WHAT IS **ACTIONABLE INSIGHT?**

THE COMPLETE GUIDE

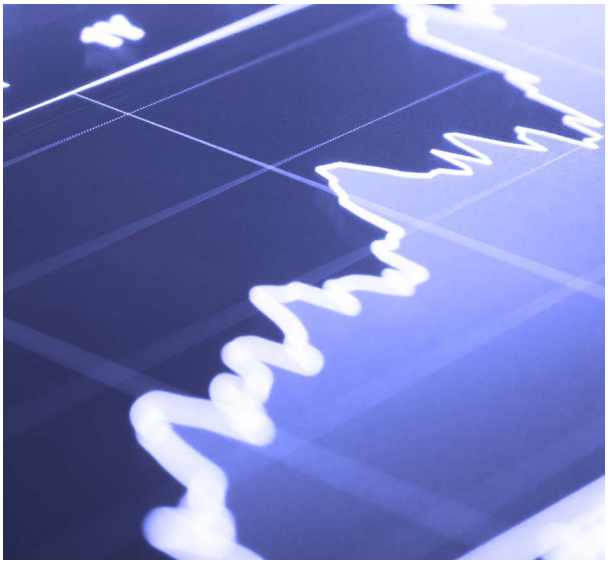
CONTENT

CORE SECURITY

CH:01

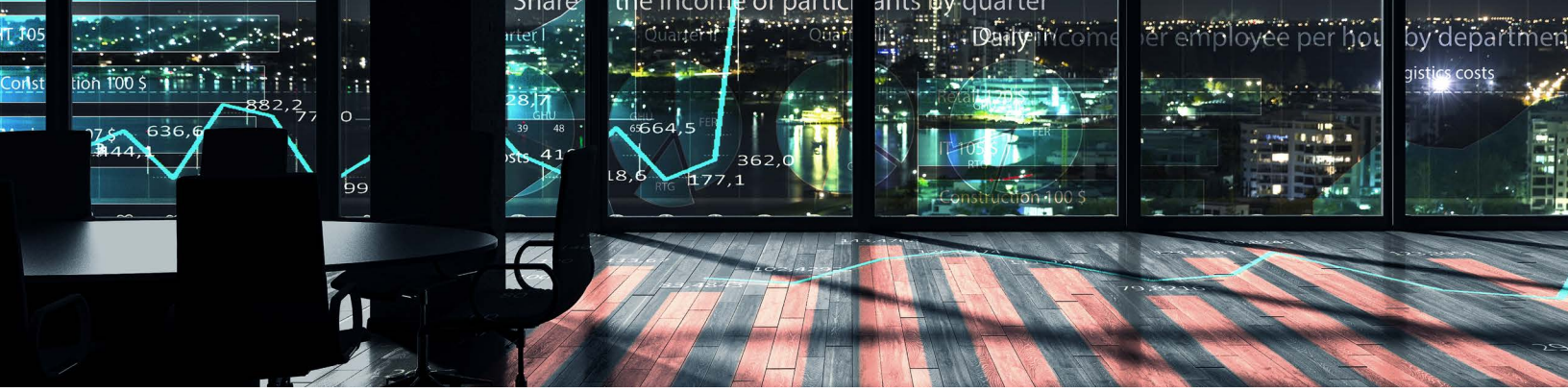
WHAT IS ACTIONABLE INSIGHT?

We have reached a state of data overload. Not too long ago "big data" just seemed like a buzz word thrown around to scare people into needing more tools to digest and consume the data overload within the organization. Now, big data has taken over our lives and our security organizations.



Just from a security perspective, **there are over 700,000 known vulnerabilities in the world, millions of access relationships within your organization and over 25 billion internet records being shared daily.** We are practically drowning in massive amounts of data that spits out at us every day with no real meaning.

What's worse? The data only means something in its own silo. Even when your data gets broken down into reports that give you more context into what it says, the reports don't talk to each other. Instead of having one list with all of your immediate issues on it, you have three or more lists that you have to try and put together. We call this the "swivel defense." With alerts going off all day across multiple systems, **you're constantly swiveling your chair from one screen to another** to try and keep all of the highest risks at bay. What kind of risks are these? Are they real risks or regulatory risks? Again, with so many reports and so much information, how many of these threats need to be patched in order to remain compliant and how many need to be patched in order to stay secure?

