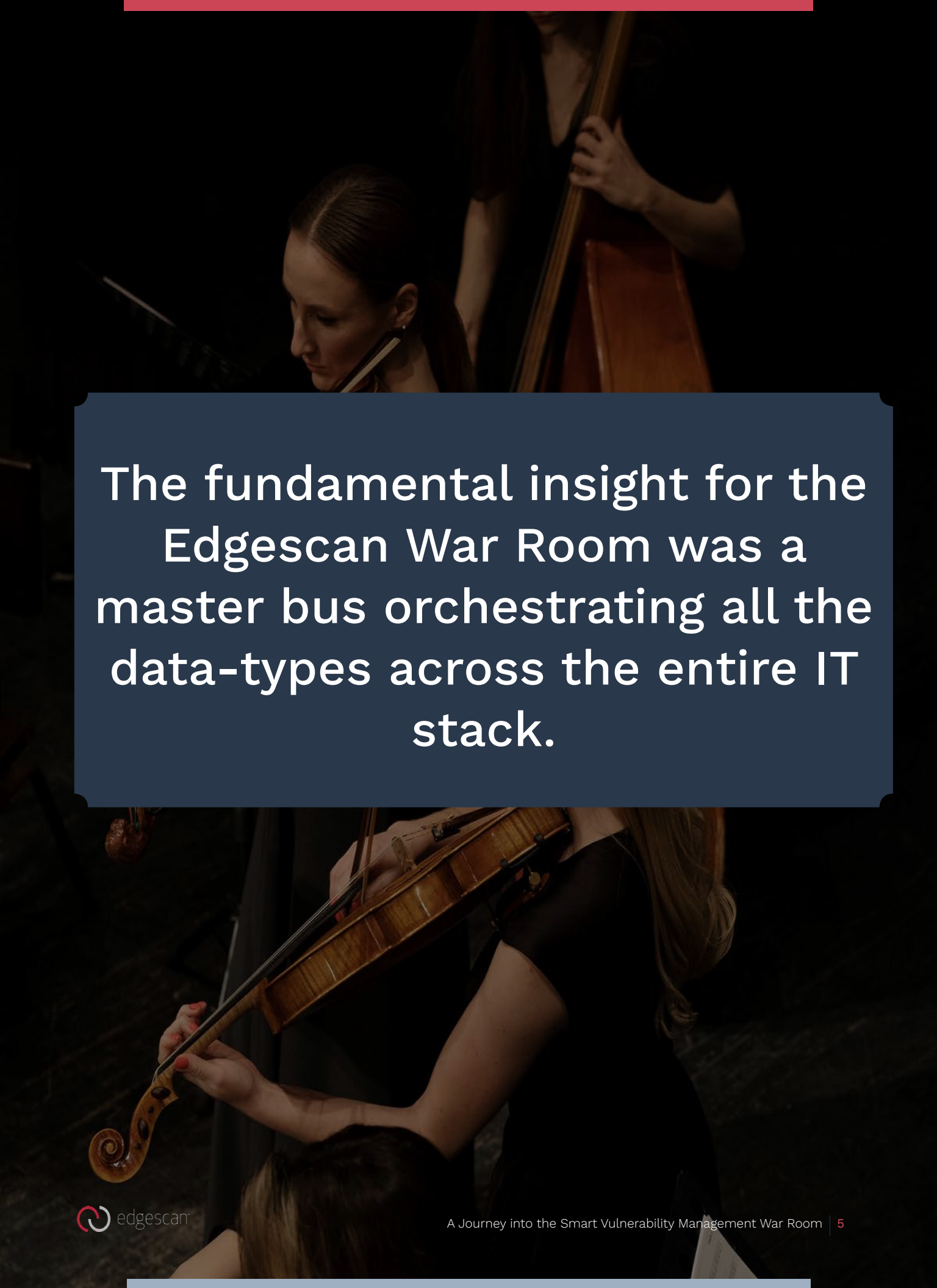
“If NASA built a Smart
Vulnerability Management War
Room - *What it would look like?*”

