Enabling Enterprise Operations with Smart Vulnerability Management

edgescan™

Operational Excellence and the Hacker

The ever-looming threat of cyber security incidents is casting a large shadow over Enterprise operational and development teams. However this threat is not typically their core focus, nor their core competency. Yet even if they adhere to a very progressive and innovative service delivery model following operational, software development and networking best practices – it can all be rendered worthless in one stroke of a hacker's keyboard. In one simple act, a hacker seizing a timely attack-opening at any given moment of the day, can undo the best technology and operational infrastructure. They can bring the business down.

Enable without Weighing Down

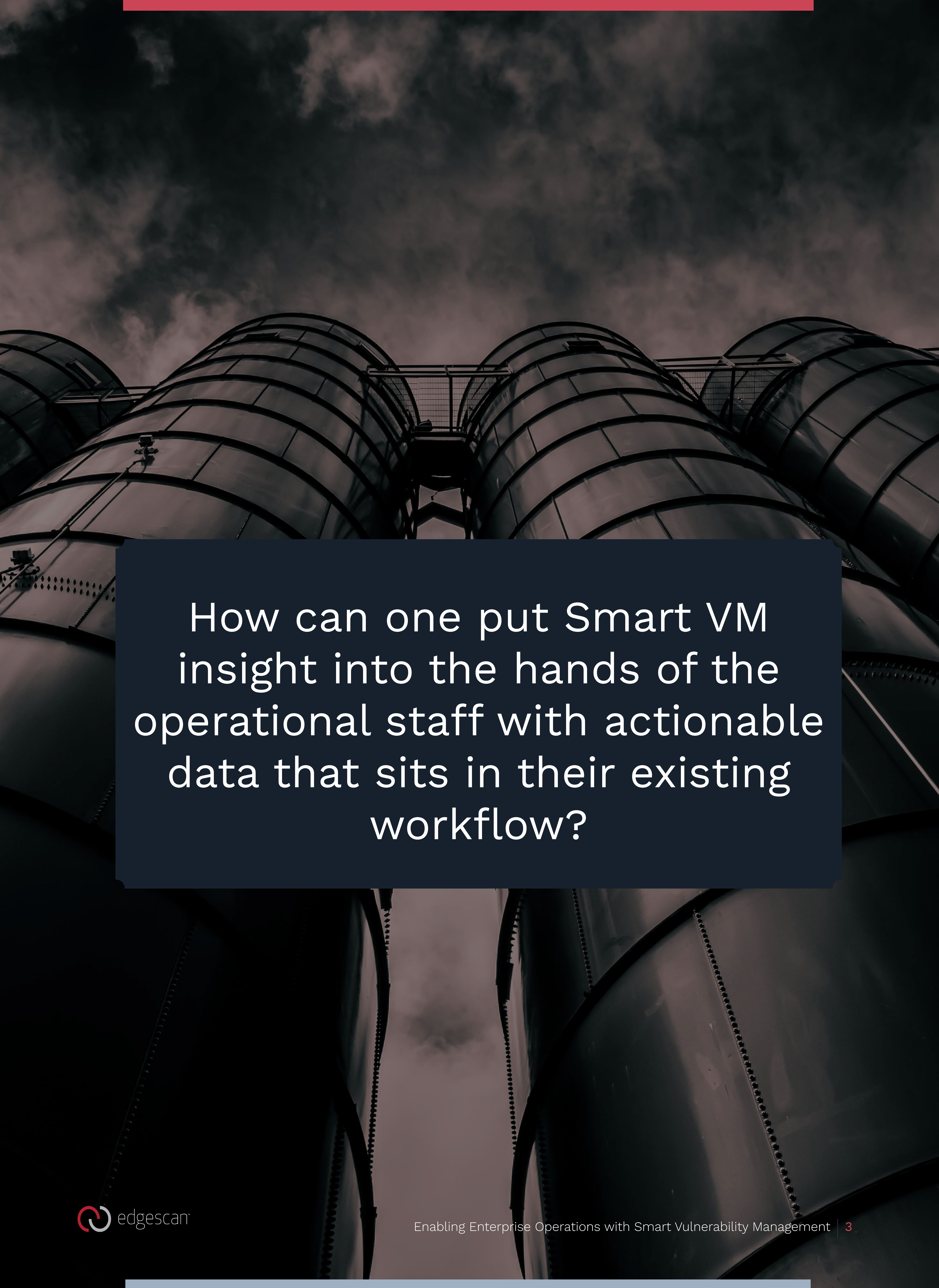
So, the enterprise it seems is caught in a logical dilemma – we want non-security experts – the operational team – to anticipate and resolve all business-relevant security vulnerabilities before they become incidents. And so the challenge becomes - how to enable them with insight and remediation guidance without filling their workday.

IT Traditional Siloes Do Not Help

Far from being integrated – departmental boundaries between Security and IT and Operations are exactly that – they are boundaries. While Security staff attempt to acquire and refine third-party security tools for each layer of the attack surface with specific scanning engines - they still face the herculean task of removing all of the noise and sorting out those vulnerabilities that really matter to the business AND THEN communicating the signification issues to the relevant Operational teams to work on the resolution.

There Has to Be a Better Way

In this paper we lay out steps to take to solve this gap problem and outline important things one should consider if you are serious about enabling your operations to integate Smart VM in their existing workflows.



How can one put Smart VM insight into the hands of the operational staff with actionable data that sits in their existing workflow?