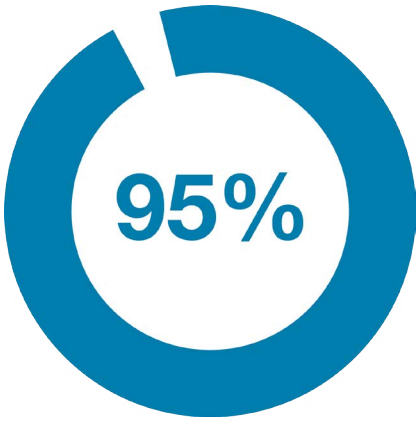


We know you have a large, complex IT stack with cloud and shadow IT adding more challenges for security and you have several security tools that all provide great point solution capabilities, but they don't talk to each other and have built up artificial barriers within your security organizations creating silos that keep your data from telling you more. There is never going to be enough time and resources for your organization because attackers are getting faster and more sophisticated. They are able to devote all of their time and resources into compromising our data so that we are quickly outnumbered and seeing attacks that happen across our systems is impossible with the barriers that have been built up between the security solutions.

How do you solve this issue of too much data and not enough time, resources, or visibility? **Actionable Insight.**

The reality is that the IT stack is going to continue to get more complicated with new and emerging applications and devices, and there will rarely ever be enough time or enough resources to fully combat the problem as the adversaries are moving faster and have more scale and resources than we do. It's difficult for us to change the complexity of the IT stack because we, as security professionals, do not want to be labeled as preventing the business from moving forward, so we are often left with no choice but to support business enablement while focusing on risk mitigation which makes our jobs harder. We can try to garner more support and investment to justify more resources but that is often out of our control.

In addition, breaches are inevitable. According to the Verizon Data Breach Investigations Report, the time to compromise is getting shorter. **Over 95% of compromises took only days to complete. However, companies who were able to discover this breach within days is still hovering at around 25%.**[1] We need a way to make faster decisions and reduce the time from infection to remediation. While we can't control the bad actors, we can control how much visibility we have in order to help us prioritize and make better decisions about what to focus on to address security risks to our businesses. We need the actionable information to make better decisions.



With Actionable Insight your data flows through a funnel starting with the massive amounts of data that are garnered from your system daily and then turned into information, reports or alerts, as to what the data actually means. In the next stage of the funnel you take these reports and apply actionable intelligence to them so you can prioritize these risks, threats, alerts, and reports into a more manageable picture of your organization and what needs to be acted upon first in order to keep your organization safe from compromise. Then, when you've prioritized your list of threats and you know where you infected devices are, what vulnerabilities exist in your network, and what access credentials could be compromised, Actionable Insight puts all of these reports together and gives you context as to what these reports mean to each other and can help you build a holistic case to help prioritize remediation efforts.

1 *VERIZON DATA BREACH REPORT 2016*

The value that an Actionable Insight platform can provide is to:

- Provide data and evidence to build a case to provide a recommended prioritization plan to address and remediate security risks
- The ability to continuously and comprehensively monitor the network for infected devices, the infrastructure and application landscape for any vulnerabilities, and accounts and privileges to better understand any access risks
- Provide holistic visibility of both present security risks as well as historic risks to better learn, over time, where root causes might be as well as to better understand how our security teams are performing with managing down the threat surface
- Get the right information in the hands of the security professionals to more effectively make the correct decisions to act on security risks and minimize any business loss or disruption that may be due to an inevitable breach. This information will also help them to be proactive in preventing possible loss by getting ahead of the security risks before anything happens
- Provide a governance process and the management discipline with KPIs to understand how we are performing as a security organization and where we can continue to improve over time

To complete the comprehensive view of your organization we will look at the three solutions that make up our Actionable Insight platform – Network Insight, Vulnerability Insight, and Access Insight. This book will take you through the entire Actionable Insight platform, week by week, and show you how to continuously and comprehensively visualize access, vulnerability, and device compromises on your network.

CORE SECURITY

CH.02

WHAT IS **NETWORK INSIGHT**?

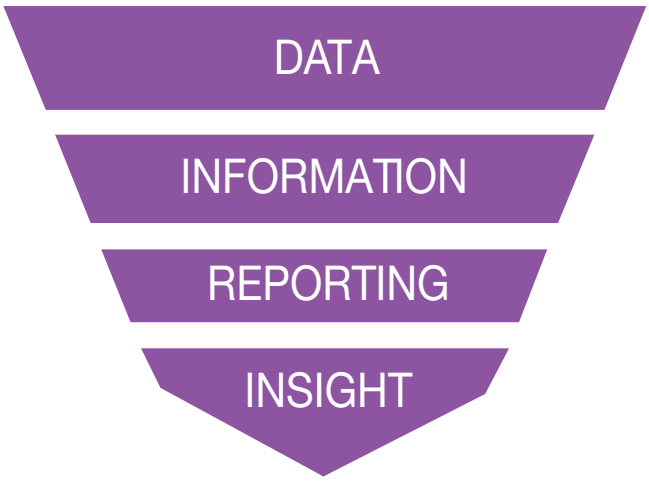
You can't stop something you can't see. In today's world, threats are evolving constantly and prevention tools like anti-virus, firewalls, IDS/IPS and sandboxes are unable to stop infections that they haven't seen before. Core Network Insight is different. It fills the gap between failed prevention and your incident response.