Core Innovation – Orchestration

Over 30 years of combined security consulting experience produced a considerable list of everything that needed to be integrated into a single platform. Orchestrating the integration of all of the data fed from the evolving attack surface and the vulnerabilities from each IT layer proved to be the core problem to solve. Some of the high level orchestration components include:

- Full Stack Orchestration – scanners had to be tuned for each layer – from web apps to network to API's
- Human Intelligence Integration – in order to achieve both scale and depth – the scale of tuned automation scanning needed to be blended and balanced with expert human remediation and false positive removal.
- Continuity - The assessments themselves had to be continuous or on-demand and unlimited.
- ASM and VM Convergence -The continuous scanning both for vulnerabilities and the attack surface identification had to be converged into one.
- Alerts – The system needed to generate metrics both for security alerts and business-ranked intelligence across every layer into one unified interface.
- Administrative Layer – each client needed a dedicated instance of cloud control with each connected to a virtual machine to support non public facing assessments. A dedicated tunnel from Edgescan to each client serving scanning data and validation and assessment data.
- Client Privacy – the client needed to actually control access attributes for their situation – so they essentially can control what Edgescan can see
- Client Operational Integration - Client connects using API's (e.g. dev ops or automatic assessment project)





The fundamental insight for the Edgescan War Room was a master bus orchestrating all the data-types across the entire IT stack.

Best of Both Worlds - Human Interpretation and Automation

One fundamental requirement was the need to deal with the noise generated even with tuned scanners for each IT layer stack. Traditionally noise (i.e. false positives) is a problem for automated scanning on any of the individual layers but when the optimal war room was designed to cover the entire IT stack – the exponential rise in noise had to be dealt with at the outset. And the decisive solution was to combine human expertise to triage and remove the noise before the alerts were communicated to the client. But while this simple and elegant solution took out the core problem of noise – there were other benefits to be had using human expertise.


Capturing Client Individual Business Concerns

While establishing accuracy and removal of false positive were initial drivers – especially when considering enterprises typically with limited bandwidth are traditionally crippled with chasing false data – the goal from the start was to offer contextualized industry-specific intelligence. The war room was designed to deploy client-specific custom rules for vulnerability assessment. For example, a streaming sports company places a lot of importance on cryptography, such that those weaknesses are highlighted, while a pharmaceutical will place more priority on protecting intellectual property, hence associated risks are highlighted. Here code related issues can be easy to detect. But when it comes to authorization (or logical vulnerabilities) say with a bank account, then logic-related vulnerabilities need to be managed. That is where expert validation comes into play to detect a logical weakness – something automation still cannot identify.

White Glove Service

And for ongoing, proactive security support – the human side of the Edgescan War Room can initiate escalation workflows. For example, if they pick up that a huge ransomware attack is coming out to take advantage of a common gap in security, then they can proactively alert the client and provide specific guidance on how to fix it immediately. And on an ongoing basis, the human experts can set up reoccurring custom schedules of assessment to individually go through specific vulnerabilities - prioritize them within the client's business context and weigh options between the complexity of the fix and the severity of the issue.





“While the human experts within the war room primarily provide false positive removal, the Global 3000 Enterprise also has a trusted world-class penetration tester on their side via Edgescan.”

ASM Meets VM

And while integrating automated scanning engines tuned for each layer of the IT stack represented a new paradigm change – integrating automated attack surface scanning engines was equally revolutionary, Edgescan has been delivering ASM since 2016. For without knowing what avenues of attack exist on an ongoing basis – the CISO is flying blind.

How do you Capture Something That Nevers Sits Still?

For the uninitiated, keeping track of all avenues across your network maybe seem more benign – something akin to library tidiness – it however is really a significant problem. For something as banal as leaving a dormant public web service open – just in case it needs to be reactivated -- is precisely what the attacker is looking for – and precisely the opportunity to do severe damage.

