

OCTOBER 2021
Newsletter #27

Blog Box

By CXO Strategies

BUSINESS

NetWitness – A Brief History of an Iconic Threat Detection & Response Platform

INFOGRAPHIC

5 Ways Threat Intelligence Improves Orchestration and Automation

STRATEGY

How Useful are your Threat Intelligence Feeds?

EXECUTIVE INTERVIEW

Redefining Cybersecurity in the Middle East

RANSOMWARE: A BEGINNER'S GUIDE TO THREAT DETECTION

Powered by

 **NETWITNESS**
An RSA Business

NOT WHAT IT SEEMS

**THREAT INTELLIGENCE,
DETECTION & RESPONSE**



EDITOR'S NOTE

THE OTHER EPIDEMIC: CYBERCRIME IS UP 600%, AND RISING

As we navigate one defining crisis of our time (the COVID-19 pandemic), we are facing another that has far-reaching consequences as well. Crisis that's growing exponentially, with no end in sight: cybercrime.

At the onset of the pandemic, malicious emails increased by 600%, according to the UN Disarmament Chief. The threat has only grown since, with the subsequent increase in digitalization, as businesses pivoted to remote working, and customers increasingly adopted digital practices. Increased digitalization in a globalized world could spell trouble, if we are under-prepared; not only in conventional high-risk sectors like banking, but just about every sector with internet-facing assets and operations.

Expanding attack surfaces, and ever-evolving vectors, warrant an effective response from businesses. And their resilience against new threats, responsiveness to the challenge, and readiness for future ones, will have a defining bearing on business outcomes. Businesses that create a foolproof security posture will be able to operate without the shadow of a cyberattack hovering over them.

But doing so is easier said than done. Cybersecurity is an umbrella term encompassing a range of critical functions, including threat identification, security posture protection, analysis, remediation, and recovery. And CISOs and security teams now find themselves facing an uphill battle, requiring additional technological reinforcements and support from the C-Suite.

Many forward-thinking business professionals believe that cybercrime is no more a human-scale problem. This belief is now translating to increasing investments into automation-first technologies, which are poised to resolve machine-scale problems with the concerted efforts of humans and machines.

This approach is based on using past problems for future excellence, by leveraging threat intelligence to stay a step ahead of vectors. Threat intelligence, cutting-edge technologies, and integrated cybersecurity models are poised to enhance efficiencies, eliminate human-centric errors, and simultaneously ensure that businesses can achieve incremental ROI.

The writer is the Technology Editor and ROI Strategist at Dubai-based CXO Strategies. She can be contacted via twitter @CXOConnectME



