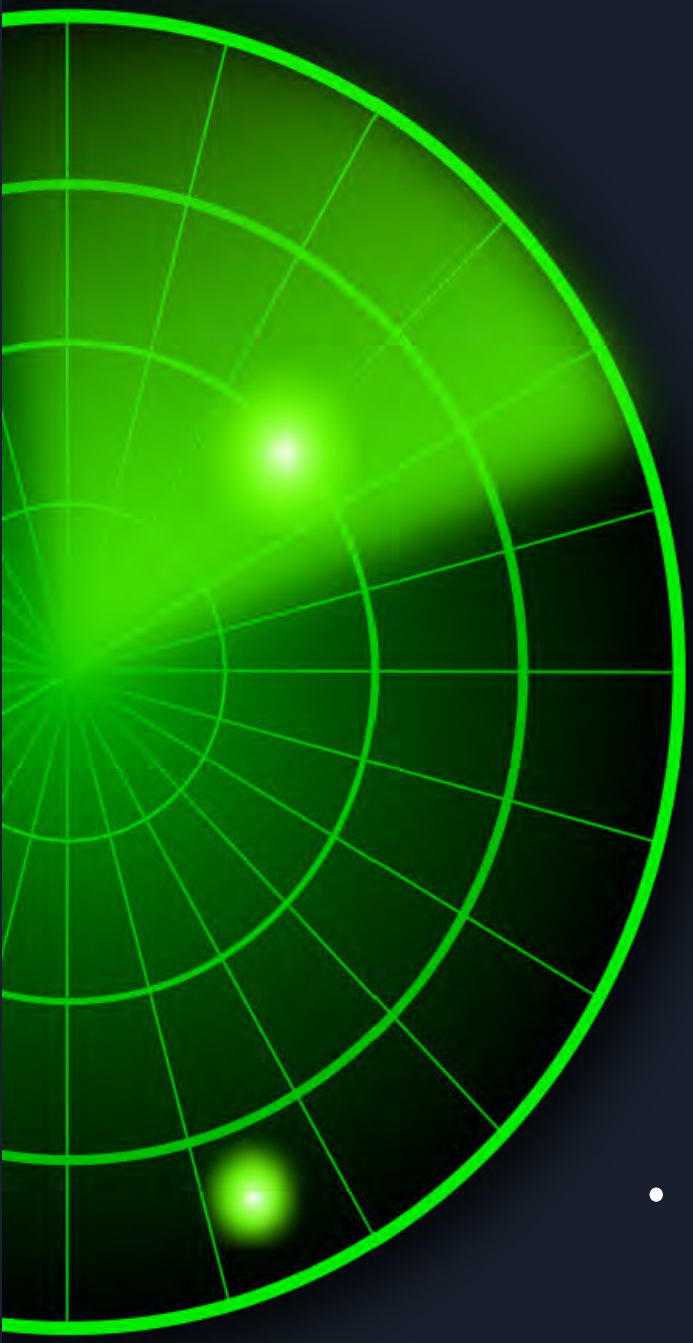
edgescan™

FULLSTACK VULNERABILITY MANAGEMENT™

Does a Hybrid Model for Vulnerability Management Make Sense

Does a Hybrid Model for Vulnerability Management make Sense?



Do Automated Scanning Tools Require a Human Touch?

A new model for Vulnerability Management (VM) – the Hybrid Model – layer on top of the emerging scanning tools. And on the surface it appears to be going backwards – why would we retreat from the advances and sheer scale that automated scanning technology can deliver and burden ourselves with the slow pace of a team of humans? Does the hybrid model make sense?

Will Scanning Automation Delivery Vulnerability Management Nirvana?

If there has been one theme in 2021 to define the last decade of Vulnerability Management (VM) - it is the rise of automated tools to deal with the deluge of the ever-increasing number of attack surfaces and the frequency and ingenuity of the attacks themselves. And so as the tools become more refined and more accurate and expanded in scope to handle all the layers of the attack surface including not only the network but the application layer itself – one might reasonably ask - ***Are we now in 2021 headed to a utopian state?*** Are we headed to a point where the technology and its ability to handle the sheer volume of incidents is simply going to outgun the attackers?

Software testing Software, who thought that would ever work?

The view from the Trenches is Not Pretty - Its Actually Noisy

The answer is a firm “No”. For those on the front line tasked with managing incidents, their day-to-day is not close to utopian – if it was to be described with one word, it would be– ***Noise.***

Far from VM nirvana – the front line VM staff leveraging automated scanning tools are now faced with a new herculean task. For all the scaling efficiencies automated tools, they have effectively created a new massive problem – ***How with the proliferation of automated alerts do the tools actually separate the wheat from the chaff?*** For a significant amount of the alerts represent false positives (noise) – an alert that accurately detects an incident but the incident does not represent an actual issue.

