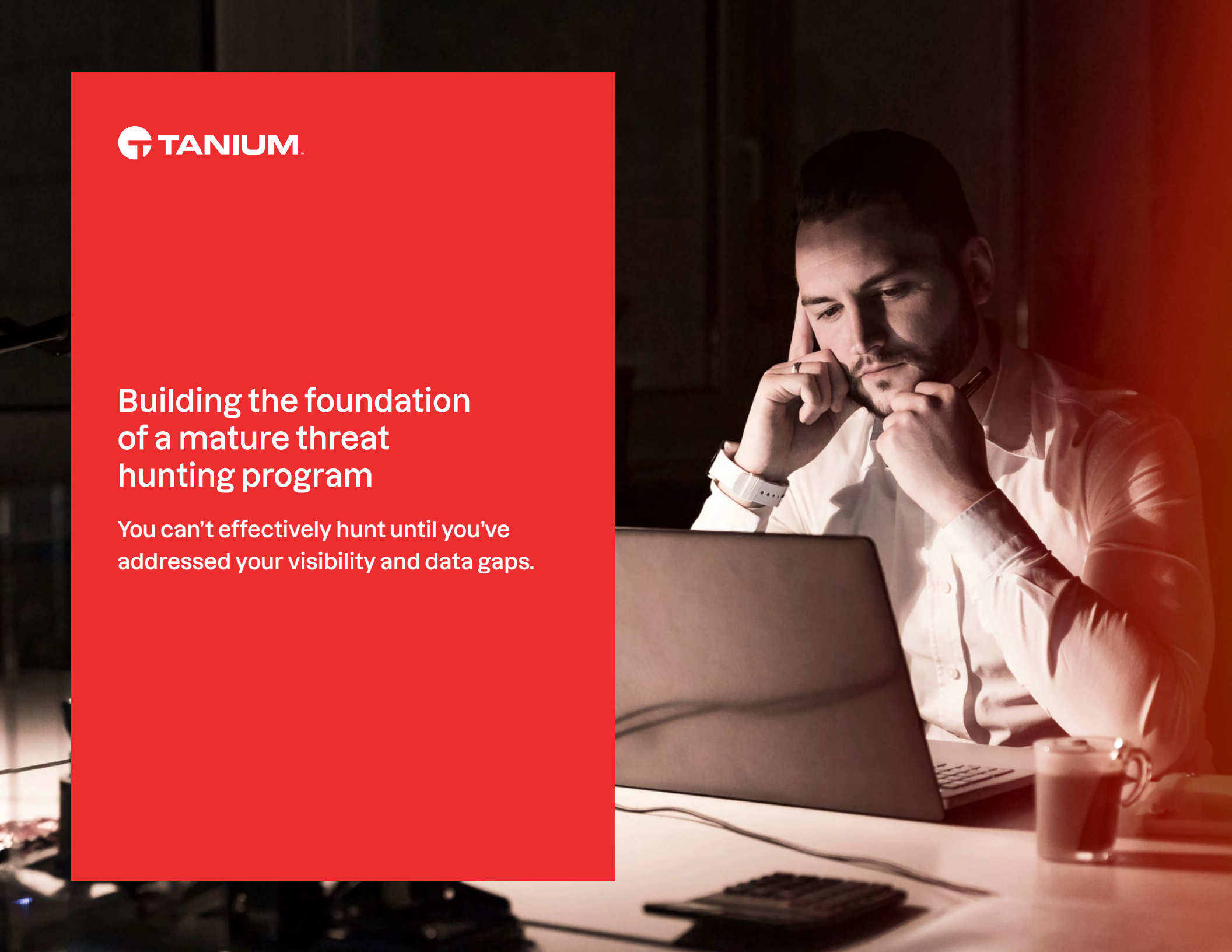

TANIUM

Building the foundation of a mature threat hunting program

You can't effectively hunt until you've addressed your visibility and data gaps.