And Delivering Smart ASM to the Global 3000 Has its Own Challenges

So each Edgescan client has its own ASM solution. Some clients have geography related concerns – where one will literally see something different from United States than France who sees something differently from Brazil. It might look different based on rules. But leveraging the global cloud – one can work ASM from multiple locations simultaneously. And Enterprise Global 3000 clients like that – it removes the concept of geographic restrictions entirely. Edgescan in AWS maintains a presence across the world, with traffic coming from all over the world. That's the inherent beauty of large cloud providers. And to speak to privacy concerns – the data is held in multiple failover locations within northern Europe – where privacy laws are very strong – as opposed to say India or China where the privacy laws are not so stringent.

Integrating ASM with Hybrid Full Stack VM Completes the Puzzle

It is important to stress that the ideal war room was designed from scratch. It was not a matter of refining existing third party scanning tools and augmenting and Cobbling together what would have been essentially a Frankenstein point solution. Instead a new paradigm was applied – a paradigm that starts with one single platform that integrates tuned automated engines with business contextualized alerts across the entire IT stack and integrates it with human validation and remediation for the client's operation teams. But by integrating ASM – the complete VM solution is now married to continuous and complete visibility of the evolving attack surface - the war room is complete.

“If you are only capturing incidents across a partial view of your entire attack surface, then the cards are stacked against you right from the start”



Cloud and the Complexity of Data Processing

While leveraging best of breed technologies including:

- Cloud-based
- Ruby on Rails web-application framework
- Redis in-memory data structure

proved to be straightforward choices – it was the actual large volume and complexity of the data that proved to be the largest challenge for a number of reasons.

Early Bumps in the Road

There were initial bumps in the road developing the early prototypes. Azure Cloud Computing Services proved not to be a fit as it was blocking legitimate traffic because of its security controls. However, a quick pivot to Amazon Web Services (AWS) remediated the issue. But there still was the problem with the sheer volume.

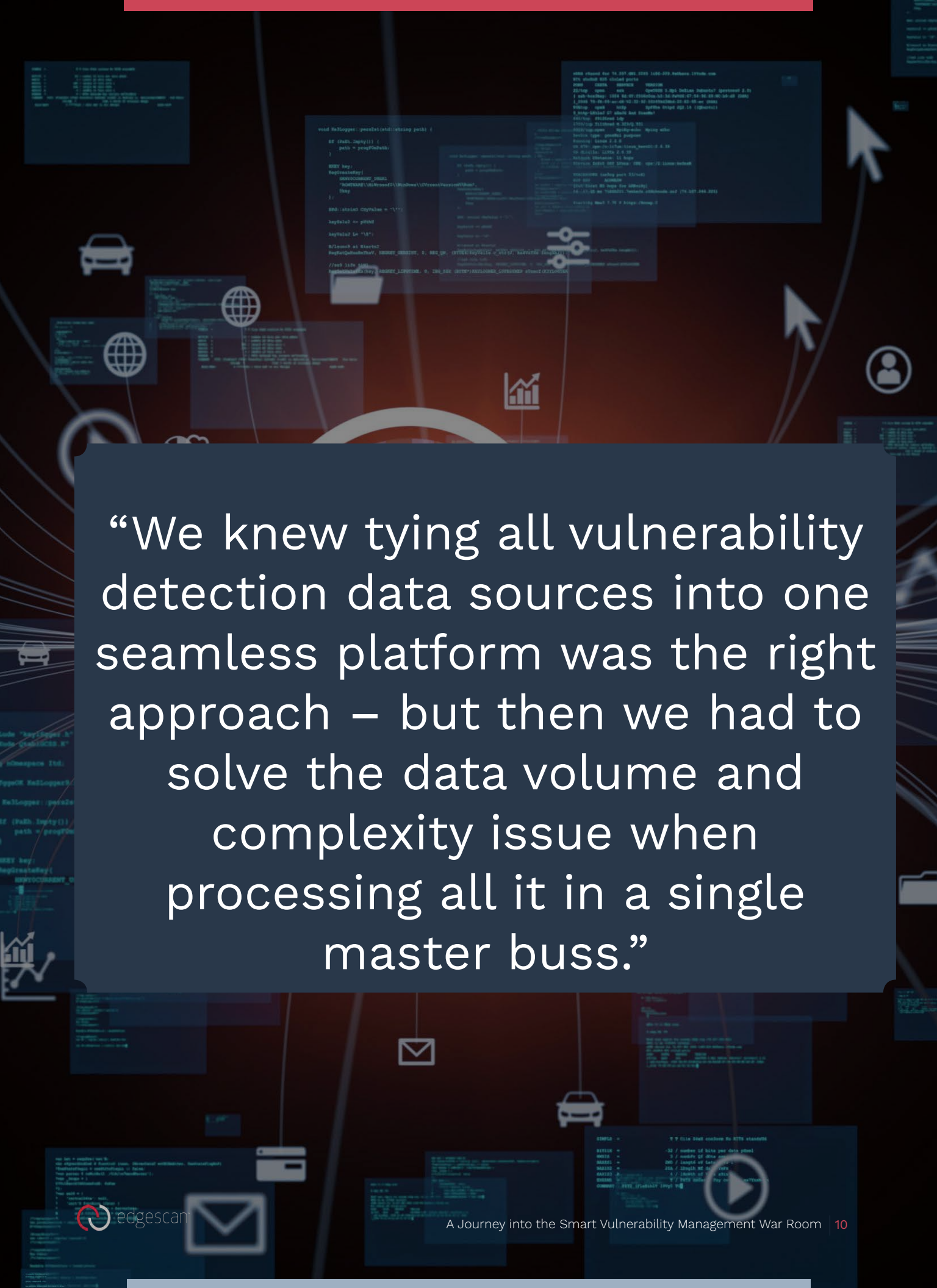
Can the Engines Handle It Captain?

