TANIUM

IT Analytics: The Foundation for Cyber Hygiene

Tools and best practices for a healthier, more secure distributed enterprise.

Cyber hygiene describes a set of practices, behaviors and tools designed to keep the entire IT environment healthy and running at peak performance. Robust security depends on cyber hygiene.

This eBook describes the foundations of cyber hygiene in the context of data and analytics. What data do you need, and how can you use it to make the most informed, effective IT decisions for your organization?

Chapter 1: The disconnect between tools and policy

Analytics and fresh data can highlight the disconnect between tools and policy. People become attached to and comfortable with certain tools, so it's very common that they create policies around what their tools can do instead of what the situation requires. Entire careers and partner ecosystems are built on the ability to use and maintain certain tools for certain purposes.

Here's a common scenario. Before deploying Tanium, some of our customers had 12-hour maintenance windows in which to patch their devices and get them up and running. The maintenance window was 12 hours because they couldn't do it any faster with the tools they used.

When we demonstrate this can be done faster and more efficiently with less downtime, management sees the business value of that. Engineers usually want to stick with the tools they've been using. It often takes a business driver — backed by data — to force a change.

Chapter 2: Operations and security. Collaborators or competitors?

In a perfect world, the work of IT operations and security would coalesce into one seamless, joint effort. But in most organizations, there's a fairly sharp dividing line between the two.

At Tanium, you'll often hear the operations team say to security, "Our job is hygiene and if we do it right, it makes your life easier." And it's true. Because then the forensic analysts, the threat hunters, can focus on bigger threats — like nation-state hackers — instead of the commodity malware that gets caught by antivirus (AV) or the alerts based on a known patch.

The tension between operations and security comes from different worldviews. Security wants to lock everything down. Operations wants the environment to be secure but open enough to allow the organization to maximize performance at every opportunity. Patching and vulnerabilities are usually where conflicts arise because these things live in the "netherworld" between operations and security.

On the operations side, tools exist to deal with those things before security ever sees them. If you're doing your job on the operations side, when security says, "Here are the vulnerabilities we found," it should be a very small number because you're not waiting for them to tell you what to patch.

Then, of course, is the user experience. Have you consumed so many system resources with security tooling that users can't do anything? Is memory blown out? Are applications crashing? You need to have a way to measure user experience. There are no industry standards for user experience, so you have to set your own.

Analytics should be the common language of operations and security

IT analytics is an extremely broad topic since IT is spread across several areas, including computing, user experience, infrastructure, storage, and networking. Analytics has different meanings depending on what it's applied to and for whom the results are intended.

For example, if we think about the end-user experience, IT analytics can provide the boot time of a device, the application launch or response time, as well as application crashes over a period of time, a set of devices or a department.

With a remote workforce potentially using virtual desktops, you might look at the trend of storage use over time and how WFH has or could influence infrastructure spending for the next 6, 12 or 18 months.

Analytics is about maintaining your ability to discover relevant data, making sure endpoints are delivering the right kind of reporting when queried and accurately describing the capability of the network.

Analytics provides the hard data you need to measure network performance. Operations uses that data to maximize business productivity. Security uses it to better protect the organization from threats. Analytics is equally critical for operations and security. A platform approach to tooling, rather than a point solution, can build a bridge between operations and security.

Chapter 3: What is good cyber hygiene?

Good cyber hygiene is knowing what you have and controlling it. Do you have the software licenses you need? Are you out of compliance and at risk for penalties? Are you paying for licenses you're not using? Are your endpoints configured properly?

To assess your cyber hygiene, ask the following questions:

- What endpoint devices do you have?
- Are those endpoint devices being managed?
- Do managed endpoints meet the criteria set for a healthy endpoint?

Think of endpoints in three categories: managed, unmanaged and unmanageable. Not all endpoints are computers or servers. That's why good cyber hygiene requires tools that identify and manage things like cell phones, printers and machines on a factory floor. There's no single tool that can identify and manage every type of endpoint. But the more visibility you have, the better your cyber hygiene and your risk posture.