Step One – Go Full Stack

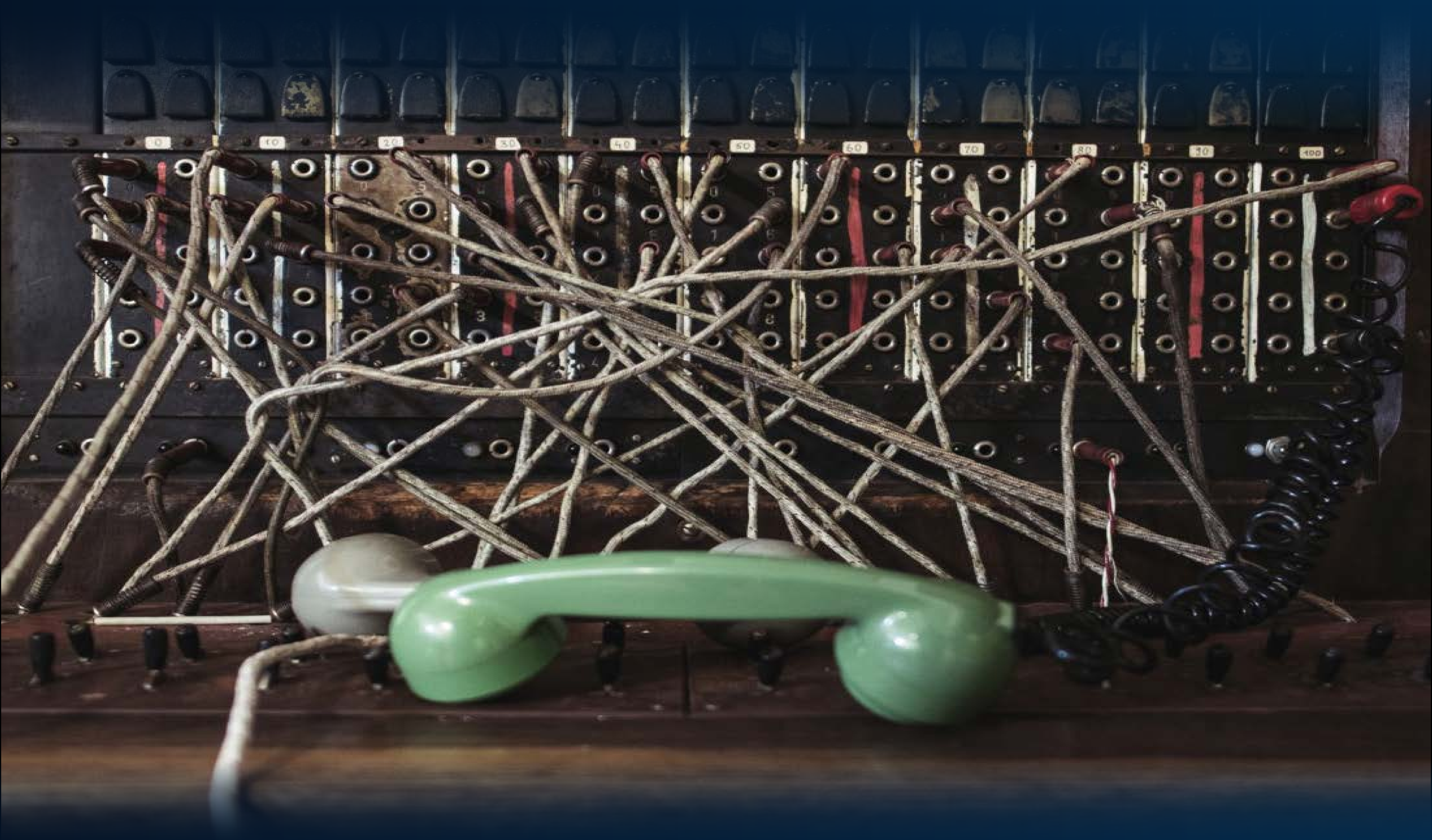
Let's start with low hanging fruit. The IT layers have expanded with the evolution of IT itself and so have the number of security specific scanning tools for each new layer. In fact, Gartner has reported that 78% of CISO's have sixteen, yes sixteen or more tools in their portfolio! – and 12% have 46 or more! (Gartner Top Security and Risk Trends for 2021). This complicates the communication problem for the Operational Support team.

Can We Have a Single Touchstone of Truth, Please?

Again, the goal here is to improve the situation for the operational team by streamlining VM insight within existing workflows – not to complicate things. Expressing vulnerability issues with one type of alert for web applications and then another tool for networking issues – is simply making the situation worse. At the end of the day the Operational Team needs to know in a timely, proactive manner what issue is of concern in their business across the entire attack surface in one timely communication. The hacker does not care about attack surface layers nor the point tools for each one and neither does the operational staff. They want to know if there is a problem and how to fix it.

Are Their Full Stack Smart VM Platforms in 2022?

While even within the security community there has been a tradition of managing security with a plethora of tools – there are vendors who offer a full stack Smart VM solution. One such vendor is in fact Edgescan as they have built their entire platform with a centralized engine tied to contextualized scanners across the entire full stack. The fact that all alerts across the entire stack ranked in terms of business significance are presented to in single view of truth to the operational team is a huge enabler. The operations team now can operate with a holistic view.



“ Having too many security vendors results in complex security operations and increased security headcount.” (Gartner Top Security and Risk Trends for 2021

Step 2 – Leverage a Hybrid Model to Stop Wasting Their Time with Noise

While reducing all the alert layers to only one platform is significant – perhaps an even more significant step to take is removing the noise delivered to the operational team. For even within a well-oiled security team – while the vulnerability scanners can continuously scan at scale - they in turn create a lot of noise – false positives. This sheer volume of noise creates a tremendous work-load. In the security industry – it's referred to as the donkey-work. Sifting through the seemingly endless fool's errands of false signals is tough enough with a dedicated security team - but to pass this onto a development and operational support team represents a fundamental problem.

What About the Operational Day Job?