Building the foundation of a mature threat hunting program

A cybersecurity executive's job has never been an easy one. But the challenges are especially daunting these days. The number, variety and severity of threats seem to be constantly growing, and these are coming from multiple sources.

Attacks are more sophisticated than ever, with hackers and other cybercriminals able to find and exploit the smallest (or unpatched) vulnerabilities to gain entry into corporate environments.

They're learning new ways to gain entry into IT environments without security teams even being aware of their existence, so they can inflict damage or steal data for profit.

In addition, security leaders and teams are responsible for protecting increasingly complex IT environments that often include multiple cloud services, a growing number of mobile devices and apps, an expanding ecosystem of connected objects, and a growing number of remote and hybrid workers.

As if all of that were not enough, companies also need to be aware of an increase in supply chain attacks which can have a multitude of effects on the business.

If an enterprise suffers a data breach, ransomware attack, or other incident, the damage can be significant. It can include not just the immediate financial impact from the loss or theft of data and business downtime, but harm to a company's reputation and brand and competitive position.

For companies in industries such as software development, pharmaceuticals, aerospace, auto manufacturing, entertainment, and others, attacks can result in the theft of intellectual property or creative property. This can also have a serious impact on revenue.

Supply chain attacks on the rise

But today's threat actors are using more refined approaches than just ransomware. Supply chain attacks are a particularly notable problem because they affect more than one organization and can be more complex.

Research shows that companies are aware supply chain vulnerability is an issue, but many are doing nothing to protect themselves. A study by BlueVoyant[1] shows that of the 1,200 organizations surveyed in multiple countries, 93% said they have suffered a cybersecurity breach because of weaknesses in their supply chain or third-party vendors. Ninety-seven percent reported they have been negatively impacted by a cybersecurity breach that occurred in their supply chain.

Fortunately, the situation looks to be improving in terms of awareness. In 2020, 31% of companies said supply chain and third-party cyber risk was not on their radar, and this year only 13% of companies said third-party risk was not a priority. In this year's survey, it's clear that priorities have shifted in response to a rapidly evolving threat landscape, the researchers noted.

Still, awareness doesn't always equate to action. Organizations need to take steps to improve their ability to hunt down and stop attacks before they can do damage. They need to be proactive to the point where they anticipate the moves of bad actors and stop them before they can gain the foothold they need.

With today's cybersecurity reality, threat hunting is no longer a nice-to-have option, but a must-have for the modern security program.

[1] https://www.bluevoyant.com/resources/managing-cyber-risk-across-the-extended-vendor-ecosystem/

Basics of an effective threat hunting program

Simply backing up systems is not the answer when the threats include extortion, brand damage, and financial, legal, and other repercussions. Nor is operating a cybersecurity program that virtually ignores threats coming from the supply chain.

Many organizations, especially large global enterprises, don't always have the best visibility into how many third-party vendors they are using at a given time, or what types of assets are in their environment because of those third-party vendors. In addition, they are at the mercy of their third-party partners' security as well as their own.

To address the growing challenges, organizations need to build the foundation for a mature threat hunting program. Several key components make up a foundation for threat hunting.

One is to maintain a complete, real-time picture of the enterprise environment so threats have nowhere to hide. If a cybersecurity team can't see the threats in their organization's environment, then it can't take steps to stop them.

This is not easy to achieve. The diverse, dynamic, and distributed endpoints in use today create a complex environment where threats can easily hide for days, weeks, or even months. Organizations need to deploy a solution that enables them to:

- Find every endpoint in the environment and know if it is local, remote, on premises or in the cloud.
- Identify active users, network connections, and other data for each of the endpoints.
- Visualize lateral movement paths that attackers can follow to access valuable targets such as Active Directory.
- Verify if policies are set on each of the endpoints and identify gaps in key controls.

Another foundational component of threat hunting is having the ability to proactively hunt for known or unknown threats across the environment within seconds. Once a security team can see the environment, it needs to be able to differentiate between normal and abnormal behavior to identify active threats.