Work from home (WFH) made visibility much harder. If endpoints aren't always on the network, how do you measure them? Many tools weren't built to manage that. But once you know what devices you have, where they are and what's on them, you can enforce policies that ensure devices behave as they should.

Good cyber hygiene also requires that you patch and update software quickly. When Microsoft Patch Tuesday comes around, can you get critical patches on all your devices in a reasonable period of time? Will you know in real time what's been patched and what hasn't?

That way, when security comes to operations and says, "There's a zero-day flaw in Microsoft Word, how many of your endpoints have this version?" operations can answer, "We know, and we've already patched it." That's the role of visibility in cyber hygiene.

Or, if the chief financial officer (CFO) says, "We're burning money on Adobe Acrobat. Are we really using all our licenses?" These types of questions can be answered with the consistent practice of cyber hygiene.

Chapter 4: Data freshness is the key to effective analytics

The importance of data freshness, or the definition of it, is not uniform across IT operations. For example, if hardware is on a low refresh cycle, such as two or three years, it's not significant if central processing unit (CPU) or hard drive model data is a month old.

But if you're making decisions about retiring servers or migrating workloads from a physical to a virtual environment, data that is days old will very likely cause problems. You could be retiring a server a business unit that depends on or moving workloads that support a critical service.

With real-time data, you're in a much better position to act.

Here's an example. Tanium had a customer engaged in the Federal Risk and Authorization Management Program (FedRAMP) certification. To maintain certification, they performed an audit for the federal government once a year.

Every six months, they paid an outside auditor to see how close they were to passing or failing the audit. Passing the audit was crucial. Failing the audit put tens of millions of dollars in revenue at risk.

A great place to start. Six cyber hygiene best practices.

For a big picture view of what data, analytics and cyber hygiene can do, here are six best practices that encompass the fundamentals of cyber hygiene:

1. Create an accurate inventory of everything that's connected to your network, managed and unmanaged.
2. Document what's on devices: software, data and processes.
3. Assess vulnerabilities and patching status to determine risk posture.
4. Make sure third-party software — Adobe, Microsoft Office, Google Chrome, etc. — gets the same attention as operating system (OS) software.
5. Don't neglect configuration management. Know where group policies are being applied and make sure all devices meet the minimum requirements.
6. Lockdown access controls to services and devices. Remove local admin rights by giving employees limited self-service capabilities to install software through a controlled interface.

By doing these six things, you'll get a sense of where to focus your efforts to provide better hygiene to the organization. For example, if your workstation devices have a worse risk posture than your servers, you know to look at end-user compute devices. This typically means making sure OS and third-party software patching are diligently applied.

Then they deployed Tanium to check every four hours on the status of elements that would be part of the audit. This switch from getting information every six months to every four hours meant that engineering, operations and dev-ops teams, which were making system changes constantly, could see the impact changes have on system audit readiness. With fresh data, the customer knew every day how their systems were operating in relation to passing or failing the audit.

Old data lies

Old data is almost never accurate, so decisions based on it are very likely to be wrong.

Old data is almost never accurate, so decisions based on it are very likely to be wrong. Regardless of the data set, whether it's about patching, compliance, device configuration, vulnerabilities or threats, old data is unreliable.

The rate of change in IT makes fresh data vitally important. If your data is even a week, let alone months old, you'd be better off licking your finger and holding it to the wind rather than making decisions based on 90-day-old data, which doesn't tell you the current state of your applications, workloads, customers — or potential risks from cyberattacks.

One of our hospital customers hadn't updated its configuration management database (CMDB) in 90 days. That's like flying an airplane on 90-day-old instrument data. And that really understates the problem.

Pilots don't have to worry about a new mountain or a new skyscraper popping up every couple of weeks. But in IT, the equivalent of a new mountain can emerge in hours or days.

Pilots don't have to worry about a new mountain or a new skyscraper popping up every couple of weeks. But in IT, the equivalent of a new mountain can emerge in hours or days.