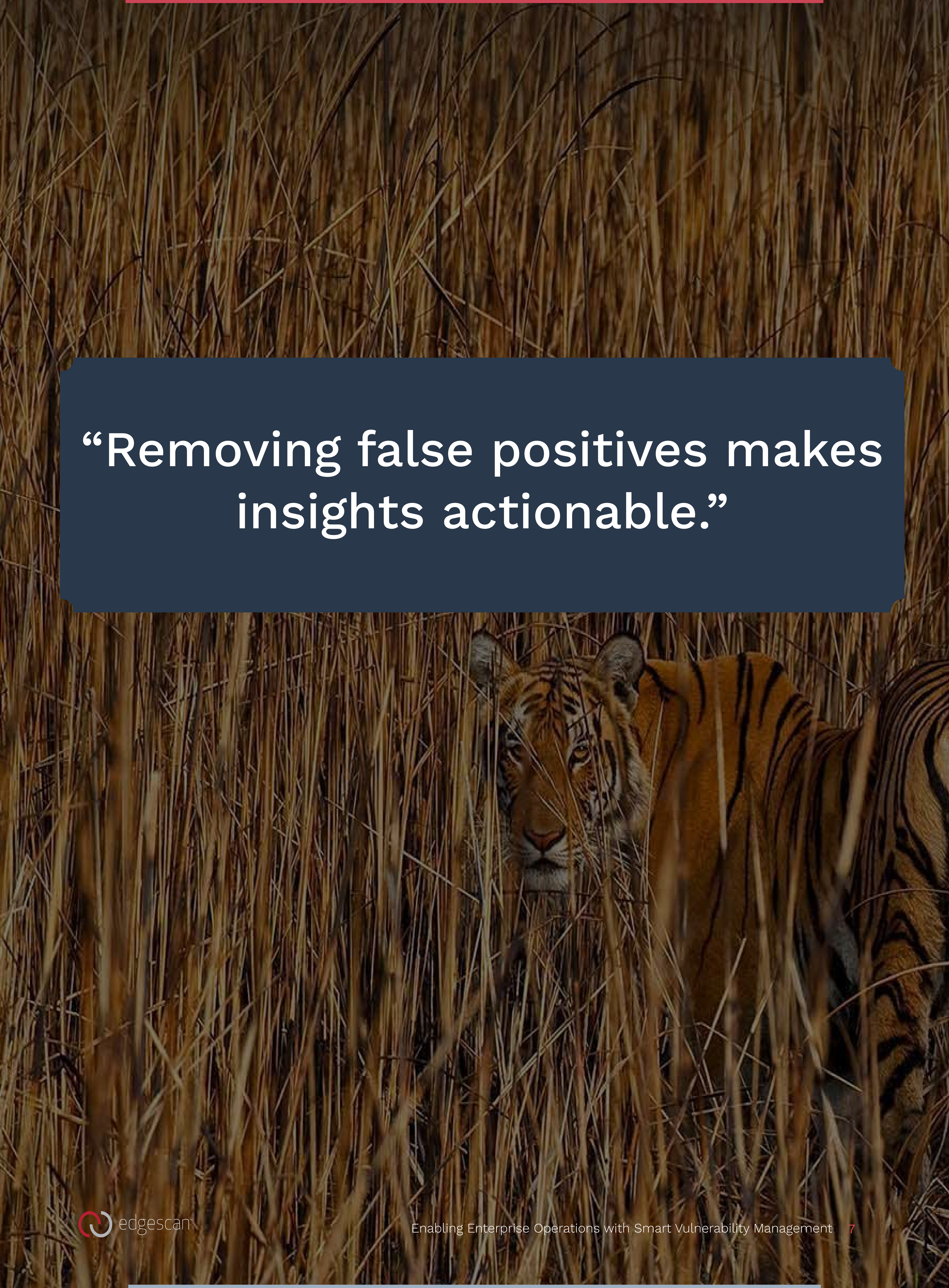
And so our original problem we set out to solve – streamlining Smart VM insight into daily operational workflow – gets even more complicated to solve when one considers the amount of bandwidth required dealing with the noise. But just as the Full Stack approach helps unifying alert communication into one channel as opposed to say 17 tool-driven alerts – there is a Smart VM approach that can handle the noise burden. It is called a Hybrid Model.

Bring on the Expert Validation

With a hybrid Smart VM platform - all alerts are validated first by security experts. This effectively removes the false positives and provide accurate reports on issues that actually are real. Instead of chasing noise – the operational staff are now are confidently resolving real issues. A logical consequence of removing false positives is that the operational teams are dealing with less data and lightening the burden with less disruption to their daily workflow.

Actionable Insight

At the end of the day – the goal is to normalize data into actionable insight. False positives are not actionable insights. If one wants the operational support team to take on additional remediation work then the work should count. They should be resolving real issues.



“Removing false positives makes insights actionable.”

Step 3 - Ecosystems Integration

Now we consider how to actually automate communication with the relevant operational resources. While one might think that one is solely concerned in getting accurate alerts with timely remediation solely to the IT development and support teams - the enterprise is typically more complex than that. In order for the Enterprise to leverage Smart VM – the insight has to be integrated on a much wider scale – it must be integrated into all of the relevant Ecosystems.

Types of Ecosystems

Aside from the ticketing systems – one must also integrate insight into the relevant GRC (Governance, Risk and Compliance) systems.

Governance Systems

Governance is focused on aligning processes and actions with the organization's business goals. So, in this case one must contextualize the severity of each alert against the impact is had on their particular business goals.

Risk Systems

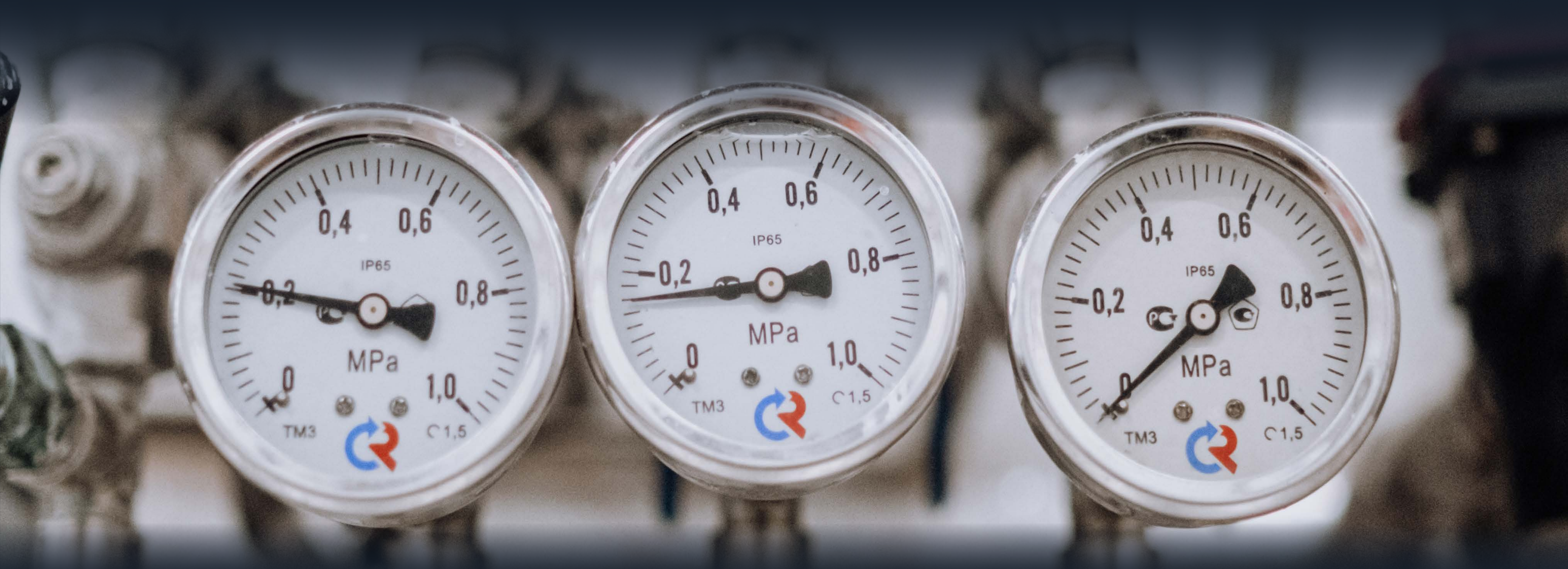
Risk of course consists in identifying and addressing all of the organization's risks including the well know risks like financial and operational and safety risk but also includes reputational risk. In each risk category – security incidents can be a significant driver – including ransomware and financial risk but perhaps currently even more prevalent is the reputational risk impact associated with front-page security incidents.