So while detection automation looks after the incident scale issue – it passes on a new scaling problem – dealing with the noise.

“More than 60% of security professionals estimate their security function spend over 3 hours per day validating false-positives. Nearly 30% are spending over 6 hours on this task. Most agree that it is too much and the time could be better utilized. For most, it is the part of their job they like least.”

by Infosecurity Europe 2019

Software testing software - We accept false positives in scanners (Software getting it wrong) but we don't accept vulnerabilities (Software getting it wrong).

Hybrid to the Rescue - Can I have some Human Expertise Please?

Imagine yet another future utopian state. We rank all the types of incidents against technical and business severity and pass them through a skilled, experienced set of cyber security experts that parse out severity-ranked alerts of those that represent a significant problem from those that are false positives. And imagine that communication comes with expert remediation advice to resolve the issue efficiently and how to avoid the issue in the future. Now in this scenario, the front-line VM worker is equipped with scale for both incident detection through automation tools and immediate resolution guidance against only those incidents that matter. Indeed, such a desirable state is in fact available in 2021 – it's the hybrid approach.

The Future is Now - ***What are we waiting For?***

So if the enterprise now can embrace a truly hybrid model – a model that both leverages the scale of automated detection tools against the entire stack as well as integrated human security expert guidance to rule out all the false positives and provide timely expert remediation guidance for equally timely resolution – then surely the enterprise is 100% onboard – ***correct?***

The answer is "no" and for the remainder of this paper, we will examine why and submit the approach to a pro and con analysis - weighing the merits and areas of concern for adopting the hybrid approach and then counter whether those areas of concerns are valid.

The reliance alone on automation to defend against an experienced and determined human adversary will not work.

Pro's and Con's for the Hybrid Model

Pro's

1. Scale

Hybrid model still offers all the scaling automation benefits of the automated side of hybrid.

"Scale vs Depth – Scanners do scale, Humans "do" depth. – Our enemies "do" depth every time and are focused."

2. Accuracy

The entire point of the human expertise side of the hybrid model is to verify incidents and remove false positives.

Automation accuracy is not a strong as human accuracy – Our attackers are humans.

3. Expert Support

Again expert is exactly what the human side of the hybrid model delivers needs to cover everything – testing both the technical and logical security posture of every asset – including API's, cloud-based infrastructure and web and mobile applications.

IT and developers are not cyber security experts – Expert guidance is necessary

4. Removing Noise

The human touch will remove 100% of false positives.

Chasing noise is a fool's errand

5. Timely Remediation

When experts present real incidents they offer expert guidance how to resolve now and for the future. And no time wasted or distraction from chasing false positives.

Far from slowing remediation – relevant expertise pins down the source of the problem quicker

Pro's and Con's for the Hybrid Model

Pro's

6. Severity Ranked Guidance

The human side gets rid of the false positives and the automated scanning platform can be mapped in the setup phase to automatically rank the severity appropriately for each enterprise.

Effective VM intelligence requires alert significance context

7. Staffing Challenges

Having a team of security experts within a hybrid model offloads the stress of inhouse recruitment.

Extending your security team with world class experts offloads staffing challenges

8. Automate Remediation into Operational Workflow

The alerts can be integrated to the enterprise support and development systems to automate remediation practices into the daily operational workflow.

Change gives rise to Risk. Change occurs when a system does not change & When a system changes (duh!!)

Pro's and Con's for the Hybrid Model

Pro's

9. Instilling Confidence on Alerts and Remediation

When a significant amount of alerts from just the automated side of the hybrid model are presented with no human filter, then there is a large expectation built that they are acting on noise – false positives. When the noise is removed with expert human review, then the enterprise confidently knows they are acting on things that matter.

Over time critical vulnerabilities are discovered. Patches are released. Yesterday I was secure, today I've a Critical Risk. Need to patch/Redeploy. Also....when a system changes: New features deployed, new services exposed, larger attack surface, more exposed, more to attack, more headaches t his also gives risk to risk.

10. Enabling the Enterprise to Act Strategically

Equipped with verified accurate intelligence, the Enterprise Security Team can now plan and strategically align their goals with the overall business goals of the Enterprise.

Business Goal Alignment – How to ensure Cyber Security has a seat at the strategy table.

11. Staff Morale

Removes the drudgery – the multiple hours per day – of the repetitive work of removing false positives.