As mentioned above, Redis for in-memory data structures, was deployed because the volume of the data was a concern. And also our war room required the ability to access the data really quick. On the front end data from multiple web app scanning engines, to ensure coverage as well as network scanning across all device types meant a large master bus with complex data types and large volumes.

Cost vs Performance

Costs for cloud computing services have gone up significantly (10X). Fortunately computation power has also gone up significantly and the system was designed to auto-scale when one area was busy and move seamlessly from one instance to another as the traffic scales.





“We knew tying all vulnerability detection data sources into one seamless platform was the right approach – but then we had to solve the data volume and complexity issue when processing all it in a single master buss.”

Global 3000 Enterprise Requirements

The need to fit the ideal hybrid VM solution against the requirements of a Global 3000 Enterprise produced a requirements list that was broad and deep. Some of the highlights include:

1. Time Zones – Global means global so basically through staggered 100% in-house operations the service will follow the sun
2. Disaster Management - Resilient zones across Europe with a two to three second return to service after any failure
3. Performance – no lag for human operations
4. Contextualized Alerts – custom alerts that make sense for particular client needs and the industry they operate within
5. Integration to Enterprise Support Systems – ranked alerts are automatically communicated in format the client operational support teams already leverage (IM, Tickets, email etc.)
6. Prioritization of Assets – the system had to be pre-built to allow assets types to be prioritized against what matters the most to each client's business
7. Modular Platform – while the greatest benefit is achieved by leveraging the complete platform – the solution needed to be adaptable to accommodate clients who only need a sub-set of the services on offer or want scale to the full platform over time.
8. Client Self-Service - Clients can configure what alerts – network, web apps, API etc. – and what locations (e.g North American server) get alerted.



“For the Global 3000 Enterprise, the ideal war room does not measure success simply by number of vulnerabilities identified but by the number getting closed.”

UX – Showing What Matters

Another requirement for the ideal war room was visual in nature. If all the continuous and accurate complete vulnerability intelligence data was not easily accessible, then effective remediation would be challenging. So like the computation challenge dealing with the data complexity – this new novel approach demanded an innovative User Interface to show what matters to each client.

We Won an Award!

It was extremely gratifying to win the Good Design Award for User Interface Design in 2020. As we have seen accessing insights that mattered to each client was a necessary condition to completing the ideal war room.