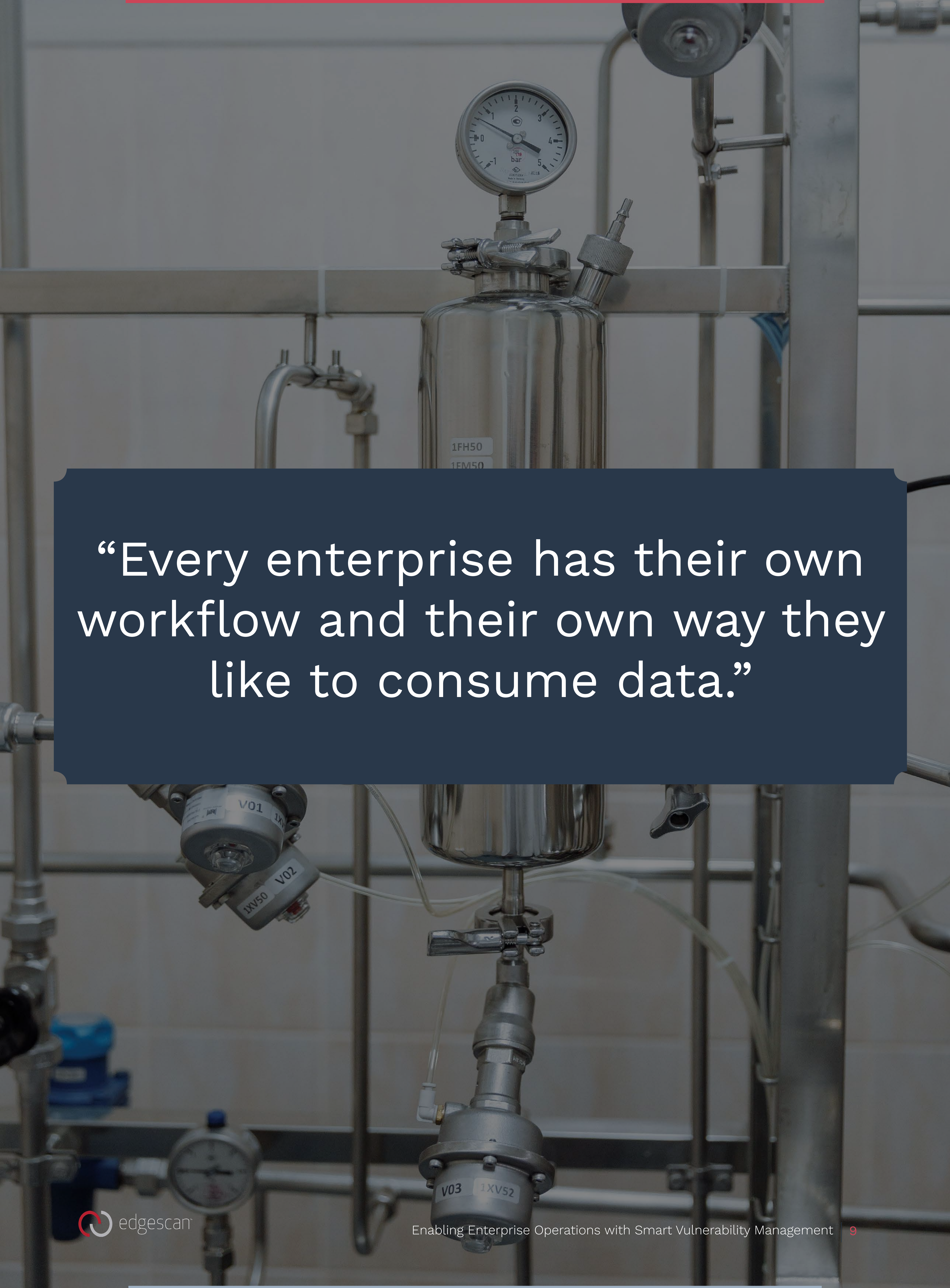
Compliance

Compliance programs ensure all activities meet legal and regulatory requirements. Of course security audits speak directly to compliance requirements and progressive Smart VM solutions will ensure even challenging problems like PCI compliance.

Tying it All Together

At the end of day, operational support and development staff as well at those tasked with GRC Programs all operate in unique ways. They require the data and insight to be normalized to their day-to-day activities without disrupting their regular workflows. An enlightened Smart VM program will come pre-built with integration hooks and customized data presentation capabilities to ensure that is exactly what happens.





> “Every enterprise has their own workflow and their own way they like to consume data.”