Network Insight is an automatic breach detection system that detects successful infections with certainty, terminates their activity and gives responders the ammunition needed to rapidly prevent loss.

Network Insight observes network communications from endpoints within the customer's environment destined to / from the internet. It identifies when those communications are occurring with external systems intent upon exploiting those devices for criminal purposes (threat actors). It delivers KPIs for Infected Endpoints, Malicious Files and provides Organic Threat Intelligence.

Network Insight delivers actionable information about known and unknown threats regardless of the infection's source, entry vector or OS of the device. It arms responders with definitive evidence so they can rapidly prevent loss on high-risk devices while blocking activity on the rest.

Think about your network like a funnel where data flows through into actionable insight:



Data: There are over 8 trillion unique, new DNS records recorded annually and millions of malware samples analyzed weekly
Information: Network insight analyzes the network traffic using patent-pending communication and risk profilers to narrow down what devices on your networks are communicating with notorious malware families and prioritize them .
Reporting: Once the information is analyzed it is given to a Case Analyzer to determine the certainty of the infection status. These aren't alerts for possible breaches, they are actual infected devices along with the threat actor it is communicating with and what the prioritized infected devices are.
Insight: Responders are provided with a definitive verdict and forensic evidence about infected devices and their risk level. With this information you can tell exactly what devices need to be remediated and act immediately, in real-time, to stop data loss.

How does it work?

- A – Automated Communications
- B – Sandboxing
- C – Connections to disreputable websites
- D – DNS requests for disreputable websites
- E – Indications of execution post-download
- F – Domain Fluxing
- H – TCP Request Structure Match
- O – Tor Detection
- P – Peer-to-Peer C&C Communication
- T – DNS Tunneling

Why do you need CNI?

In a word, real-time visibility. Ok so that was three words but think about it, threat actors always have the first move, especially if they have decided to target your organization. With Network Insight you are right behind them by automatically discovering and containing advanced threats. How?

- By monitoring network traffic in real-time for threat behaviors and activities
- By automatically verifying which devices have successful infections
- By assigning a risk level for each infected device

With Network Insight you are no longer chasing alerts for what could be an issue. You are now given a list of verified infected devices so that you can remediate faster and stop data loss. Network Insight will give you in-depth network visibility into your enterprise with actionable intelligence that your team can use to address viable threats to the company.

Do you know what's in your network? Find out today by requesting an assessment at www.coresecurity.com/network-insight

CORE SECURITY

CH.03

WHAT IS ACCESS INSIGHT?

How often do you delete security groups? Maybe the better question is DO you delete security groups or not, and why? Here is an easier question: How many people have access to Active Directory? What about your financial data? Personal Health Information?

If you can't answer these questions, don't worry, you are not alone. It is becoming increasingly rare to delete these groups because you simply don't know what is in them and who or what application it will affect. Can you imagine deleting a group thinking that you were only cleaning up after a group of old interns only to learn that you also shut out the director of marketing from her automation system? Not a good look for the security team.

All businesses, regardless of industry, are facing three challenges when it comes to change: business change, routine change, and infrastructure change. What do these changes mean to your organization?

- Business Change: You restructure the company org chart, buy and implement a new product, there are changes that happen every day, many without input from the security team as to why and how this should be done.
- Routine Change: Here we are talking about the day-to-day items like hires, terminations, promotions and transfers that happen in your company. With so many people coming and going from your organization you need to stay on top of provisioning and de-provisioning for all applications but there is often times not a system in place to alert you of these changes.
- Infrastructure Change: You're getting into the mobile market, you've decided to put everything in the cloud, it's time for a system upgrade or a new application; these decisions are made constantly. Just like before, they are not always made by consulting the security team.

According to the most recent Verizon Wireless Data Breaches Investigations Report (link here) at least 42% of security professionals are not confident in their ability to detect if access was breached or stolen. Why is this number so high? Because they don't have visibility to access risk within their organizations.