Not Simply a Beauty Contest

As we have seen the main challenge really was to display a high amount of information from scanning and identifying vulnerabilities and at the same time display exactly what the customers need to see. They needed to see what mattered to them in an environment free of clutter and non-essential information. This in turn has a dramatic effect on saving time and improve efficiency remediating important issues.



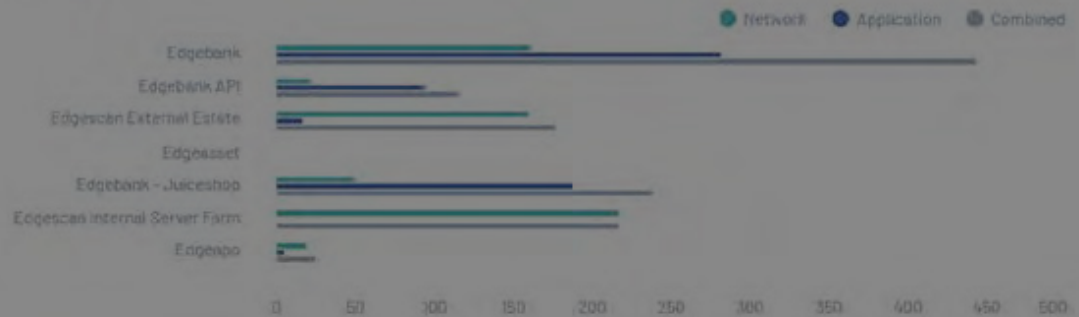
Hi, you have **16 critical vulnerabilities** across **5 assets**

Exposure factor

Mean time to remediate

“The requirement was a matter of decluttering – show me what matters simply and quickly.”

Asset risk



Support

Staffing up the War Room

The war room is staffed fully in-house and is located in Dublin. To meet the Global 3000 Enterprise requirements including follow-the-sun support – the specialists all work in a remote fashion.

Layered Expertise

As one might expect the war room is built with tiers of testers including:

- Expert Penetration Testers with OSCP, CREST, CSP, GIAC Certifications.
- Red Teaming Specialists
- Software Security Engineer Skills to provide pragmatic advice.
- Penetration Testers with Secure Coding Skills
- Subject matter experts for specific technology stacks

So when the Global 3000 Enterprise client speaks to members of the team, they are speaking to expert, seasoned penetration testers who also rotate on and off between Edgescan support and professional services.

Staffing Up Penetration as a Service (PTaaS)


The War Room challenge in this case is to offer the same coverage and depth as a traditional, pre-scheduled stand-alone pen test service. But in the ideal war room – a full blown testing engagement can be carried out via the platform itself whenever the client requires it. Additionally, the PTaaS offering allows for unlimited retests to assist with remediation and verify that the vulnerability is actually closed. So in turn this requires not only expert pen testing staff but each has to be OSCP and CREST certified. And the staff has to be large enough to be available on-demand continuously. Indeed, the breadth and depth of the PTaaS staff ensures breadth and depth of the service.

HR and the War Room Staff

The quality and longevity of the staff are key to success. Some relevant features of the staff makeup include:

- World-Class Security Quality Skills
- Continuous training
- Churn rate is less than 3%
- Morale is high – The Environment is a rewarding workplace working with the best of the best.
- Robust Onboarding Process to contextualize new members of the war room to the robust platform




A vertical image of a space shuttle launch. The shuttle is white with a red nose cone and is ascending against a dark background. Bright white plumes of smoke and fire are visible at the base of the shuttle. A dark blue rectangular box with rounded corners is superimposed over the middle of the image, containing white text.

**“A world-class war room attracts
world-class talent”.**

The Future War Room

Well that concludes the War Room tour – well at least the current state of the war room. Edgescan has an equally aggressive and innovative product road map that will seek to harness even further security improvements leveraging new technologies and approaches including Artificial Intelligence and Crowd Sourcing Intelligence to name a few. Our vision is developed in concert with new requirements from our current Global 3000 client base as well as from industry leaders through our Advisory Council Program. If you would like to extend this virtual tour to a live demo, please reach out to our team.



“The future is the shape of things
to come.”
(H.G Wells)