Step 4 – Cadence Integration

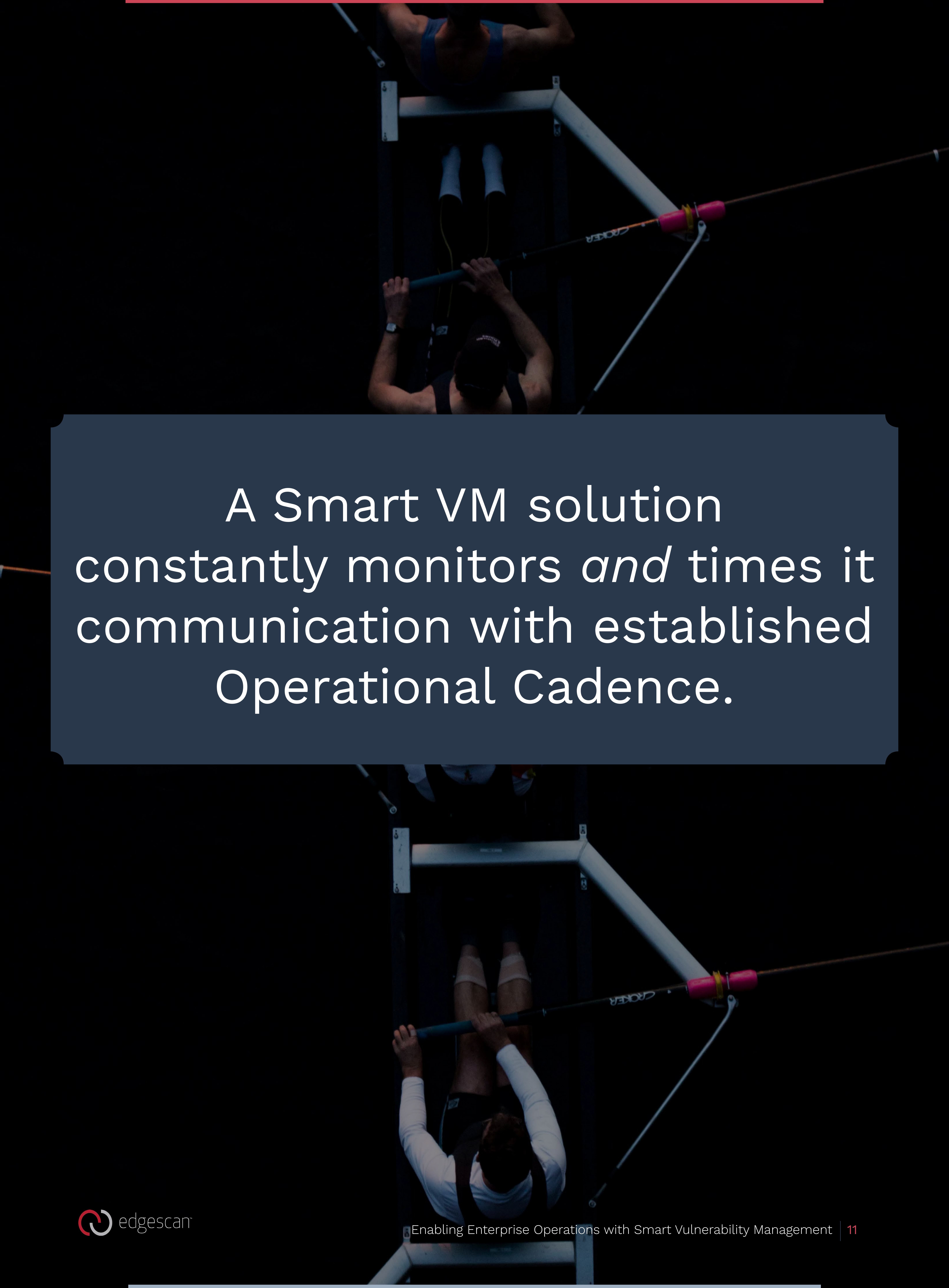
Operational workflow is highly individualized for each organization – each has its own cadence. Each organization likes to consume and integrate security insight against the pattern of their pre-existing workflow. And again, if the goal is to streamline actionable intelligence into operation workflow - the insight has to occur at the same cadence.

Business Drives Cadence

Clients requirements for the specific frequency of fresh results is largely dictated by type of Enterprise. Financial Institutions tend to be fairly conservative and so typically would like a penetration test done once per year. Their corporate personality is such that they only like to be told their house is in disorder once a year. However more progressive organizations simply do not want the penetration testing to stop. They require they are done every quarter and in terms of vulnerability scanning – they require a fresh batch of results every 2 hours. The results are directed to an internal consultancy team (not operations) who serve in an advisory capacity to each department.

But Is There Not a "Right" Cadence?

As an illustrative example – the Edgescan solution does time its communication updates to reflect the cadence of the organization it serves – but this does not mean scanning and verification stops. Edgescan performs scans and verification continuously in parallel to customer operations. Every organization certainly has a different cadence in assessment when scanning takes place – annual, monthly etc. Edgescan however in the background does it continuously against every piece of technology. When if an issue is detected, then a communication will be directed to the relevant resource.



A Smart VM solution constantly monitors *and* times it communication with established Operational Cadence.

Step 5 – The Key to Communication is Simplicity

One might be tempted to think if communication is reflective of the first four steps:

1. Funneling in business-ranked alerts from the entire stack (Step 1 – Full Stack)
2. And ensuring accuracy with expert validation (Step 2 – Hybrid)
3. And automated linking to all relevant Ecosystems (Step 3 – Ecosystem Integration)
4. And coincides with the same cadence as the operational workflow (Step 4 – Cadence Integration):

