White Paper

Combining NetOps and SecOps into Risk Engineering

Holistic, Network Data-Driven Risk Management

Jason Bloomberg
President, Intellyx

January 2023

Organizations are finding that managing their networks, software infrastructure, and cybersecurity separately are leading to inefficiencies, cost overruns, and excess risk.

Bringing these efforts together, however, leads to an alphabet soup of combined efforts, including NetOps, SecOps, DevOps, and others.

To achieve effective collaboration requires a formal approach to managing risk across these different team efforts. Risk Engineering – the most important role of the NetSecOps team – brings these efforts together.

NetSecOps teams, however, require comprehensive, real-time data – telemetry that gives them insights into all aspects of managing risk. At the heart of such telemetry is packet data, the result of deep packet inspection that provides the least common denominator for all risk management efforts.

Packet data alone, however, lack sufficient context. To address this problem, NETSCOUT offers Adaptive Service Intelligence that enriches packet data with metadata in real-time, giving NetSecOps teams the context they require to make the most effective risk management decisions.

Making Sense of the Dev + Net + Sec + Ops Chaos

It seems that everybody today wants a piece of IT operations. Shortened to the single-syllable *ops*, we now have DevOps, DataOps, MLOps, SecOps, and NetOps – not to mention the triple whammies DevNetOps, DevSecOps, and numerous other combinations of techie-sounding syllables.

This ops insanity began with *DevOps* – originally a cultural and organizational movement that sought to bring development and operations together, but now focuses more on leveraging automation tooling to support continuous integration and continuous deployment (CI/CD) of software.

NetOps, in contrast, was simply shorthand for *network operations* – a critical, but well-established part of the IT operations landscape. Today, however, NetOps has evolved, bringing DevOps principles and tooling to bear to better automate NetOps tasks and processes.

NetOps is shorthand for *network operations* – a critical, but well-established part of the IT operations landscape. Today, however, NetOps has evolved, bringing DevOps principles and tooling to bear to better automate NetOps tasks and processes.

Adding security to the mix only adds to the confusion. DevSecOps seeks to bring the DevOps and security operations (SecOps) teams together in order to create and deploy more secure software. Meanwhile, NetSecOps embeds network security testing into DevOps CI/CD pipelines, thus representing better collaboration among the network security, development, and ops teams.

IT leaders who seek to strip away the noise and confusion over this petting zoo full of ops terms must focus on three core enablers that such combinations must exhibit:

- An organizational and cultural shift to greater collaboration and communication among dev, sec, and ops teams
- Ops tooling that provides consistent and coordinated management across network, operations, cybersecurity, and software deployment activities
- Common data that provide a single source of truth across all of these teams, empowering them to understand common risks and coordinate adequate solutions to problems that span the IT organization.

Of these three enablers, data are the most fundamental. Without a common set of telemetry that provides insight into the network, the software infrastructure, and applications as they move through their lifecycle to production, there is no way tooling can coordinate efforts. As a result, it becomes impossible for the teams to collaborate effectively.

Without a common set of telemetry that provides insight into the network, the software infrastructure, and applications as they move through their lifecycle to production, there is no way tooling can coordinate efforts. As a result, it becomes impossible for the teams to collaborate effectively.

The inherent complexity of today's IT environments requires such collaboration. Problems occur all the time and figuring out why there's an issue and how to fix it can require an all-hands-on-deck effort. Without adequate collaboration, such efforts devolve into finger pointing war room arguments that focus more on assigning blame than addressing the issue in question.

Simply telling people to collaborate doesn't work. Giving them the right tools helps but doesn't shift the needle sufficiently. Common data are the key, but people must still have the proper understanding of how to leverage the data to approach problems collaboratively.

Managing Risk Across Network, Security, and Ops

The key to solving complex IT ops problems collaboratively is to build a common engineering approach to managing risk across the concerns of the security, network, and ops teams – in other words, a holistic approach to managing risk.

