BETTER TOGETHER

John Matthews *on why converging security IT ops and cloud expertise holds the answer for better business outcomes*

Once, the job of Network Operations (NetOps) was to make sure the network was operating at its fastest and best. Security Operations (SecOps) made sure it was protected from all manner of hackers, vulnerabilities and cyber threats. And for that time, there has been a great gulf between these two departments – interacting at a distance and with little reference to what it's like 'over there'. That separation has robbed them of the top-down, strategic view we all to move forward.

In a 2019 SANS SOC survey nearly 50 percent of respondents said there was very little direct communication between NetOps and SecOps. This tired arrangement is based on a distinction between these two roles and that distinction is increasingly hard to make. The erosion of the traditional network perimeter and the rise of BYoD, the cloud, virtualisation and Everything-as-a-Service make it increasingly hard to continue to justify their separation.

Boundaries are no longer as clear as they used to be – and that goes for the disciplines of IT just as much as it does for the network perimeter. The 'ivory tower' approach that we've used for so long is just no longer tenable. In fact, it's all too wasteful for the lean, agile enterprise that digital transformation was supposed to bring about.

This isn't some marginal technical question – which the enterprise might survive without thinking too much about – but a real business concern. This is about waste of a kind which threatens the very future of an enterprise.

NetOps and SecOps share many of the same functions – network analytics, new device discovery and so on. However, because they exist separately, their tools are often duplicated, creating not just an overlapping arrangement, but a fundamentally confusing one too.

This doesn't just mean wasted efforts and budget spent on identical tools for two different departments, but it's a missed opportunity too: tool consolidation could enhance collaboration between the two departments.

Generally IT teams have more tools – they're larger and their remit is wider than their counterparts – but the superfluity of visibility tools ironically creates visibility gaps. IT teams might be able to see everything, but they won't always know what it means, especially when it comes to security.

The information that SecOps relies on often comes to NetOps first. And yet only when SecOps picks up on that intelligence is it actionable. Even before we reach the business outcomes for that disconnect – merely on a technical level – a network that has to acquire and store packets twice is wasting a tremendous amount of energy. A 2018 Dark Reading Survey found that in only 43 percent of cases did SecOps receive threat data first. More surprising was that in 2019 that number dropped to as low as 37 percent.

IT teams generally tend to have more visibility tools in their grasp, giving them a wider view of the network, but not necessarily the charter to use it for security-focused objectives. In fact, security often relies on data from IT teams for their investigations. Furthermore, IT teams know their machines intimately and are potentially more aware of what is and isn't abnormal behaviour, but they may not consider it their responsibility to leverage this for security purposes. If the business doesn't incentivise IT and Security to work together, all of this knowledge goes wasted.

Security is a highly specialised discipline, for which there is a yawning skills gap. Good security people are hard to find. From that point of view, it makes little sense to keep them hidden away. As we've said – there tend to be far more general purpose or otherwise specialised IT staff than security people and they also tend to be equipped with more tools to answer the kinds of questions that SecOps ask.

There also remains the simple fact that security skills are in short supply. According to the Cybersecurity Jobs Report, there may be 3.5-million empty security jobs by 2021. The security personnel that an organisation can afford come at a high price and we could always do with more. The cyber skills gap will yawn contemptuously in front of us for a while. Many noble efforts are being made to bridge it, but it remains stubbornly wide and deep. It's a speciality, certainly, but it could do with a little more democratisation. NetOps especially, who are trapped in their own disciplinary cell, could benefit greatly from cross-training in security, which in the long run may create new generations of security analysts.

As it stands, neither are capable of fully benefiting from the skills and capabilities of the other. NetOps cannot draw from the specialised knowledge and experience of SecOps – letting their estranged colleagues pick up the slack when it comes to protecting the network – and SecOps find it hard to draw on the size and strength of traditional IT. It's an amalgamation that would make the lives of both easier and the roles of both more effective.

> WHILE SECOPS LENDS ITS EXPERTISE, NETOPS CAN IN TURN LEND ITS CAPABILITIES

This trenchant distance ultimately means that neither department can live up to its full potential. SecOps and NetOps perform a variety of tasks that require collaboration, but so often that collaboration is like people shouting from two far ends of a room. Take policy compliance, for example. SecOps teams create policies and then NetOps go about implementing those policies – that distance leads to loose interpretations and poor implementations.