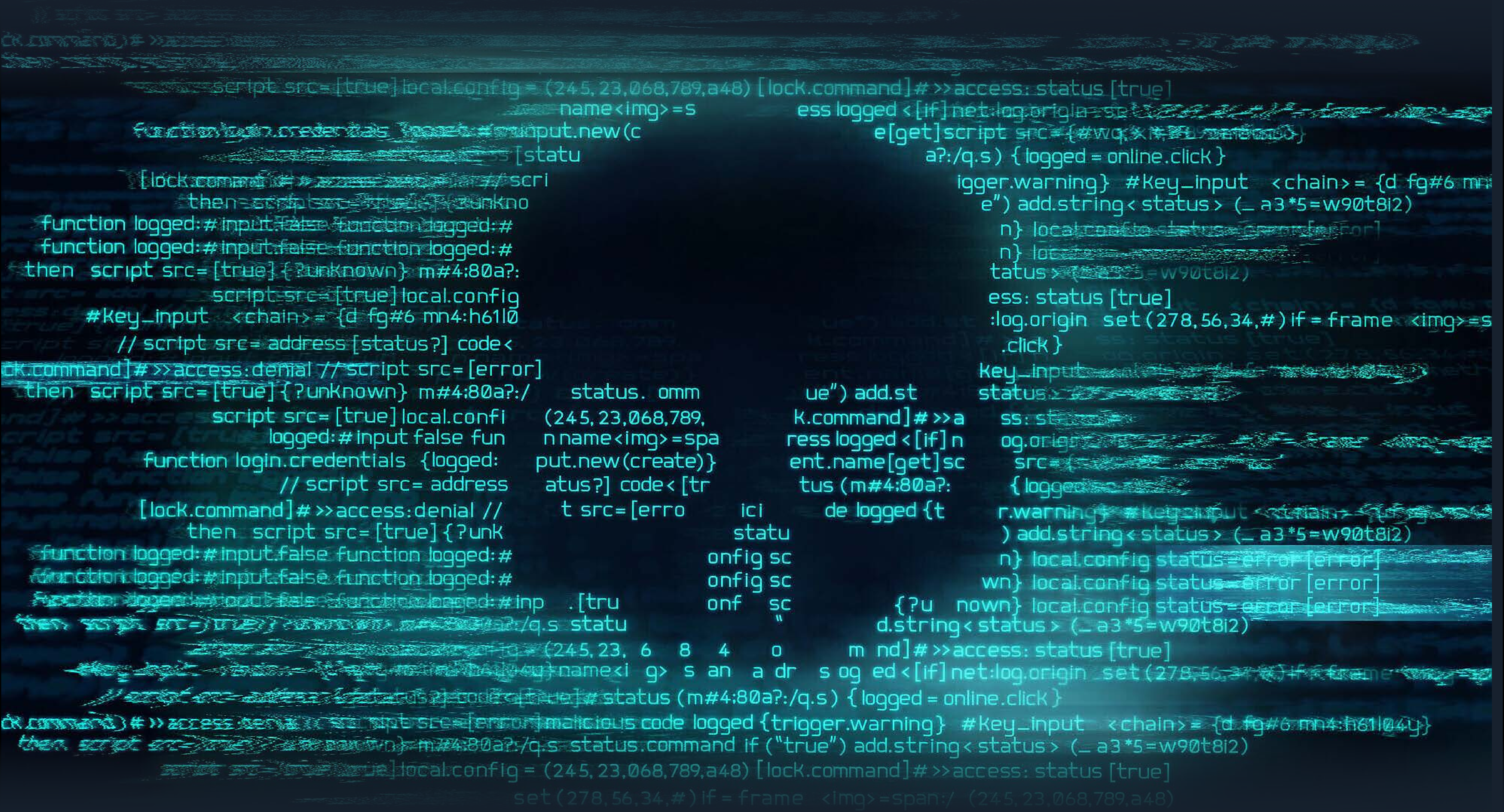
then the communication interface or visualization must be quite complex. But the opposite is true.

Just the Relevant Facts Please

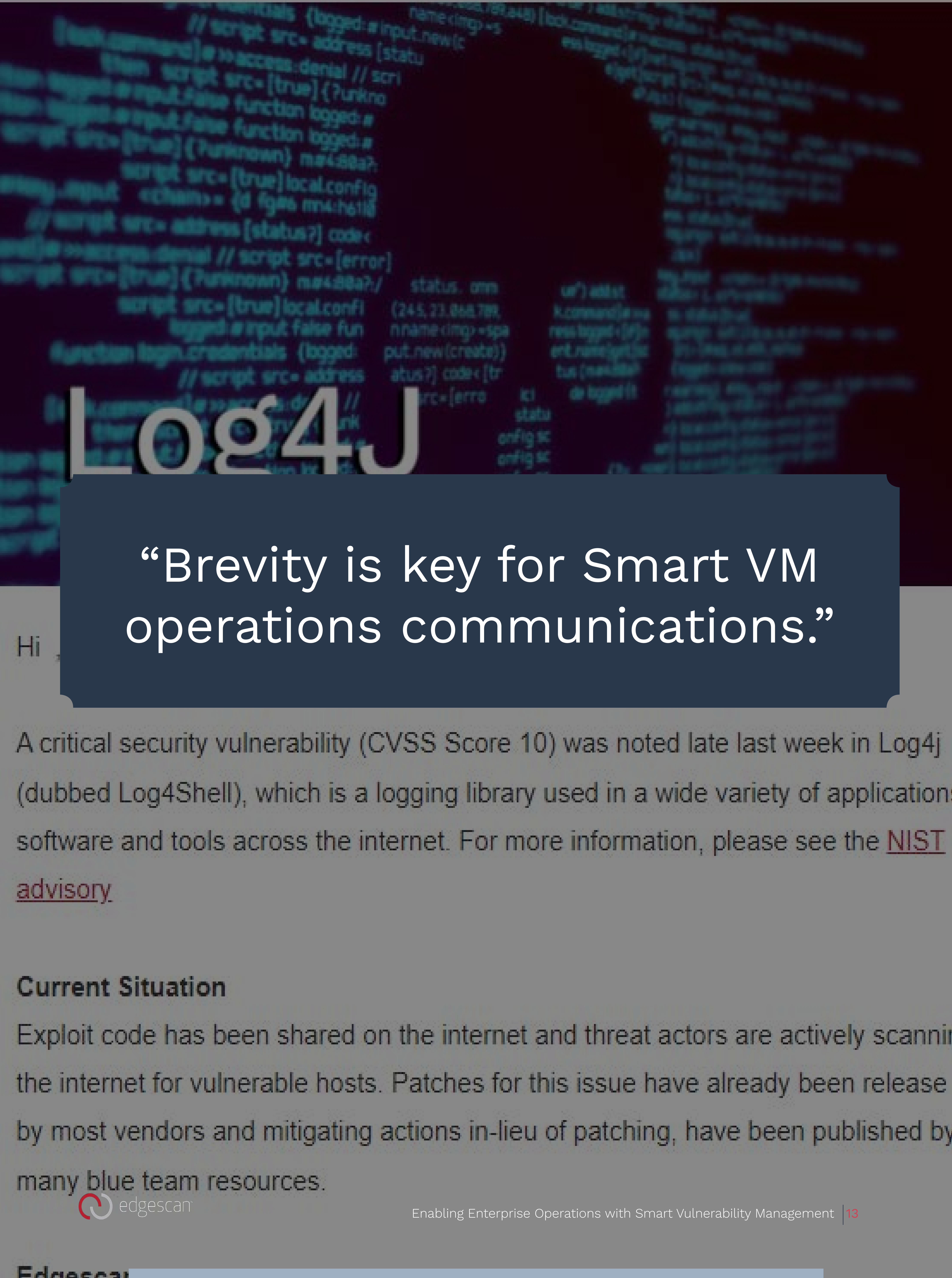
One is reminded of Mark Twain's famous line – "If I had more time, I would have written a shorter letter." Brevity is key here. Remember the most important goal when injecting Smart VM into Enterprise Operations is to present actionable intelligence. This means stripping down to the bare necessary details while ensuring every piece of actionable data is included.