By engineering, we mean a formal, quantitative approach to measuring and managing ops risks. The starting point for such an approach is *site reliability engineering* (SRE). SRE is a modern technique for managing the risks inherent in running complex, dynamic software deployments – risks like downtime, slowdowns, and the like that might have root causes anywhere, including the network, the software infrastructure, or deployed applications.

The ops team – now including NetOps – must be able to make fact-based judgments about whether to increase a service's reliability (and hence, its cost), or lower its reliability and cost in order to increase the speed of development of the applications providing the service.

Instead of targeting perfection, the real question is just how far short of perfect reliability should you aim for. We call this quantity the *error budget*. This budget represents the total number of errors a particular service can accumulate over time before users become dissatisfied with the service.

Most importantly, it should never be the operator's goal to entirely eliminate reliability issues, because such an approach would both be too costly and take too long – thus impacting the ability for the organization to deploy software quickly and run dynamic software at scale (both of which are core cloud native practices).

Instead, the operator should maintain an optimal balance among cost, speed, and reliability. Error budgets quantify this balance.

Bringing SRE to Cybersecurity

Reliability risk is only one facet of the risks facing the IT shop. Organizations should extend SRE principles beyond site reliability to all risks facing the software landscape, including network and cybersecurity risks.

The most fundamental enabler of this holistic approach is *observability*. Ops and NetOps personnel must have sufficiently accurate, real-time data about the behavior of the systems and services in their purview to perform the calculations they require to determine whether an organization is within its error budget.

The most fundamental enabler of Site Reliability Engineering is *observability*. Ops and NetOps personnel must have sufficiently accurate, real-time data about the behavior of the systems and services in their purview to perform the calculations they require to determine whether an organization is within its error budget.

SecOps engineers require the same sort of observability specific to the threats that they must manage and mitigate. Based upon this observability, SecOps engineers

must calculate the risk score for every observed event that might be relevant to them.

The risk score for any event is a product of the risk impact (how severe would the effect of the threat's associated compromise be), risk confidence (how confident the engineer is that the event is a positive indicator of a threat), and a risk modifier that quantifies how critical the threatened user or system is.

Risk scores give the SecOps engineer the information they need to make informed threat mitigation decisions, just as reliability-centric observability provides the SRE and NetOps engineers with the data they need to mitigate reliability issues.

The *threat budget* represents the total number of unmitigated threats a particular service can accumulate over time before a corresponding compromise adversely impacts the users of the service and thus the company as a whole. Threat budgets should never be 100%, since eliminating threats entirely would be too expensive and would slow the software effort down, just as 100% error budgets would.

Introducing the Threat Budget

Once SecOps engineers have a quantifiable, real-time measure of threats – threat telemetry, as it were – then we can extend the notion of error budgets to cybersecurity. Similarly, we can create the notion of a *threat budget* which

represents the total number of unmitigated threats a particular service can accumulate over time before a corresponding compromise adversely impacts the users of the service and thus the company as a whole due to loss of business, fines, or loss of intellectual property.

The essential insight here is that threat budgets should never be 100%, since eliminating threats entirely would be too expensive and would slow the software effort down, just as 100% error budgets would.

Some threat budget less than 100%, in fact, would reflect the optimal compromise among cost, time, and the risk of compromise.

Error budgets and threat budgets, however, are two sides of the same coin. They are both examples of approaches to measuring and managing two different, but related kinds of risks. Bringing threat management to the same level as SRE may very well help these two teams align over similar approaches to managing such risks.

The result is *Risk Engineering:* a coordinated risk management effort that brings together SRE and cybersecurity. Risk Engineering, in turn, requires a common effort among Ops, NetOps, and SecOps personnel – in other words, Risk Engineering becomes the primary focus of NetSecOps.

Risk Engineering Observability Starts with Packet Data

Both cybersecurity and SRE manage IT risks, and both leverage real-time observability data to do so. While the priorities of the Ops, NetOps, and SecOps teams vary, they share this mutual focus on risk and a common set of data.