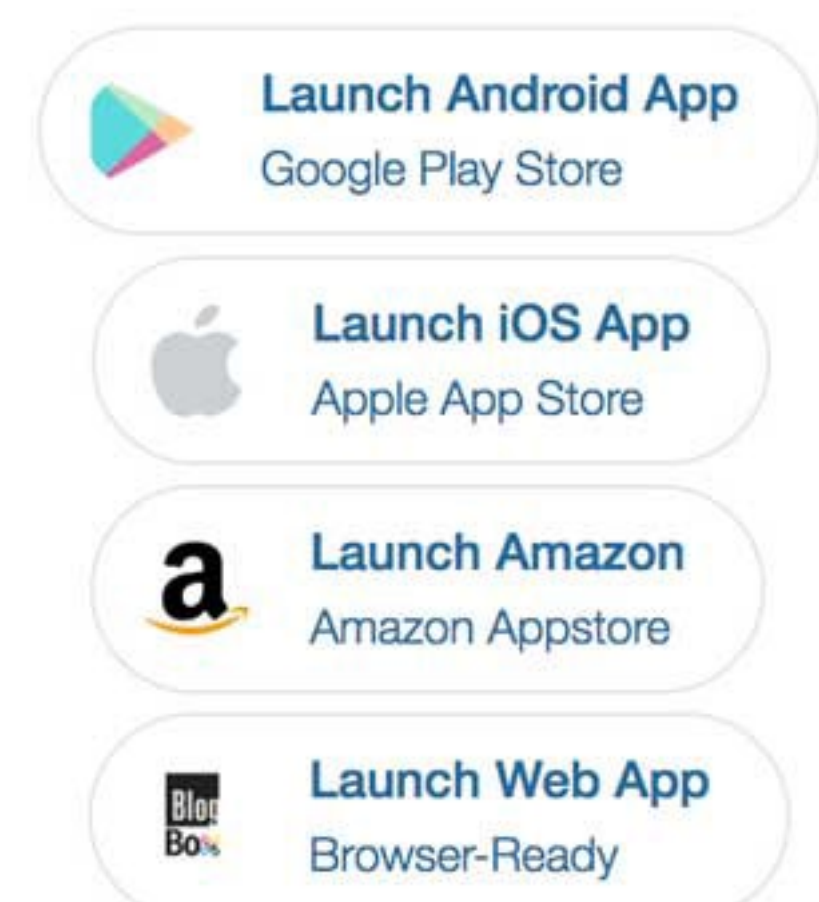
KAVITHA RAJASEKHAR

Technology Editor and ROI Strategist at Dubai-based CXO Strategies

Email: Kavitha@cxostrategiesme.com

Twitter: [@CXOConnectME](https://twitter.com/CXOConnectME)

The only thing that shapes Opinion is opinion itself. CXO Blog Box is an industry compilation of insights and opinions. Our focus is to curate the opinions shaping the tech industry



NetWitness – A Brief History of an Iconic Threat Detection & Response Platform

By Arthur Fontaine

NetWitness' transition to become an independent business unit marks another step in its remarkable journey. Started nearly a quarter-century ago as a U.S. intelligence research project to perform security analysis of network traffic, today NetWitness is recognized for its leadership position in both the Evolved SIEM and XDR markets.

NetWitness customers include many of the world's largest, most complex, and most security-conscious organizations. The depth and richness of the NetWitness investigative toolkit, with comprehensive visibility, advanced AI analytics, and incident orchestration and automation features empower NetWitness customers to defend against advanced cyber threats.

Through its long and storied existence, NetWitness has fought for the good side in one of history's most dynamic contests: the war between the black hats and the defenders. This is the story of that evolution.

The Early Years

NetWitness originated in 1997 as a U.S. Intelligence Agency research project managed by CTX Corporation, a Vienna, Virginia-based consultancy where most employees held Top Secret security clearance. NetWitness was custom-built to help analysts understand large volumes of captured network data. CTX saw the value of the technology across broad use cases and obtained permission to sell it in other engagements.

In 2002, CTX was acquired by ManTech International Corporation, which further developed the technology to aid federal law enforcement agencies in criminal investigations.

In 2006, ManTech launched NetWitness as a privately-held spinout to bring its network analysis technology to the worldwide commercial market. NetWitness was offered as a packaged software solution and adopted by some of the world's premier organizations, many of which still rely on NetWitness to this day. As a private company, NetWitness redirected development to create an enterprise solution.

RSA Investments & The Advent of SIEM

In 2011, RSA acquired NetWitness and paired it with the RSA enVision SIEM in a combined security message. During this period, enVision was a leader in a SIEM market in transition. Originally compliance-focused, SIEM logs were increasingly being utilized for security analytics. Harnessing this trend, RSA combined enVision and NetWitness to give NetWitness even greater enterprise reach, deep packet inspection, and log parsing in a common metadata language.

Staying true to its consultancy-based origins, RSA Professional Services introduced Incident Response (IR) services based on NetWitness. RSA expert threat hunters still deliver IR on retainer or on-demand, standing shoulder to shoulder with customers around the globe. Because NetWitness is used continually for real-world investigations in complex environments, the data it captures provides RSA with constant and important input to shape NetWitness' product development; this feedback loop has been a critical factor in NetWitness retaining leadership and relevance for decades.

RSA's investments delivered tightly integrated network and log analytics capabilities, augmented with rich threat detection and forensic tools. And in 2014 the new combination was rebranded as RSA Security Analytics, then rebranded once more in 2016 as RSA NetWitness Suite.

Through its long and storied existence, NetWitness has fought for the good side in one of history's most dynamic contests: the war between the black hats and the defenders. This is the story of that evolution.

