7/11/22 | Reshare Crowdstrike

The more digital growth you company experience, the more risk you face from security threats. This whitepaper from @Crowdstrike is an excellent resource for operationalizing a Zero Trust framework for your organization:

7/14/22 | Cyber Woes Blog

In our latest blog on fixing cybersecurity woes, we share the stories of two companies who face supply chain attacks and zero-day vulnerabilities. The truth is that, as important as IT departments and endpoint security is, the best protection doesn't come from playing defense. We believe that the future of protection is in risk hunting: finding and fixing any weakness a threat could exploit before hackers do.

As you read more, think about the attacks you've faced recently. Can you relate to the stories we've shared about cyberattacks? Let us know your experience and whether you think risk assessment could help. After all, the best defense is a good offense.

7/14/22 | Cyber Woes Blog

We talk a lot about cybersecurity risk hunting because we believe it is the only method for preventing a cyberattack before it happens.

As our global workforce continues its digital transformation, endpoint security becomes increasingly important—and the numbers are staggering. 68% of organizations have had an endpoint attack that compromised corporate data; 80% of cyber incidents are the result of a brand new or unknown zero-day attack; 33% of workers use an endpoint dev ice to work remotely.

With every year that passes, hackers get better at infiltrating cybersecurity defenses. Today, it only takes a single user error for attacks to breach your protection. We've created this whitepaper to help you think through what it would mean to take your defense on the offense. It's time to take a new approach:

Zero-day flaw in Atlassian Confluence

LinkedIn: No matter how fortified your defenses are against zero-day vulnerabilities, hackers can and will discover a way to breach those walls. That's why companies everywhere need to stop playing defense and start investing in risk hunting. Because the only way to truly defeat an attacker is to diagnosis the problem before they do.

Twitter: Your defenses will always be open to zero-day vulnerabilities. It's time to stop playing defense and start investing in risk hunting. After all, the only way to truly defeat an attacker is to diagnosis the problem before they do.

2022 Cybersecurity Almanac

LinkedIn: In the 2022 Cybersecurity Almanac, it is reported that companies will spend up to $1.75 trillion from 2021 to 2025 on cybersecurity products and services globally. Despite that, cybersecurity crime will end up costing $10.5 trillion by the end of those five years. We're paying more money than ever before for worse results than we've ever seen. It's time for a change. If spending money on our defenses isn't getting the job done, it's time to use our resources to go on the attack:

Twitter: From 2021 to 2025, companies will spend $1.75 trillion in cybersecurity products and services, yet will lose $10.5 trillion by the end of those five years. Spending money on our defenses isn't working—it's time to go on the attack:

Cyber risks top worldwide business concerns

LinkedIn: Allianz Risk Barometer rates cyber incidents as the number one concern for global companies this year with a nearly 50% vote share. That means company concern regarding cyber incidents is higher in 2022 than business disruptions, COVID-19, and the growing shortage of skilled workers. If we want to lower that concern to where it belongs, we'll need to invest in proven solutions like risk hunting:

Twitter: Global companies view cyber incidents as their number one concern over business disruptions and a growing shortage of skilled workers. The fear is that their defenses aren't enough. Which makes it a great time to invest in risk hunting:

Gartner Predicts 40% of Boards Will Have a Dedicated Cybersecurity Committee

LinkedIn: Gartner predicts that, in the next three years, there will be a 30% increase of the boards of directors who have a dedicated cybersecurity committee overseen by a qualified board member. Perhaps this is because "relatively few directors feel confident that their company is properly secured against a cyberattack." Perhaps this is because the way companies have traditionally defended against cyberattacks is outdated, counterintuitive, and relatively ineffective. To defend against cyberattacks, we must embrace the adage "The best defense is a good offense" and attack the problem head on:

Twitter: Traditional defenses against cyberattacks are outdated, counterintuitive, and relatively ineffective. To truly stem the tide, we must embrace the adage “The best defense is a good offense” and attack the problem head on:

New Cisco Annual Internet Report

LinkedIn: Cisco is reporting that 5G will support more than 10% of the world’s mobile connections by 2023. This is great news for consumers and businesses as 5G speeds operate 13 times faster than today’s average mobile connections. However, this may lead to some concern that increased usage could lead to further endpoint vulnerabilities that companies are struggling to defend against. What do you think? How is the widespread adoption of 5G going to affect the cybersecurity landscape?

Twitter: In two years, more than 10% of the world’s mobile connections will utilize 5G. But how will companies defend against the inevitable increase in endpoint attacks? Risk hunting is a proven solution that will ensure your preparation:

Top Security Threats of Smartphones

LinkedIn: Recent reports show that, despite the superior security of mobile devices compared to computers and tablets, mobile security threats are increasing. The numbers are staggering: mobile devices now account for more than 60% of digital fraud, due to malicious apps, weak security, and spyware. The truth is that mobile devices have as many points of vulnerability as your other devices. What are you doing to protect your data and information?