At the heart of the observability data landscape available to these professionals are network data. After all, the network supports the software infrastructure and applications, and provides a medium for virtually all cybersecurity threats.

At the heart of network data for any IP-based network, in turn, are packet data. IP networks are ubiquitous, and thus packets carry all the data every organization

uses anywhere for virtually any purpose. Gain insight into packets, and you have insight into everything taking place across your IT landscape.

At the heart of network data for any IP-based network are packet data. IP networks are ubiquitous, and thus packets carry all the data every organization uses anywhere for virtually any purpose. Gain insight into packets, and you have insight into everything taking place across your IT landscape.

Leveraging packet data as part of comprehensive observability in support of Risk Engineering priorities, therefore, has several benefits to the organization:

- *Cost savings, or more generally, greater cost efficiencies* – Integrating NetOps and SecOps into a common NetSecOps team eliminates redundancy among people as well as tooling and facilitates a coordinated approach to Risk Engineering.
- *Improved mean time to repair (MTTR), or more generally, better network performance overall* – Unified NetSecOps teams spend less time troubleshooting, focusing more on problem resolution than assigning blame. Furthermore, improved focus on security threats that can impact availability and performance helps improve MTTR for those threats as well.
- *Balanced risk mitigation across network, security, and reliability risks* – by combining these priorities into a common Risk Engineering perspective, organizations can achieve better end-to-end visibility across on-premises and cloud-based resources, including front-end, middleware, and back-end assets.

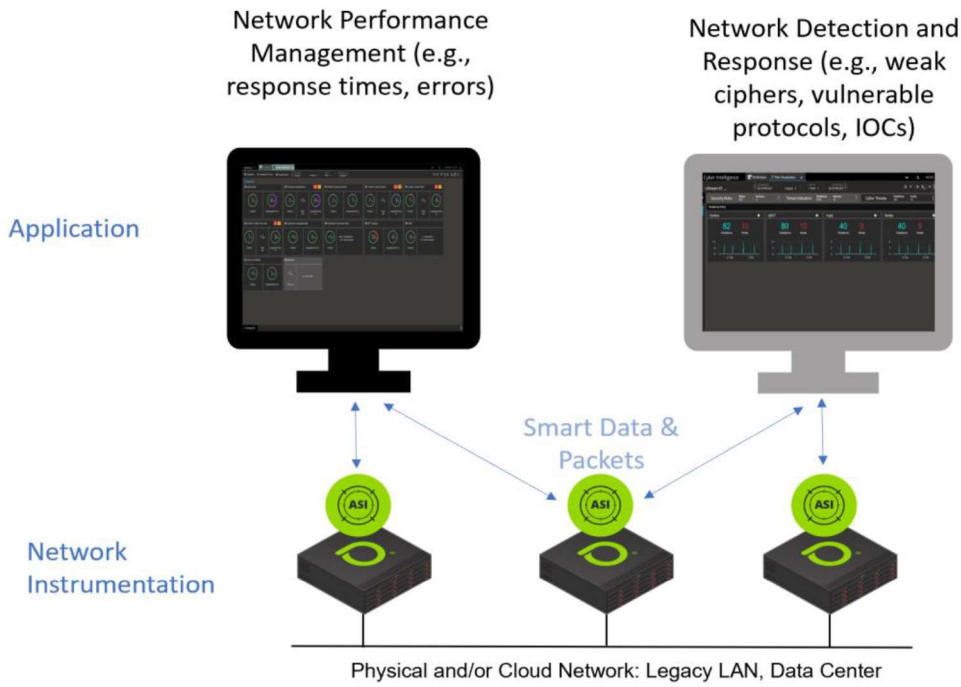
The complexity of this hybrid IT landscape presents challenges to such a holistic approach – challenges that network-level observability is uniquely positioned to address.

Implementing Risk Engineering with NETSCOUT

Deep packet inspection (DPI) refers to processing data within packets as they traverse a network and is thus the starting point for all packet-centric telemetry. DPI alone, however, lacks necessary context.