In 2012, NetWitness acquired Silicium Security and its flagship Enterprise Compromise Assessment Tool (ECAT). Integrated with NetWitness, ECAT – later rebranded NetWitness Endpoint – gives threat hunters a powerful tool to detect endpoint-based anomalies that other solutions miss.

Evolved SIEM

In 2018, NetWitness acquired Fortscale, a pioneer in User Behavior & Entity Analytics (UEBA). Security Orchestration, Automation & Response was added with NetWitness Orchestrator. Building atop the strong foundation of NetWitness, the UEBA and SOAR evolution introduced RSA NetWitness Platform, a comprehensive Threat Detection & Response and Evolved SIEM solution.

In 2020, NetWitness released IoT Security Monitor, a cloud service to monitor and alert on Internet of Things devices and systems. Integration with NetWitness adds an important visibility vector for IP-based devices.

XDR Futures

The evolution of NetWitness has aligned squarely with the next major market evolution: XDR, or eXtended Detection & Response. XDR embraces all of the existing Evolved SIEM capabilities – visibility, integration, analytics, and automation – but emphasizes single-vendor integration and support, as old models of mix-and-match security are unable to keep up with sophisticated and emerging challenges.

Cloud support is key to XDR. Recently, NetWitness launched Detect AI, a pure cloud SaaS analytics component for NetWitness Platform. Next up is NetWitness Cloud SIEM, a SaaS (Software as a Service) offering that encompasses both software and infrastructure. In the pipeline is Big Bang, a big data analytics module for NetWitness that will provide asset discovery, characterization, and prioritization, with continuous analytics that detect new assets as well as changes to asset importance.

NetWitness: The Next Era

In 2006, RSA Security, independent since its 1982 founding by legendary encryption scientists Ron Rivest, Adi Shamir, and Leonard Adleman, was acquired by EMC. It operated as RSA, the Security Division of EMC until 2016, when Dell and EMC merged to form Dell EMC.

RSA operated as an independent unit of Dell Technologies until 2020 when it was spun out as an independent organization in a sale to a consortium led by Symphony Technology Group (STG). Reformulated as an independent business unit, NetWitness is reorienting to focus exclusively on XDR market opportunities and requirements. This evolution is technically and logically consistent with the heritage of NetWitness, from its genesis as an intelligence agency research project, to its current and future role protecting the world's most security-conscious organizations. The new logo honors that heritage, introduces the next generation of NetWitness to serve our customers, and marks the next chapter in this solution's long and storied legacy.

Source:

<https://www.netwitness.com/en-us/blog/2021-04/netwitness-a-brief-history-of-an-iconic-threat-detection-and-response-platform>

5 WAYS THREAT INTELLIGENCE IMPROVES ORCHESTRATION AND AUTOMATION

Benefits of Applying Intelligence to Better Respond to Incidents

There is a lot of conversation around the need for security orchestration, automation, and response (SOAR). Security organizations agree that having a system to automate tasks and keep the entire security team working from the same game plan has become more critical as the number of alerts and incidents that must be addressed increases. The bigger question these organizations must answer is, "How do we know that the threats and incidents we are investigating are the ones that we should be focused on?" This is where threat intelligence, working in unison with your orchestration and automation system, can help. Here are five reasons why:

1 Lower-level tasks no longer consume valuable resources

As orchestration and automation systems work to automate detection and prevention tasks, validated threat intelligence derived from a broad range of sources ensures that the system is quickly alerting and blocking the incidents that could cause your organization the most harm. This process eliminates the repetitive tasks that require a large amount of analysts' time while properly identifying the incidents that matter and reduces false positives.

2 Increase accuracy and precision

The key to getting in front of threats? Awareness and understanding the context of the situation early on. To do this, threat intelligence can automatically identify and extract key evidence to be applied to a case under investigation. This allows your organization to work quicker and prevent attacks or stop them in their tracks, minimizing impact. Be more proactive by automating more tasks up front.



○ Fine-tune your threat intelligence

Your own team and data are the best sources of intelligence you will ever have. The analysts know your environment and they can determine how insights, artifacts, and sightings automatically captured using threat intelligence apply to your specific organization. This process refines the vast amounts of threat intelligence gathered to understand how new indicators of compromise (IOCs) and adversary tactics and techniques will have an impact on your specific environment.