Communication is Deadly Serious

When contacting the client about something serious – a Smart VM approach will of course not only alert and explain the significance of a vulnerability – it will explain the severity and provide remediation steps. Ongoing communication occurs until tests prove the issue is resovled.



> “Brevity is key for Smart VM operations communications.”



Hi ,

A critical security vulnerability (CVSS Score 10) was noted late last week in Log4j (dubbed Log4Shell), which is a logging library used in a wide variety of application software and tools across the internet. For more information, please see the NIST advisory.

Current Situation

Exploit code has been shared on the internet and threat actors are actively scanni the internet for vulnerable hosts. Patches for this issue have already been release by most vendors and mitigating actions in-lieu of patching, have been published by many blue team resources.

Edgesca

Step 6 - Communicating When it Matters

Every year and all during the year the Media reports – or rather sensationalizes – dooms-day type headlines about discovered vulnerabilities. Like the noise generated with false positive alerts generated in scale with scanning engines – these media reports take the Enterprise off of their game dealing with real security issues.

Is False Vulnerability Media News Really a Problem?

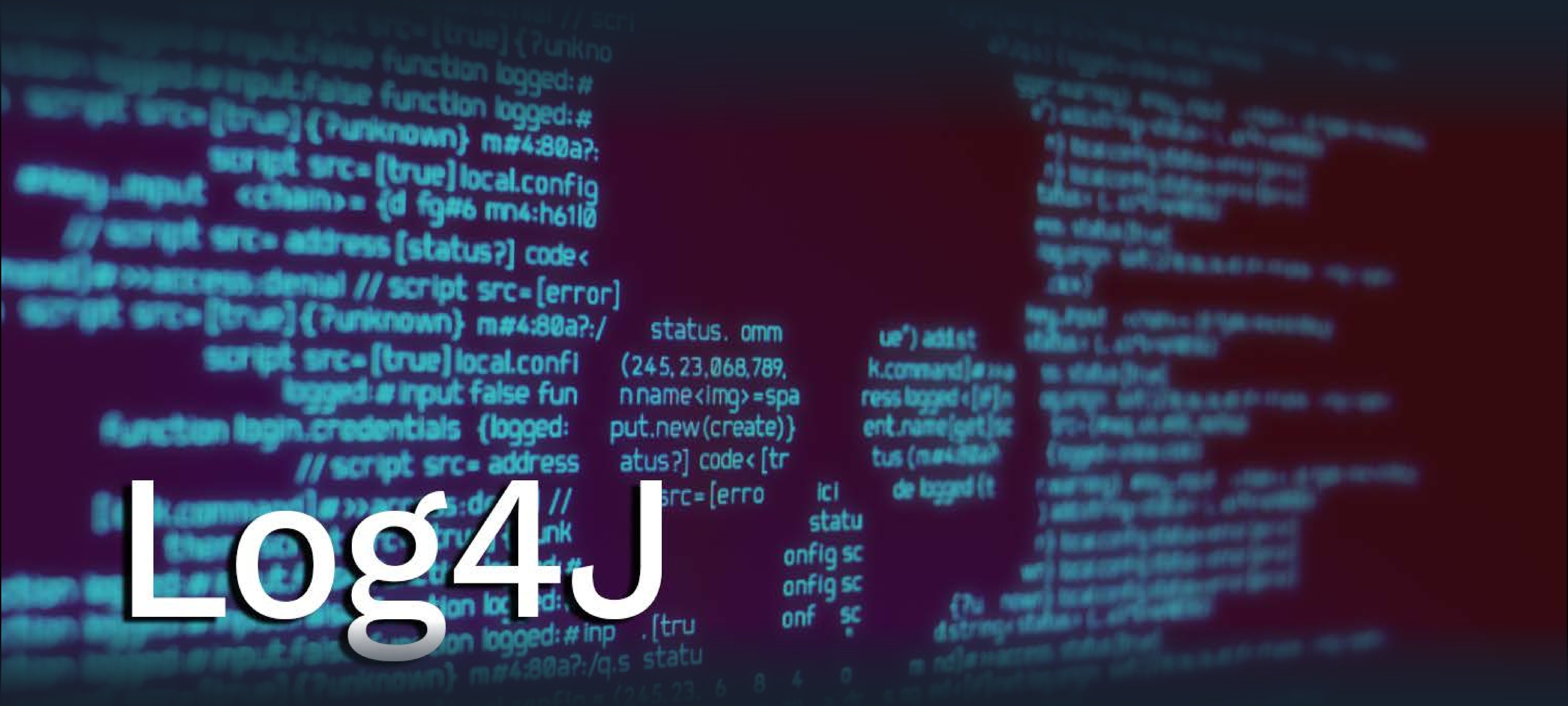
It's a serious problem. Typically, while there are on average about 200 media-reported vulnerabilities per year, there end up only being one to two vulnerabilities that actually live up to expectations. This creates a boy who cired worlf problem unless you are equipped with a Smart VM platform.