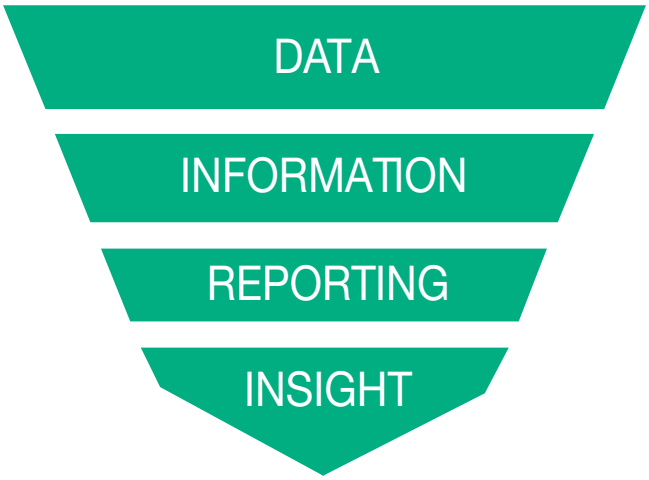
We've said it before and we will say it again, you can't stop what you can't see. And if you can't see it, how can you prove what you are doing is working? Pretty much every industry has rules and regulations when it comes to access management, and compliance regulations are more strenuous than ever. If you can't show a trail for the auditor when asked, you could be in for punishments both financial and regulatory.

So what is the answer to seeing into your identities and visualizing all of your billions of access relationships? **Core Access Insight.**

Access Insight works with any Identity and Access Management (IAM) solution to give you a continuous and comprehensive view of your network while helping you to improve compliance and prioritize access risks.

Let's go back to the funnel:

Data: Enterprise organizations can have billions of access relationships within their network. It is impossible to think that you can gain insight into all of those relationships to see which ones are acting improperly, are orphaned or abandoned accounts, or have higher privileges than they should.



Information: Even when going one layer down there are still too many relationships to understand. You may have a list of accounts with privileged access or a list of groups and what they should have access to. However, you will not be able to see exactly what they have access to, especially if the groups are nested within each other, and you won't be able to see how these accounts are acting.

Reporting: Ok now we are getting somewhere. This is fairly typical for any IAM solution and can show you things like your orphaned accounts, privileged accounts, and abandoned accounts and where the risks are within each of those. This is progress but still only gives us a list of issues with no information on which ones are putting you most at risk.

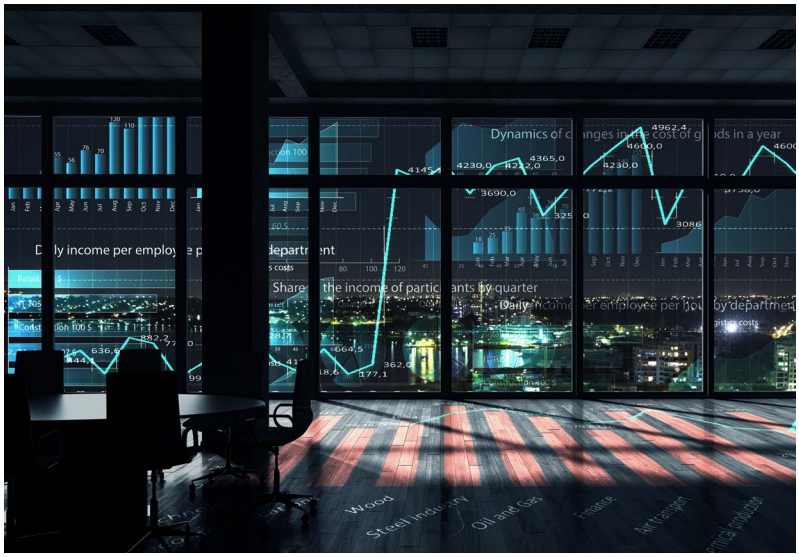
Insight: Here is where things get clearer. Now, you are taking the reporting that you got from your IAM solution and applying actionable insight in order to not only see these relationships more clearly but also see which of these are putting you most at risk so that you can go after them immediately.

With Access Insight, your system becomes more than IAM it becomes Intelligent IAM. “Access intelligence” features analyze the identity and access data using advanced analytic tools to perform data mining, statistical analysis, data visualization and predictive analytics. These are not generic data analysis tools. They draw on IAM-specific policies, rules and risk indicators to provide information of immediate value to IAM administrators and analysts, compliance officers and incident responders.

How does it work with your IAM solution?

Access Insight is IAM solution agnostic so it can work with any IAM solution or with your Microsoft Active Directory and help you with:

Provisioning users and accounts to automate the granting and revocation of access to applications, IT systems and services, tangible assets such as laptops, smartphones and security badges, and intangible entitlements such as access to secure areas.