Looking at packet data isn't simply a case of looking at trees instead of the forest – it's more like looking at individual leaves on the trees. While packets make up everything that happens across IT, focusing solely on the contents of packets risks losing the application context that brings value to the data.

NETSCOUT addresses these scalability and context issues via its patented Adaptive Service Intelligence (ASI) technology, as the figure below illustrates.



NETSCOUT Adaptive Service Intelligence (ASI) Architecture (source: NETSCOUT)

NETSCOUT's Adaptive Service Intelligence (ASI) technology converts raw network packets into a source of locally stored, compressed packets and layer 2-7 metadata in real-time.

NETSCOUT calls this combination of packet data and metadata *Smart Data.* Smart Data include:

- Key performance indicators (KPIs) such as network or application error codes, response times, and results of cyber threat analytics at the time of packet capture
- Server discovery metadata along with details of all conversations between clients and services, (for example, attributes of source and destination IP addresses, ports, and IP protocols)
- Protocol-specific details, such as TCP (flags, response/latency times, etc.), DNS (domain queries and responses, response codes, sizes, flags, etc.), HTTP/S (error codes, URI, User Agent metadata, etc.), and TLS (error codes, certificate info, cipher suite, etc.).

ASI technology removes the burden associated with packet analysis by automatically uncovering intelligence that exists within the network packet. NETSCOUT Network Performance Management and Network Detection and Response applications analyze these Smart Data for their respective network and cybersecurity use cases.

NETSCOUT ASI creates a common and consistent source of metadata that enables network and security teams to speak a common language and build an engineering approach to managing risk across the security, network, and ops teams – in other words, a holistic approach to managing risk.

The Intellyx Take

It is axiomatic that both perfect networks and invulnerable systems are impossible – or in other words, these holy grails of technology are infinitely expensive.

What is less axiomatic – and even controversial – is that there is an optimal level of imperfection for networks, cybersecurity, and for operations in general. We actually *want* to fall short of perfection, because putting too much effort into such lost causes would cost too much and slow down the ability of the IT organization to deliver business value.

This optimum – the error budget – shouldn't reflect a single type of risk. Instead, we must engineer our systems across the board to measure and manage risk in a comprehensive manner, or we'll never achieve the optimal balance among risk, cost, and time.

SecOps and NetOps teams must collaborate to achieve this balance, but in order to do so, they require common telemetry that provides complete insight into the behavior of the systems under their purview. In other words, they require deep packet data.

Such data are the least common denominator for operational telemetry. No data go deeper or provide a more comprehensive view of what's really going on.

As long as SecOps, NetOps, and the NetSecOps team focused on Risk Engineering have the proper context like the Smart Data that NETSCOUT delivers via its Adaptive Service Intelligence (ASI) technology, they will be able to quantify, balance, and optimize the risks facing the entire IT organization.

About the Author: Jason Bloomberg

Jason Bloomberg is a leading IT industry analyst, author, keynote speaker, and globally recognized expert on multiple disruptive trends in enterprise technology and digital transformation.

He is founder and managing partner of Digital Transformation analyst firm Intellyx. He is a leading social amplifier in Onalytica's Who's Who in Cloud? for 2022 and a Top 50 Agile Leaders of 2022 by Team leadersHum. He was ranked among the top nine low-code analysts on the Influencer50 Low-Code50 Study for 2019, #5 on Onalytica's list of top Digital Transformation influencers for 2018, and #15 on Jax's list of top DevOps influencers for 2017.

Mr. Bloomberg is the author or coauthor of five books, including *Low-Code for Dummies*, published in October 2019.

About NETSCOUT

NETSCOUT SYSTEMS, INC. (NASDAQ: NTCT) protects the connected world from cyberattacks and performance disruptions through advanced network detection and response and pervasive network visibility. Powered by our pioneering deep packet inspection at scale, we serve the world's largest enterprises, service providers, and public sector organizations. Learn more at www.netscout.com or follow @NETSCOUT on LinkedIn, Twitter, or Facebook.