Burnout can have an impact on readiness.

12. Executive Management Confidence and Transparency

Acting on false positives or simply inaccurate assessments can be tiresome to the Cyber Security Staff and can be equally tiresome and demoralizing when the executive management team does not think they are being presented with the truth.

Nothing motivates more than accurate and actionable intelligence.

Pro's and Con's for the Hybrid Model

Pro's

13. Proactively educate IT Staff on what is the issue and what can be done

The expert remediation guidance that comes from the human touch side of the hybrid model can also be proactive and suggest steps to be taken to avoid similar issues in the future.

> The DevSecOps elephant in the room is "Validation"

14. Supplements the Inherent Weakness of Automation

Automation does not provide human context for intelligence. Experts can identify risk. Artificial intelligence is narrow – it cannot determine meaning.

> We're protecting our systems against breach by humans, not scanners right!!

15. Determination of Vulnerability Significance

n order to be seen as significant, certain vulnerabilities require humans to quickly come to terms with its meaning. It is not just all about ruling out false positives – it's also coming to terms at the human interpretation level that a certain issue represents a significant issue.

> We can't improve what we can't measure;
> We can't secure what we can't see.

Pro's and Con's for the Hybrid Model

Cons's

1. Time

Having a human interpretation phase will slow down the ETA on resolution

Counter

This step will ALWAYS have to happen whether one utilizes a hybrid external solution or uses their own staff to rule out false positives. And the hybrid model can make effective use of a correlation engine to effectively minimize the human effort.

2. Cost

A managed service offering expert (i.e. costly) world-class security engineers within their hybrid model surely would be cost prohibitive.

Counter

The Enterprise HAS to deal with that cost themselves regardless if they staff it or use an external hybrid solution. The external hybrid solution can leverage economies of scale, produce efficiencies with its VM focus and have staff overlap in duties to lower the overall cost.

3. Resourcing

The enterprise even with their well-heeled brands has recruiting challenges for cyber security expertise, surely smaller suppliers will have the same problem.

Counter

With its global VM focus, the external hybrid solution will have more efficient recruiting and relevant ongoing staffing support while carrying less overheard. The best and brightest like to work with the team that is the best and brightest.

4. Scaling

And as incidents rise there must be a point where the human side cannot meet the scale need - even with an external provider.

Counter

is a well-know problem which experts in the community label – "resolution" – and the hybrid model is continually stress-tested to handle the scale of incidents that full automation can capture and still offer the exact same accuracy small volumes. This is partly due to the hybrid solution provider staffing correctly and also due to internal efficiencies created including a correlation engine that aids the expert team coming to terms with the significance of the issue quickly. And then to point out the obvious - an Enterprise's own Cyber Security staff only using point automated scanning tools will have the same problem. The hybrid model does not create the problem of scale – it just deals with it the most effectively.

Pro's and Con's for the Hybrid Model

Cons's

5. External experts do not possess company-specific nuanced business knowledge

Surely an external managed service cannot know the nuances like my own staff?

Counter

While the concern in understandable – it really reflects a lack of knowledge of what is on offer with a hybrid model. For a hybrid model has the capability to recognize which type of assets and related incidents are most important to an organization and map that priority ranking in the setup phase into the automated alert systems. So not only do all alerts and recommendations out of a hybrid model remove all the false positives – all the real issues are presented prioritized to what matters to that organization.

6. Widening the Gap Between Ops and External Recommendations

Does not using an external team of experts within the hybrid model widen the operational gap between VM staff expertise and the operational daily workflow.

Counter

While the Cyber Security internal department may be physically down the hall from the IT and Ops staff, the method to integrate recommendations against discovered concerns is typically quite manual and slow and burdensome and inefficient. With a hybrid model – all the alerts and expert remediation are integrated very quickly in the setup phase to all the relevant operational support, risk and development systems. And on top of integrating automated recommendation into the day-to-day daily operational workflow, the guidance itself one receives is from a team of specialized cyber security experts.

So Does the Hybrid Model Make Sense?

In Conclusion - The Hybrid Model Makes Buckets of Sense

The merits now have been shown to be numerous and significant And the areas of potential concerns have been identified but as each one was countered - none of them have been shown to have merit. And so perhaps the question now is not whether the hybrid model makes sense – its makes buckets of sense. But rather - it is so compelling for so many reasons that any enterprise considering what model represents the most compelling solution for Vulnerability Management must put the Hybrid Model at the top of their list.

"While automation certainly provides scale, its human expertise that accurately gauges significance and focused remediation where it really matters"