Governance process to enable compliance with government regulations, industry standards and corporate policies, and to verify compliance.

Intelligent Identity and Access Management to continuously collect, monitor and analyze large volumes of identity and access-related information, combining data not only from provisioning and governance solutions, but also from security products and other external systems.

Access Insight is designed to work with Identity and Access Management to work either with a provisioning system, a governance system, or with both.

Why do you need Access Insight?

The goal of access management is to make sure that the right people have access to the right systems at the right time. But how can you do that when you can't see who has access to what in your organization?

With Access Insight you can not only make sure that the right people have access but you can see what that access means. You can also increase compliance and prepare for your audits by producing a trail of access request rights and password resets to fulfill your regulatory requirements.

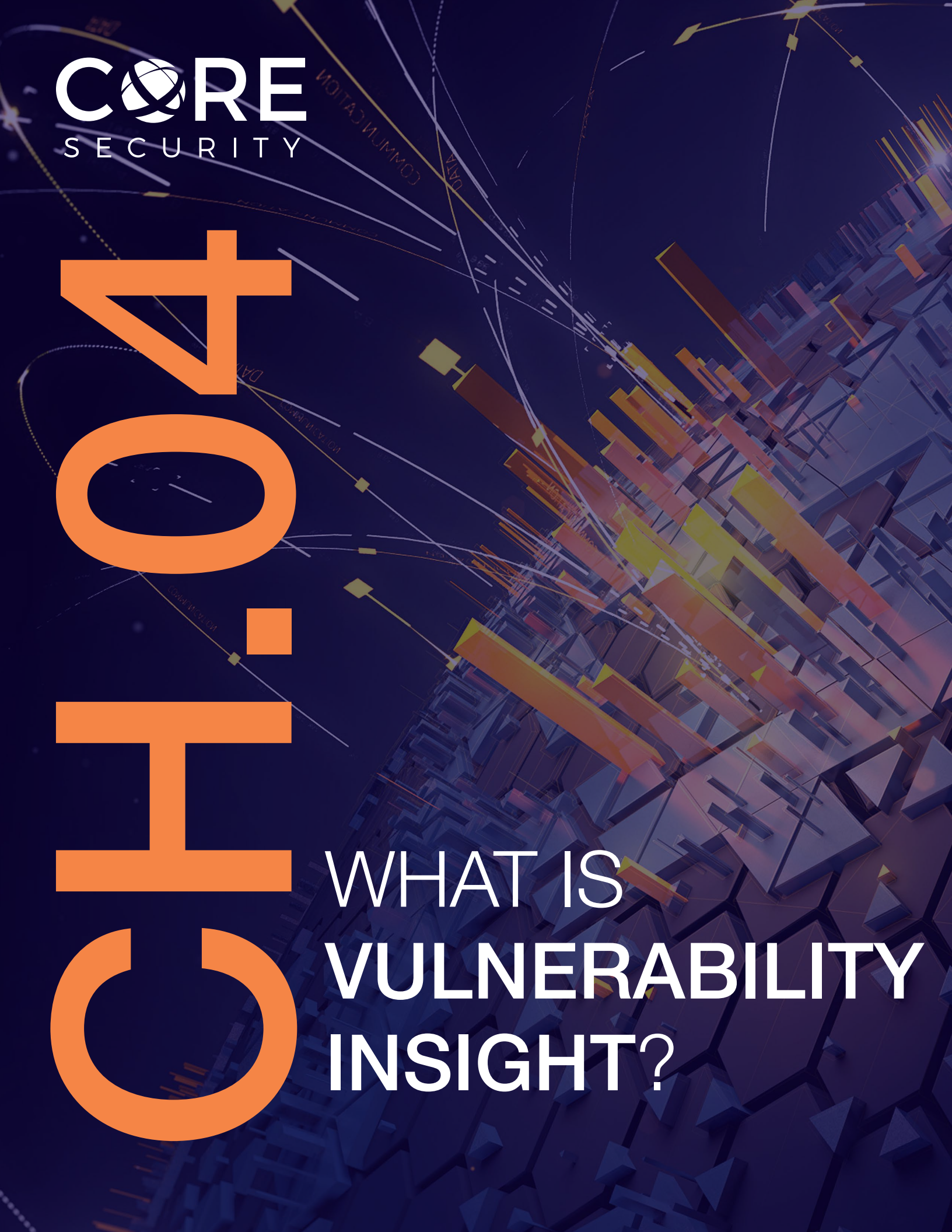
Reduce risk and continuously and comprehensively monitor your access risk as well as with:

- Segregation of Duty Violations Checks: No one should be able to request and approve their own orders. Keep these separate by not allowing over-lapping duties.
- Policy Violations: Catch them before they happen and force an alert to their manager
- Reduce Over/Under Provisioning: With so much routine change in your organization, provisioning can become a rubber-stamp exercise. Don't let that happen, compare across roles and have better insight to what your team needs.