The same goes for incident containment and mitigation. When a breach happens, security often provides instructions on how to make the necessary changes, but the groundwork often lies with the NetOps teams. Without proper communication, important security changes can again be poorly implemented. This has a particular effect on visibility. SecOps often cannot see what NetOps can: aspects of poor security hygiene, such as weak ciphers or vulnerable ports, are not readily visible to them. Furthermore, SecOps need data from NetOps in order to do their job, creating an overly bureaucratic exchange in which the vulnerability window is enlarged and ultimately more time is wasted.

TIME MATTERS

All this boils down to wasted time. The numbers bear it out – in a 2018 IDG survey respondents listed what happens when they don't collaborate: 34 percent said that response to security events was slower, 32 percent reported an increase in breaches, 28 percent reported lost productivity and 27 percent increased service downtime. This is all happening at a moment when time matters more than ever. The speed of business is not slowing down, and time is more expensive. Further compounding that pressure is the cloud.

With it has emerged the Shared Responsibility Model. There are a number of different versions, but the arrangement mostly sounds like this: cloud providers will take care of the security of the cloud itself and customers will take care of the security of its data and their applications. The large majority of so-called 'cloud breaches' happen on the customer's end, not the cloud provider's.

Cloud Migration is one of the key steps in the modernisation of the enterprise. However, an all too common problem migrators face is something known as the Great Stall – the moment at which, after a period of successful cloudward movement, migrations suddenly stop. In fact, 70 percent stall after 15-20 percent migration and 20 percent never recover after that.

LACK OF VISIBILITY

That stall is principally about visibility. Security needs visibility into network traffic within the cloud to identify attacker behaviour and carry out forensics while NetOps have to manage network performance and untangle knots. The Great Stall often comes when either team decides that they cannot abide that lack of visibility. The introduction of this new environment has further created visibility gaps. Now, not only can SecOps not see what NetOps is seeing, but both have trouble seeing into the cloud.

That could stem from tool sprawl – cloud visibility tools often being different to the ones used on premises – or future challenges like TLS 1.3, which is going to make encrypted cloud traffic the norm. NetOps teams are still going to need to see into that traffic to optimise a network's performance and SecOps teams know that most attacks are now hidden within encrypted traffic – they'll need to see into it too.

From that point of view, what better excuse is there to join forces? That could mean they're physically pushed into the same working area and it could also mean involving NetOps in pentests and red team exercises to foster closer collaboration. Mostly, they're going to need to share so enterprises should set about bringing on tools and platforms that can be used by both to see into cloud traffic; data which can be shared and workflows that they collaborate on.

Furthermore, NetOps (as well as everyone else in the enterprise) should be deputised as security personnel. Security Hygiene is tremendously important for everyone to be cognizant of and NetOps teams, given their intimate knowledge of the network, make great threat hunters.

While SecOps lends its expertise, NetOps can lend its capabilities. SecOps needs the network visibility that NetOps possess, and NetOps sorely needs instruction on how to stop threats in their tracks. It's not quite as simple as flipping a switch. Instead, it takes a change in mindset.

The network no longer ends at the office door: part of it is working from home or in a coffee shop, another part of it is in a data centre and a great deal of it is up in the cloud. Treating the network as though it were still merely contained within the enterprise's HQ can be a grievous misconception. That could serve as a great opportunity for eager cyber criminals, and can increase the risk posed by misconfigured services, sloppy employees with poor security hygiene or undetected tranches of critical enterprise data.

> A NETWORK THAT HAS TO ACQUIRE AND STORE PACKETS TWICE IS WASTING ENERGY

Any cloud-first security strategy has to take into account that hybrid attack surface. The new recognition must incorporate all aspects of an enterprise's IT infrastructure, leverage SecOps expertise, NetOps capabilities and enable visibility into every part of that diverse, amorphous hybrid enterprise ●

John Matthews is the Chief Information Officer at ExtraHop Networks, where he oversees the continuous expansion of the ExtraHop IT environment and counsels the company's enterprise customers as they evolve their IT operations.