The hospital was deciding which workloads to shut down, virtualize or move to the cloud based on 90-day-old data. Then Tanium gave them timely and accurate data. They went from using obsolete data to data that was one day old. From guessing to informed decision-making.

Chapter 5: IT analytics and network data capacity

Whether you're a 5,000- or a 100,000-endpoint shop, streaming huge quantities of real-time data requires network bandwidth to carry it. You may not have the infrastructure to handle real-time data from every system you're operating. So, focus on the basics.

That means, as an organization, you need to understand and identify the core business services and applications most in need of fresh data. Those are the services that keep a business running. With that data, you can filter out the noise and see what your IT operations and security posture look like for those systems.

To simplify gathering the right data, streamline workflows

Once you've identified your core services, what do workflows look like with your tooling? Most organizations are in the mindset of "My tools dictate my workflow." That's backward.

Articulate the goal. You want a high-performance network that has low vulnerability and strong threat response. So, you want tools that can service your core systems, do efficient patching, perform antivirus protection and manage recovery if there is a breach. That's what your tooling should support.

Your workflows should help you weed out the tools that are not a good operational fit for your business.

Chapter 6: Analytics and the user experience

When something breaks, you must have a way to measure its impact. Let's say you've closed 10 endpoint vulnerabilities. Are your applications crashing or using more resources? Do you have more systems sitting at 100 percent CPU usage than you did before? That means nobody can use those systems. This is where you need analytics. Otherwise, you're just guessing. You can't depend on users for timely, reliable information.

You can't depend on users for timely, reliable information.

To take some of the burden off the service desk, many large organizations give all users admin rights. But that can affect security tooling on your endpoints. It's a shortcut organizations use to have fewer service desk calls and reduce user frustration because they can't identify systems ahead of time that are likely to have problems. They have nothing to measure resource utilization, which is done regularly on servers but not on user devices. So, they're clueless about user experience.

Performance metrics are critical. For instance, when the security team wants to install five more agents, operations can show user systems that are already running at 75 percent of maximum capacity. Add those tools and users won't be able to work. Those are the analytics that support business decisions.

It's important to find tools that support your policies. But an often-overlooked part of that support is the ability for the tool to provide real-time information to engineers in a format that tells them whether policy goals are being met.

Chapter 7: Analytics for the C-level

The primary concern of C-level executives is "Can my users do their jobs?" Many IT decisions are based on risk — risk of IT systems getting in the way of employees being able to work. But making those decisions without supporting data leads to trouble.

You can't make decisions based on what some users say and project it to the entire organization. So, you need to ask yourself, "Can my users do the job they're hired to do, and are my devices secure?" Where is that line for your organization? That's what C-level executives need analytics for.

Some organizations only patch operating systems because they feel there's too much risk of downtime if they patch productivity applications like Microsoft Office. They have no way to test them, so they don't patch. And they believe their systems can't be breached from one of these applications, which is not true. They're not drawing the line between security and usability based on data.

Executives need summary analytics

This is where executive-level dashboards that display easily consumable key indicators of IT health can help them figure out with data where to draw the line between security and operational risk.

For example, if a key indicator shows 20 percent of organizational systems are missing critical patches, that's cause for concern. Nevertheless, if the dashboard shows that last month the figure was 50 percent, the trend is headed in the right direction. Dashboards need to show the current state and the historical trend.

Here are three key indicators an executive dashboard might include:

- Percentage of systems with baseline security tooling.
- Percentage of systems vulnerable due to missing patches.
- Percentage of systems performing above or below a defined performance threshold — CPU, RAM, disc utilization, etc.

If there's a problem at the summary level, executives can alert their IT teams to dig into it. They don't need to know the details; they just need to know that approved thresholds or standards aren't being met.

Targeted operational analytics for C-level executives

For chief information officers (CIOs) and CFOs, the role of analytics can be somewhat narrower. CIOs need analytics to tell them what IT issues impact a business service or revenue-generating application over time. How many application crashes, and CPU and memory alerts, are affecting the IT components that deliver the service? And how is the user experience affected?