○ Orchestrate with more confidence

Analytical processes applied to external threat intelligence and backed by internal intelligence allows for more accurate alerting, blocking, and quarantine actions with fewer false positives. It goes beyond simply ingesting multiple threat intelligence feeds or acting from a shared indicator of compromise (IOC). It is about making sense of them at scale using techniques like adaptable scoring and contextualization to know what actions to take, if any.



○ Constant improvement

The automated extrapolation of context and tasks based on threat intelligence thresholds, such as indicator scores, followed by the memorialization of data enables security organizations to undergo strategic reviews and hone processes. As a result, the team's improvement grows, allowing it to rise to the challenge of growing threats.

Many orchestration and automation solutions only incorporate intelligence to trigger certain workflows. NetWitness® Orchestrator is different – it gets the highest value from external and internal intelligence enabling security organizations to automate tasks, work systematically across teams, and address potential business-impacting threats with greater efficiency.

Learn more at netwitness.com

In today's hyper-digital world, the business case for threat intelligence makes itself

As digitalization makes inroads into every sector - fueled by the pandemic-induced rise in remote working and accelerated tech-adoption - the critical role of cyber threat intelligence (CTI) has been reinforced, in the business ecosystem. On the flip side, this period has also witnessed cyberattacks of an unprecedented scale. Consider the Kaseya ransomware attack, for context – it sent ripples across the globalized world, affecting as many as 1,500 businesses of all sizes, various government institutions, and even the diplomatic relations between the US and Russia. The group behind the attack demanded a ransom of \$70 million, which is nearly a third of Kaseya's yearly revenue!

What led to an attack of such scale, in an organization of Kaseya's calibre? According to ex-employees(1), wide-ranging cybersecurity concerns were flagged between 2017 and 2020, and reported to leaders. But these concerns went unaddressed. The disproportionate focus on sales, at the expense of security, led to the attack, the ex-employees said. Nevertheless, the type of attack, the vectors used, the modus operandi, and the target areas will now add to the threat intelligence, which Kaseya, and other businesses, must take stock of.

The business case: Contextualization, triage, remediation

Actionable threat intelligence encompasses information on past and potential cyberattacks, enabling CISOs and businesses to create a foolproof security posture. Eclectic threat intelligence is not just a prerequisite for traditionally high-risk sectors like banking and aviation; with every sector now accelerating digitalization, all businesses need to take informed and contextualized decisions, in terms of security. Internal threats, like data breaches and malware incidents; external ones, like subscription feeds; and known threats faced by similar organizations; are all factors that businesses must consider, when making security-related decisions.

Threat intelligence also helps businesses identify priority areas, allocate risk scores to indicators, and make better correlations - all leading to effective triage and remediation. Many businesses that have boosted their investments into threat intelligence have optimized their existing technologies, like secure web gateways (SWG) and firewalls as well. This is to say, threat intelligence is an investment that can drive multi-fold, incremental value. But secure outcomes depend on how the intelligence is analyzed, and the quality of the insights derived - which is where the presence of technologies like security information and event management (SIEM) and security orchestration, automation, and response (SOAR) becomes a business imperative.

By one estimate, the SIEM market valuation grew to \$3.9 billion in 2020 despite the pandemic-related economic downturn and liquidity crunch in the business ecosystem.

Maximizing the value from threat intelligence

As the number of use cases increases in threat intelligence, they require more resources to run, correlate, and respond to incidents promptly. SIEM technology, integrated with threat intelligence data, can perform real-time analysis, keep security logs, investigate incidents, and give reports on the severity of threats and their potential impact on businesses. Such real-time threat monitoring and management are key to empowering CISOs and security teams.

By one estimate(2), the SIEM market valuation grew to \$3.9 billion in 2020 despite the pandemic-related economic downturn and liquidity crunch in the business ecosystem. Real-time threat detection and response remain the primary drivers to SIEM adoption, followed by compliance and reporting. More recent adopters are engaging vendors and service providers based on new criteria, including integration, cloud capabilities, and most importantly, the scope for automation. This approach is geared towards harnessing AI analytics, and supporting analysts working on investigation and response, through automated processes.