Twitter: Mobile security threats are increasing, with mobile devices now accounting for more than 60% of digital fraud. Mobile devices are just as vulnerable as laptops and tablets. So what are you doing to protect your information?

Many security executives say they’re unprepared

LinkedIn: Although there is a lot of great information in this TechRepublic article, we can't stop thinking about the opening sentence. “As cyberattacks grow in both number and sophistication, organizations are increasingly under the gun to protect themselves from compromise.” The concern is that digital transformation is leaving companies vulnerable to attacks that don't yet exist, in a future they can't plan for. We understand that concern because it is precisely what we have been preparing for at Reveald. Risk hunting isn't just about going on the offensive—it's about giving companies a flexible framework that allows them to adjust to any problem they're facing:

Twitter: As monumental as digital transformation is, companies are left vulnerable to future attacks they can’t yet envision. We’ve been preparing for the future with a tool that gives companies a framework to adjust to any problem they face:

Software supply chain attacks hit

LinkedIn: Software bills of materials are an underutilized piece of your security defense. Not only do they allow you to actually see the different applications of software you're using, it also opens the possibilities for improved cybersecurity practices. When paired with risk hunting, SBOM can be a powerful tool. And with more than three-in-five companies being the victims of software supply chain attacks last year, companies need all the cybersecurity support they can get:

Twitter: When paired with risk hunting, SBOM can be a powerful tool. Not only are you able to see the software you're protecting, but it also allows you to defend against software supply chain attacks, which aren't stopping any time soon:

Cybersecurity trends: Looking over the horizon

LinkedIn: No matter where you are in your cybersecurity protection, it's important to stay aware of cybersecurity trends. In this McKinsey report, three key trends and their implications are considered and discussed. Let us know what you think of these trends—are they matching what you're seeing on the ground? And how do you think risk hunting could address them?

Twitter: Staying ahead of cybersecurity trends is almost as important as setting up solid cybersecurity protection. Read this report and let us know what you think of these trends. How could risk hunting help address them?

7 hot cybersecurity trends

LinkedIn: In this CSO feature, @Neal Weinberg gives 7 hot cybersecurity trends that companies should be aware of. Check these out and let us know what you think. Is the recent rise in ransomware attacks here to stay? Are we going to experience an increase of attacks against internet of things and operational technology? And most importantly, how do you think risk hunting plays a role in effective cybersecurity protection:

Twitter: Here are seven hot cybersecurity trends that companies should be aware of as we continue through the rest of the year. And here's a hot tip not included in this CSO feature: risk hunting can help with many of these potential concerns:

Adversarial machine learning explained

LinkedIn: We all know that hackers are continually finding new ways to attack our cybersecurity defenses, but how serious is this threat? A report from Microsoft shows that 90% of organizations are unprepared to defend themselves against adversarial machine learning. This means that attackers can breach your security walls to affect the training systems of your AI, wreaking havoc. As you read this feature to learn more about how AI systems can be disrupted, think about whether risk hunting could

help solve the issue:

Twitter: 90% of organizations are unprepared to defend themselves against adversarial machine learning. So if your business depends on AI training systems, consider how your cybersecurity defenses are going to hold up during a cyberattack.

The changing role of the board on cybersecurity

LinkedIn: As we saw with recent Gartner reports, boards and senior leadership are placing more emphasis than ever before on cyber risk. Not solely an IT problem, companies are correctly realizing that cyberattacks have the potential to disrupt their entire enterprise. In this Deloitte presentation, it is said that “cybersecurity oversight has now become the most important topic for the Board after strategic planning.” The question is whether your leadership realizes how important taking action against your cybersecurity vulnerabilities is:

Twitter: Gone are the days when cyberattacks were viewed solely as an IT problem; companies now correctly realize that cyberattacks can disrupt their entire enterprises. Is your leadership aware of the best tools for fighting cyber risk?

Feds Uncover a ‘Swiss Army Knife’ for Hacking

LinkedIn: When the Department of Energy, the Cybersecurity and Infrastructure Security Agency, the NSA, and the FBI released a joint advisory about a new hacker toolset that could adapt to nearly any industrial environment, were you concerned about your ability to defend against every possible cyberattack? Us, too. That's why we invented risk hunting to guard against "Swiss Army knives" just like this one:

Twitter: With news of the creation of a hacker toolset that can adapt to nearly any industrial environment, we’re thankful now more than ever that we have a tool like risk hunting to guard against "Swiss Army knives" just like this one:

67% of Businesses Suffer Repeat Cyber Attacks

LinkedIn: Just because you've patched up the weaknesses in your defense doesn't mean you're not still vulnerable to cyberattacks. As this CPO magazine article explores, two-third of companies that suffered cyberattacks were hit again within a year. That's because frequent changes in end-users and new third parties with corporate network access constantly alter where these vulnerabilities lie. You cannot guarantee your threats will remain stable. Instead, you need to focus on taking your defense into your own hands with risk hunting:

Twitter: Two-third of companies that suffered cyberattacks were hit again within a year’s time. Which means you need to ask yourself: are the patches in your cybersecurity defense enough to ward off hackers?