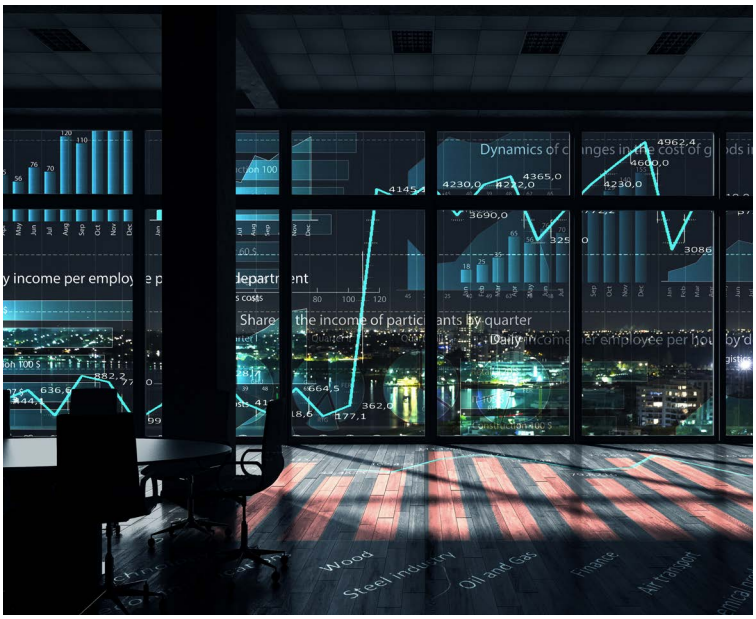
CORE SECURITY

CH:04

WHAT IS **VULNERABILITY INSIGHT**?



Did you know that over 700,000+ vulnerabilities exist in the world today? If you were to break that down into how many you would have to patch each day in order to fight each one of these, that comes to 372 vulnerabilities to patch per day. Oh, and that doesn't take into account the new vulnerabilities and exploits that are created each and every day. I don't know about your organization but I haven't seen a security team yet who had time to work on that many patches in one week, much less one day. With the limited budget that most security organizations have, you don't have time for hundreds of thousands of vulnerabilities. How do you even know where to start?



Let's say you are one of the lucky ones who has the budget and resources to build out a red team that can spend their days poking and hacking your system to see how and where can get in. Even a team of the most skilled penetration testers is still no match for vulnerabilities that they don't know exist. So the question becomes, do you spend time looking through the thousands of lines of output from your scanners and figuring out which ones of those you should prioritize? By the time you do this, even with a team, you are left with barely enough time to patch those high-risk vulnerabilities before it's time to scan and start all over.

How do you prioritize these vulnerabilities? There are the ones with the higher CVE score which look big and scary but have you thought about what would be

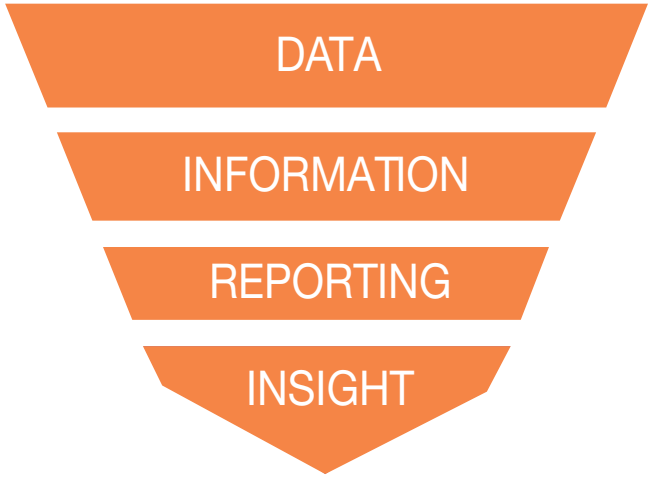
exploited if there was a breach? A Microsoft Word patch is crucial. No one will argue that. However, if your Microsoft Word was breached, do you know what it would effect? Would a bad actor be able to access any high value information from that breach or would they simply have the ability to mess with some fonts and delete your latest blog post? One thing that makes vulnerabilities even scarier is that they are the origin of an attack that could lead to administrative accounts and serve as a gateway to your most valuable information. Without knowing what a vulnerability can impact, you cannot fully understand its level of risk.