Another important metric for CIOs relates to cause and effect. Are 30 percent of users having performance issues or application crashes after changes are made during a maintenance window? This level of analytics is extremely important from the business services side as well as employee experience.

CFOs may have a financial or legal issue around license compliance. How many Windows 10 licenses are they paying for? Or is the customer billing service operating properly?

The chief marketing officer (CMO) of an ecommerce company needs to know if its customer website is running properly. Maybe it's being overwhelmed with orders on Black Friday.

The chief information security officer (CISO) wants to know about patch levels. Resolving this diverse group of performance issues all depends on fresh data for accuracy.

If organizations have tools that can access this data quickly, the next step is building a data visualization layer that won't overwhelm executives with detail.

Chapter 8: Analytics for engineers

It's critical when an issue arises that engineers have access to real- or near-real-time data on all their systems in one place. Without it, they're forced to spot-check systems or wait until they get the next scheduled report. They end up not knowing what's accurate and what isn't. The engineering team should always know about problems before leadership does. Ideally, before an issue hits the executive dashboard, it's resolved.

The engineering team should always know about problems before leadership does. Ideally, before an issue hits the executive dashboard, it's resolved.

Analytics at work

An example of hygiene informed by analytics would be metrics such as mean time to patch (MTTP) and mean time to remediation (MTTR) for vulnerabilities. Many organizations track MTTP to make sure they're under a specific threshold month-over-month. That supports compliance with whatever regulatory mandates apply to their industry.

Other metrics that apply to IT hygiene could be usage patterns, credential authentication and who's logging in where, which applies to security as well. The end result is addressing vulnerabilities and removing any software from endpoints that don't meet or surpass guidelines.

Analytics supports alerting and baselining

Alerting is one of the areas Tanium is leveraging in its partnership with Salesforce. It's a crucial diagnostic tool that saves IT time and money.

For instance, if a Tanium customer uses Enforce or Performance Monitoring and an issue arises, like a critical machine's CPU use is off the charts, it generates an alert, which takes the burden off IT to search for problems. Baselining goes hand-in-hand with alerting because alerts must have thresholds.

Baselining goes hand-in-hand with alerting because alerts must have thresholds.

There are several ways to set thresholds. One approach is "automatic" baselining. If an organization thinks its environment is relatively healthy, the current state is the baseline.

So, it sets up alerts to notify IT when something varies from that. That could be CPU or memory spikes or a changed software version on an endpoint. Analytics can play an important role here by helping organizations determine whether "normal" is the same as healthy.

It really comes down to configuration. Your tools should tell you what a healthy endpoint looks like and that's the baseline. Alerts tell you when something happens that changes the baseline state. You need the kind

Your tools should tell you what a healthy endpoint looks like and that's the baseline.

of data that lets you set thresholds with a reasonable margin, allowing some deviation due to normal activity. Without that, you end up with "alert storms," and people stop paying attention.

Conclusion: IT analytics supports data-driven decision-making

Data-driven decision-making (DDDM) is just what it sounds like. DDDM uses facts, metrics, and data to guide strategic business decisions that align with goals, objectives, and priorities. If organizations can realize the full value of their data, everyone is empowered to make better decisions.

When you look at why IT analytics and DDDM exist, it's because executives often make decisions based on a hunch. Sometimes, maybe often depending on the executive and the context, their hunches are correct. For example, Fred Smith has an insight into the transport business and, despite widespread skepticism, creates Federal Express. Michael Eisner hears a pitch for an offbeat game show, and based on his gut, commits millions to developing *Who Wants to Be a Millionaire?*

But gut instinct is not how we want to consistently operate an enterprise. Data is a much more reliable foundation for decision-making.

A modern approach

The purpose of this eBook has been to explain the importance of data and analytics to achieving good IT hygiene, which in turn improves and supports an organization's security posture. As we've outlined, analytics based on real-time data informs immediate business decisions while closing gaps in visibility and resilience. It's an approach that benefits operations and security.

Learn more about how Tanium provides high-fidelity endpoint data and analytics to inform critical IT decisions at tanium.com.