With the right threat hunting platform, teams can:

- Search for and discover new, unknown threats that signature-based endpoint tools miss.
- Hunt for threats directly on the endpoint, instead of through incomplete logs streamed to the cloud.
- Investigate either individual endpoints or the entire environment in minutes without creating large network strain.
- Determine the exact root cause of any incident experienced on any endpoint devices.

A third foundational component is being able to respond to and eliminate any threats that the team finds within the same unified platform.

Simply finding a threat is not enough; teams need to eliminate the threat. Unfortunately, most endpoint tools separate threat hunting from remediation, which can create friction between teams, delay the response, and leave threats active.

With the right solution, security teams can:

- Seamlessly pivot between threat hunting and response by leveraging a single dataset and platform.
- Rapidly apply defensive controls to any number of endpoints during an incident.
- Completely cut off communications and remove an attacker from your environment.
- Learn from incidents and harden the environment to prevent similar attacks.
- Simplify and streamline policy management to keep endpoints in a “known good” state at all times.

Getting smarter about security

One of the most important factors to look for in a threat hunting solution is the ability to use correlation and statistical analysis to better understand whether a particular event is notable and interesting versus "just another alert." That's possible only when a system can enrich data telemetry in real time, at scale and in a constantly changing situation.

Every log source, every piece of telemetry, every bit of endpoint metadata and traffic flow that can be aggregated tells a different piece of the story. No threat actor can get into an organization's environment and be completely invisible. It's just a matter of whether the threat hunters are leveraging the right data.

Historically, security monitoring and threat hunting can be hindered by lots of noise if it's not tuned and not looking for the appropriate baseline. How can hunters know if something is out of place if they don't understand what it should look like?

This illustrates the importance of having good, high-confidence, threat intelligence and following the right feeds. Enriching alerts with real-time intelligence might not always be easy, but it is definitely important. The key is to have trusted, dynamic sources of data and the ability to tune and filter the data to lessen not only the false positives but also the false negatives.

Bad actors are getting more and more sophisticated in their attempts to outsmart monitoring tools and security policies. Once they get into a network, their goal is to blend in. They have the benefit of time and can be slow and deliberate to avoid detection, or rapidly change course in reaction to your defenses. They can watch the traffic on the network and learn how it behaves normally, so they can learn how to blend in.

Despite an adversary's best efforts to appear normal on the endpoint, they will eventually take an abnormal action in pursuit of their objectives. This creates a prime hunting landscape. To be great hunters, security teams need to advance in their ability to find and stop threats before they become a problem.

That's especially true given the growing threats against supply chains. The attack surface is constantly growing and shifting. Maintaining visibility of networks, devices, assets, and other components of the modern digital business — and eliminating any gaps in visibility — is vital.

Once an organization has that complete visibility in real time, it can start building an effective threat hunting strategy on top of that because it will know that it has the necessary data to hunt efficiently.

At a basic level, the idea behind threat hunting is that hunters are going out to look for suspicious behavior itself, not relying on what another tool is going to surface as an alert. They are looking at behaviors. While a given behavior by itself might look completely innocuous, when coupled with real-time data at scale and a pattern of behavior around it, it should set off alarm bells.

Because attackers are smart, especially the sophisticated ones who can change their behavior on the fly, hunters must be even smarter. That means using a combination of experience, knowledge and technology tools that give hunters the ultimate edge.

Learn more about **Tanium's Threat Hunting solution** and **sign up for a free trial today.**

Tanium is the platform that organizations trust to gain visibility and control across all endpoints in on-premises, cloud and hybrid environments. Our approach addresses today's increasing IT challenges by delivering accurate, complete and up-to-date endpoint data — giving IT operations, security and risk teams confidence to quickly manage, secure and protect their networks at scale. Tanium's mission is to help see and control every endpoint, everywhere. That's the power of certainty.

Visit us at **www.tanium.com** and follow us on **LinkedIn** and **Twitter**.