Even with multiple scanners, penetration testers, and resources to patch your network, you are still in the dark as to what is causing your organization the most risk. Out of those 700,000+ vulnerabilities, did you know that 80% of the breaches in the world are caused by only ten of them? **Ten!** Do you know if these ten are in your network? If one of them were to be exploited, do you know what the implications would be? As usual, the world of cyber-security leads us to a lot of information and no way to sift through it all and find out what it means.

Are you sensing a theme here? Just like with access and network security you can't stop what you can't see. The same goes for the billions of access relationships you have or the billions of network traffic patterns running through your devices in a day— in order to prioritize vulnerabilities for your organization, you need a vulnerability intelligence tool.

Back to the Funnel

Data: Back to our original number. 700,000+ vulnerabilities exist in the world with more being added daily. Are you prepared to test and patch each one of these just to see if they exist within your organization? No. There is simply no way that anyone has the time or resources for that.



Information: Here is where scanner information is helpful. Instead of testing for and trying to patch every single vulnerability in existence, you are able to see which of these exist in your network. However, even with multiple scanners you are still only breaking down the list of thousands into a slightly smaller list of thousands. Even if you broke down the data and you had only one tenth of the possible vulnerabilities in your organization, could your team handle it? And would they be able to prioritize them based on their risk to your organization?

Reporting: Here is where a vulnerability intelligence solution makes sense. With a vulnerability intelligence solution like Core Vulnerability Insight, you can take all of the scanner data and compare it to your organization and receive a custom prioritization list based on your unique network. No need to patch the

top ten most used vulnerabilities if you only have five in your network. No need to patch a Microsoft update first if there is a SalesForce.com update that has a faster path to administrative credentials. With Core Vulnerability Insight, you gain direction and a plan of action to truly reduce the threat surface.

Analytics: This is where the data gets fun. With your vulnerability intelligence solution you have taken all of the vulnerabilities in your network and you know the attack path that could be followed from each breach origin all the way to the critical asset. Let's take that one step farther. If you knew that there was a vulnerability on Bob's machine because he hasn't upgraded his operating system, would you know which accounts, applications, servers, or devices could also be affected? With Actionable Insight you can. Imagine finding out that there was a chance that Bob's system could be exploited and from that machine you could pivot to other machines on the VPN. With Actionable Insight you know not only how the vulnerabilities affect your network but you can tell how those vulnerabilities can also affect your access and network risks.

How does it work with your scanners?

Core Vulnerability Insight consolidates multiple vulnerability scans across vendors, while matching known exploits and simulating attacks in your environment. It enables you to focus on the most vulnerable points of your network rather than guessing which vulnerabilities are putting you at the most risk.

Why do you need Vulnerability Insight?

Core Vulnerability Insight unifies, regulates, and prioritizes vulnerability management initiatives enterprise-wide.

With greater scalability and advanced attack path analytics, Core Vulnerability Insight helps you to accurately identify the vulnerabilities that pose the greatest threat to critical business assets, regardless of the size and complexity of your IT landscape. Once critical vulnerabilities are prioritized, you can move quickly to remediate the threat in your systems.

CORE SECURITY

WHAT IS ACTIONABLE INSIGHT?

Throughout this book, we have talked a lot about the problems facing cyber-security today and how we can combat them. However, the fact remains that we still have three very serious issues and three very different ways to handle them. Identity and Access Management (IAM) solutions do a wonderful job of helping you visualize and address access issues just like vulnerability management and network threat detection do for their respective areas. The issue that we are now facing is that these three areas can no longer work in silos. Hackers don't think one dimensionally and neither can we. In order to fight the new wave of cyber-crime, we must stop swiveling from screen to screen and instead learn how to pivot through our solutions to catch bad actors where they are most likely to attack.

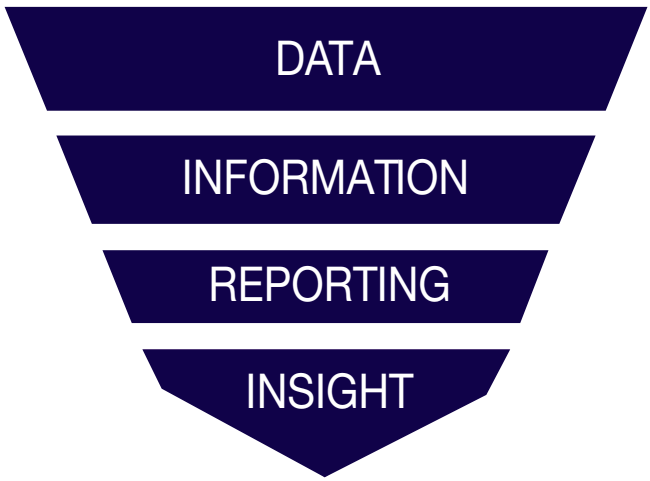
How do we do that? With Actionable Insight.