Threat intelligence integrated with SOAR

Security teams operating in today's hyper-digital world are witnessing an increase in cyberattacks - both in terms of volume

and velocity. They are required to fend off attacks at a higher frequency, quicker and more efficiently. So, the deployment of AI, as part of the SOAR platform, will soon be non-negotiable for businesses.

Proponents of this approach are realizing multi-fold value: analysts are capable of addressing diverse alerts and incidents, through automated processes; less-critical tasks no longer consume excessive resources; repetitive, time-consuming tasks are replaced by automated processes that enhance accuracy and precision due to elimination of manual errors; and false positives are significantly reduced. CISOs operating on such security postures are more confident in nipping attacks in the bud, and minimizing their impact. Moreover, every successful response adds to the threat intelligence, helping businesses further adapt to constantly evolving attack surfaces and vectors.

Vendors management is key to successful CTI strategy

Businesses cannot adopt a cookie-cutter strategy to threat intelligence and associated tech deployments. Every business faces unique security threats based on the sector they operate in, the size of the operations, and how internet-facing their assets are. It is important to go about designing a response methodically, assess all the risks, bring the opinion of security teams to the table, and get everyone on board, before starting a strategic association with a vendor/service provider.

A survey(3) found that only 28% of companies were happy with their vendors' security management. So, before you begin a partnership, it's crucial to consider the prospective vendor's security posture and its ability to turn threat intelligence into reliable, actionable insights. Look at it this way: Your security posture is only as good as the vendor's; and as the vendor network grows, so does your attack surface.

In fact, threat intelligence also helps businesses do effective vendor assessment; by helping assign appropriate security ratings and select a vendor who can best cater to their needs. Diligent vendors can bring the best out of threat intelligence data, leveraging it effectively and ensuring that the CTI strategy translates to foolproof security postures.

Source:

1.<https://www.bnnbloomberg.ca/kaseya-failed-to-address-security-before-hack-ex-employees-say-1.1627491>

2.<https://www.prnewswire.com/in/news-releases/security-information-and-event-management-siem-market-size-to-reach-usd-6436-2-million-by-2027-at-cagr-6-8-valuates-reports-811987793.html>

3.<https://www.delltechnologies.com/asset/en-us/solutions/business-solutions/industry-market/dell-bios-security-the-next-frontier-for-endpoint-protection.pdf>

The writer is the Technology Editor and ROI Strategist at Dubai-based CXO Strategies. She can be contacted via twitter @CXOConnectME

Redefining cybersecurity in the Middle East

An interview with Karim Abillama

1. Karim, the Middle East has seen increasing cyberattacks, threats, and data breaches. What types of threats are META-based organizations most concerned about?

This is an undeniable fact: many nation-state attack campaigns targeting critical infrastructure are happening in the Middle East, specifically in the Gulf countries. We have engaged with a lot of government organizations who are targeted, particularly the sensitive ones (geo-political unrest, rivalries, other vulnerability factors) who are concerned about their cybersecurity posture. Two key aspects here are threat intelligence sharing and cyber resilience.

If you think about it, the first way to get ahead is visibility—seeing what’s really happening. You can’t protect what you don’t understand. Threat intelligence sharing among different groups is at the top of the agenda of some of the national initiatives in the GCC (Gulf Cooperation Council) countries, but there’s a lot to do. So, I would say visibility is top of mind. There are a lot of blind spots and breaches undetected—happening every other day—and with that is a need for more visibility.

They’re not quite sure what’s transpiring, and suddenly these organizations are in the media. That’s damaging both to their “crown jewels” and to their reputation. And in some cases, if you think of critical infrastructure, that’s even more damaging because it doesn’t only hurt its reputation, it can also destroy it and impact a critical service to the entire population.

2. Are there any issues you are seeing consistently with enterprises? Perhaps many of these organizations have the same “blind spots” that they need to address?

Absolutely. There are two scenarios for our customers that we engage with. There are those organizations that are aware of the blind spots and they need help—urgent help—to address these areas. And then there are those organizations who are not aware of those blind spots, facing bigger risks.