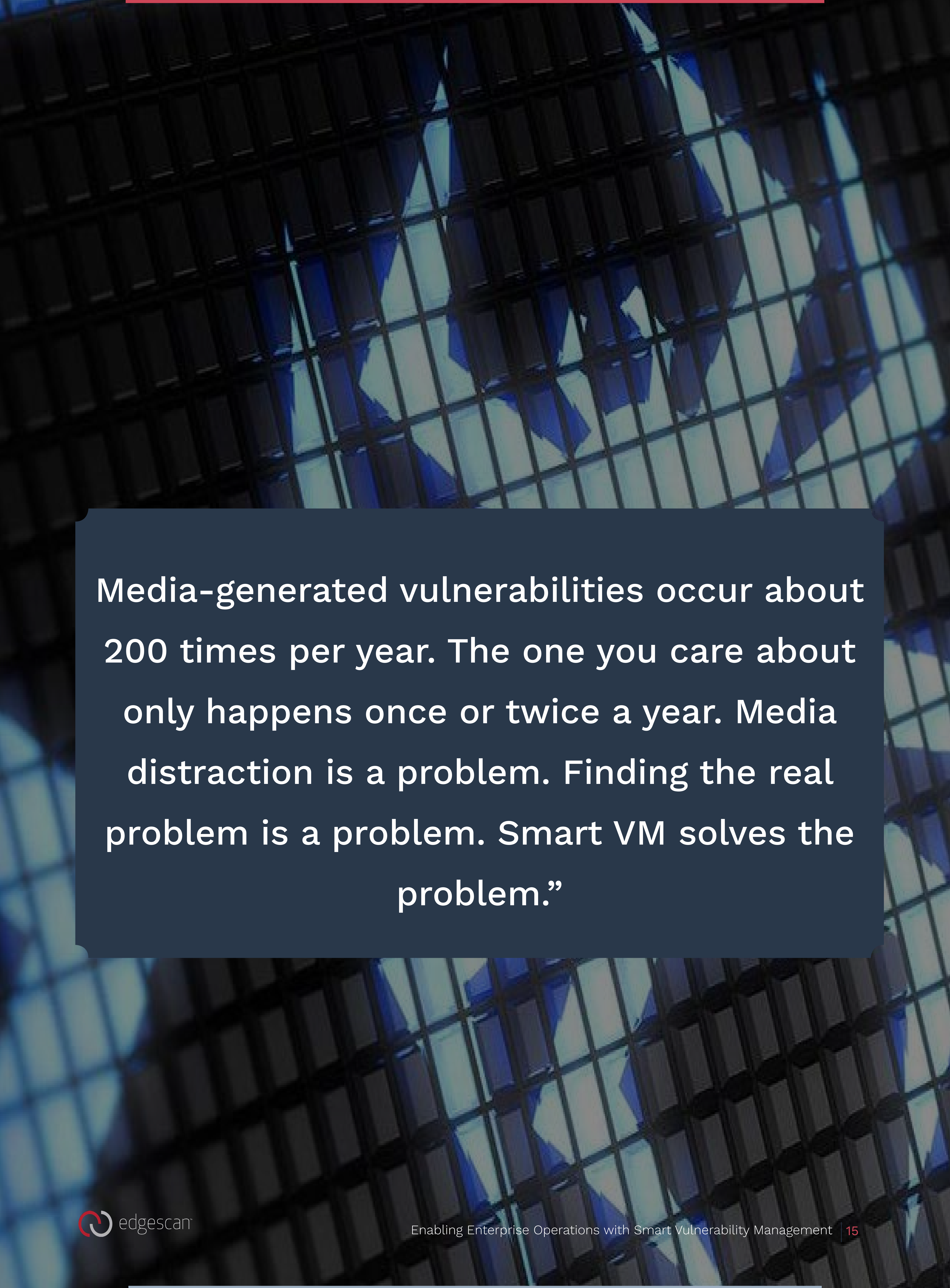
The Log4J Use Case

The Log4J vulnerability is a prime example of the once-in-a-year potentially catastrophic vulnerability that needs to be acted upon. It is not overstated, media-sweetened hyperbole. It is that once in a year issue. So an enlightened operational team armed with Smart VM will receive an accurate alert verifying its serious nature and timely guidance on level of impact for their organization and then a stream of communication from their Smart VM platform updating them on testing results and any other relevant locations that need to be dealt with.

Why Accuracy is So Important

While we highlighted the benefit of the Hybrid Approach with Smart VM to reducing alert noise, it is also extremely important in accurately determining that an issue like Log4J is at the Enterprise doorstep or already within – and that same expertise verifies that patches and remediation approaches are effectively taking away the issue throughout the entire vulnerability cycle.





Media-generated vulnerabilities occur about 200 times per year. The one you care about only happens once or twice a year. Media distraction is a problem. Finding the real problem is a problem. Smart VM solves the problem.”

Step 7 – Operational Performance Enhancement

Let’s now set the bar higher. Instead of attempting not to interfere with the daily workflow of the operational team – how could we get them to even perform better?

Morale Booster

If one really wants to destroy the soul of an Enterprise Support Team, then send them repeatedly chasing concerns off of security alerts that are not real issues. It’s almost debilitating to take on tasks to solve a problem that prove not to be problems at all. Alert fatigue is a real problem. That’s where the hybrid approach comes in – with expert validation all the noise is removed. When the Smart VM platform communicates a business-ranked alert and the Ops team adds a task to resolve – they do so knowing exactly what the concern is and why it matters and to repeat – that it is actually real. Solving real problems boost morale.

Resolution Enabler

And with that business-ranked alert comes specific remediation guidance. The experts in a hybrid Smart VM platform not only remove the false positives – they provide direct guidance on how to quickly resolve and test out the resolution to ensure it is effectively closed. In the case with the Edgescan platform – the operational staff can pick up the phone and talk directly to a world-class penetration tester who can speak to any technical dimension of the issue as well as the logic of say the technology in question.

Confidence in a Bottle

At Edgescan it is very noticeable when working with our clients – especially at the beginning of the engagement – that the client operational staff start getting used to the idea that every alert is real and every remediation step they take has a direct impact on improving operational resilience. Its inspiring.

> “Nothing kills performance more than sending the operational team after problems that are not problems.”

Step 8 – Getting Operations Strategic

And now we end on the most optimistic step. While we started with the basic requirement to normalize actionable data into the existing workflows of the operational staff without causing disruption – we now expect the operational staff to become fully integrated strategic partners.

Having Your Cake and Eating it Too

We started in this paper with the sobering reminder that most of the operational support staff are not cyber-security experts. But we end suggesting that adoption of a Smart VM platform in fact enables them with a strategic outlook – *how so?*

Timely and Contextualized Alerts

With a Smart VM platform – all of the Ecosystem practitioners – IT, Support, Dev Ops, Risk, Compliance and Business Operational staff - now have a holistic and accurate view of any issues across the full stack. With expert remediation integrated into their existing workflows and expert security advice only a phone call away – they now can strategically integrate security concerns into their operational programs.

Eyes on the Prize

The operational staff now are fully realized “Smart” Security practitioners. Now when making plans to deliver services and technologies to serve the overall business goals of the Enterprise –– they do so confidently, knowing that those business goals can be realized while the attack surface continues to evolve and new vulnerabilities arise. They have become active enablers of a Smart VM Program.

“Smart VM injected into Enterprise Operations creates strategic business goal-oriented teams.”