The Actionable Insight Platform breaks down the walls of traditional cyber-security into a comprehensive view of your organization's access, devices on the network and vulnerabilities. Moreover, it prioritizes those risks for you, so that you can focus on the most critical risks and efficiently use your team's time and resources. This platform delivers clarity to the overwhelming problem of too much information by adding intelligence to transform mountains of data into valuable, practical and actionable information.

The most valuable part of this platform is the ability to take immediate, automated action on threats against your organization. With Actionable Insight you can automate termination for any account that has been compromised before it can pivot to other areas of your network. With traditional solutions, you can see that an account has been compromised, however, you don't have enough information to act on that alert.

It's important to know your network has been breached as soon as possible. However, in order to limit possible data loss, you must also know where the breach occurred, what that account has access to and what possible points it can pivot to on your network. With Actionable Insight you can see this information within a timeframe that makes it possible to act before you experience data loss.

Let's go back to the funnel to see how this would look in your organization.



Data: We've discussed "Big Data" and what it can do to your organization. With Actionable Insight, data takes on a new level of complexity as we pull in all of the vulnerabilities picked up by scanners, the access relationships from your IAM solution and all of the billions of traffic patterns running through your network devices. While this would be overwhelming to do as an individual, Actionable Insight is built to not only handle this much data but to analyze and use it in a completely new way.

Information: Once you have all of your data, it's time to make sense of it. Now you are aware of what you need to focus on between the number of vulnerabilities found in your network, the number of devices with questionable traffic and the number of orphaned accounts, segregation of duties violations and other access-related risks. This is better than the mounds of data that we had before but still difficult to comb through and act on.

Reports: Time to make sense of all of the information. Here, with one solution,

you will be able to see all of your access, vulnerability and network risks in one place. What makes this more valuable is that you can be assured that these risks are valid. No more false reports of things that "could" harm your network, now your team will be able to focus solely on real risks.

Insight: This is where it all comes together. Now that you have the reports with all of the critical issues to be addressed, you can get to business. With Actionable Insight, you can rank all of these risks so that your team can use their precious time and resources more effectively. The issues are no longer ranked individually by type but they are ranked as one list and their ranking is informed by how they interact with each other. For example, if a vulnerability is found on a computer, you can tell who has access to that computer and if there's a possibility to get to admin privileges. If yes, then that risk will rank higher than one where there is no access to privileges. By using these functions together we are able to look across the threat surface and gain a better understanding of what we are up against.

Here is an example, let's say your CFO's account credentials were stolen. You've received an alert but when you check you see that they do not have access to many applications that could be useful to a bad actor. However, they could have information to outside information. By hacking them, you could install a keylogger and figure out that they have access to the bank and their login information— allowing them access to all of your organizations funds. It's not always knowing what account was breached

as much as it is knowing who that person is and what their access means. That's why it's imperative to have the option to automatically disable any and all compromised accounts.

Why do you need Actionable Insight?

Adding Actionable Insight to your security toolkit will enable you to enhance your security exponentially. By adding this solution you will be able to:

1. Reduce IT Costs

With the ability to automate so many functions of your security, you could save in both headcount and the number of tools needed for checks and balances. Actionable Insight automatically identifies threats and alerts you so that corrections can be made to stop losses. You will be able to continuously and comprehensively monitor your network for three different types of risk with one solution.

2. Reduce the Threat Surface

With a holistic view of your threat surface, you can now take action on ways to reduce it. By acting on the greatest risks first, you can quickly reduce your threats across multiple vectors. Not only will you be patching a vulnerability but you will also be shoring up access to privileged accounts that this vulnerability exposes.

3. Increase Efficiency

In the example above, we were able to see that a vulnerability on one machine

influenced the access risk of privileged credentials. The ability to rank issues by their degree of risk gives your team the ability to use their time and resources more efficiently. Additionally, by knowing which risks affect multiple systems, you can patch three issues in one.

4. Improve Compliance

By being able to model and analyze activity and threat patterns with Actionable Insight you can better prepare for possible attacks. Knowing the attack path and how it pivots from one solution to another will help you get inside the mind of the bad actors who are coming after your data. There is also the ability to set micro-certifications to ensure that privileged account access is protected, the ability to stop Segregation of Duties violations before they are approved and improve your regulatory compliance no matter your industry.