The more mature enterprises have some understanding of what those blind spots are, but even those organizations reach out to seek guidance on filling their visibility gaps. Those blind spots impede their Security Operations Center (SOC) to effectively detect and investigate threats efficiently.

Visibility that these organizations face is not limited to IT, but extends to their OT and IoT environments. There are many OT/IoT environments in the Middle East, not only oil and gas industries, but also “smart city” projects and other transportation and industrial manufacturing. For example, NEOM (an acronym for “New Future”) is a planned \$500 billion futuristic mega-city expected to cover 10,230 square miles in northwestern Saudi Arabia, abutting the Gulf of Aqaba. It rivals the size of Belgium! And that massive city will be built with sophisticated IoT and smart infrastructure, but with a plethora of cyber risks and exposure.

The biggest enemy is not really knowing what's happening. The unknown is what most organizations are dealing with.

3. With so much of the world's energy coming from the META region, what do enterprises really need to focus on for intelligent threat management and security operations?

It's essential to take two major actions: undertake a strategy to detect threats quickly, as well as adopt process to respond to those threats rapidly. To achieve these two vital milestones, organizations need not only a robust framework behind security processes, but also the right tool set. The challenges have been that these organizations have invested in cyber and preventative controls, yet these enterprises still have been breached. At NetWitness, we've talked to several customers who have invested in SIEM and SOC solutions—yet they are still breached frequently.

So from a technological standpoint, the solution to these threats would be for organizations to focus on a truly evolved threat detection and response platform, where they can analyze the data. Having all the data at-hand in one central location is critical so security teams can make sense of it, leveraging built-in analytics.

And by data, I mean a wealth of information coming off the network (endpoints fused with business context and threat intelligence) that you can collect from your infrastructure, whether it's your cloud or on-premise. The tendency here in the Middle East, especially within the critical infrastructure sector, is more in-country/on-premise than cloud. It's for better control and data sovereignty.

The focus comes back to the same concept I've mentioned: visibility. It's about clearly understanding what's occurring in your environment. Understanding the threat patterns. Really digging into that data. Having a “single pane of glass” to be able to quickly identify if there is a threat, and if it's possible to immediately respond and orchestrate your response to the threat(s) from a central location.

Because the challenge for many organizations I've talked to is that they're hopping in and out of disparate security tools. This is compounded by teams not having the accurate data and context behind the tool to make the right decisions efficiently. This creates fatigue for security operations teams. In many cases, it's a very manual effort that could take days (or even weeks) to analyze, trying to correlate the security information with data coming from so many different tools.

4. Karim, you work with people in many verticals, including government, healthcare, and banking industries. What's their pain—what challenges are security professionals trying to conquer?

There's the alert fatigue I've mentioned, but there's also a skills shortage problem worldwide, which is no different in the Middle East. Organizations are leaning more on technologies to help their SOC/security team or their MSS provider be more efficient at detection, analytics, response, and automation. The pain for many of these analysts is, “I have all these tools and all this data, but I can't really make sense of it; I don't have a big team.” Often, an analyst or small team isn't trained or doesn't have the right skillset to hunt: the hunt to recognize and analyze suspicious patterns.

There are scarce resources for a never-ending security battle. Organizations have turned to NetWitness' technology to help conquer that problem: how do I detect and know if there's something bad happening—and how do I respond quickly? The right threat detection and security operations, automation, and response (SOAR) platforms can make the lives of those analysts in the field easier and more efficient.

5. We mentioned oil and gas. Specifically for those industries in the Middle East, what is the state of development and investments in SOC environments?

There are some very large and mature organizations here in the Middle East that have invested substantially in cybersecurity. What I see in oil and gas are two major trends:

Trend 1: Generally there is more awareness, more breaches negatively impacting OT operations. This leads to more investment in SOCs, aimed at gaining an understanding of the situation, with visibility across both the IT and OT infrastructure. In any oil and gas environment, you're dealing with a lot of legacy infrastructure that typically relies on an external provider. The problem is many of the oil and gas customers don't have much control over those legacy applications, which means they create a bigger source of risk and don't always understand what's happening behind the scenes. That creates a BIG cybersecurity gap for them.

Trend 2: The fourth industrial revolution is leading IT/OT convergence to become a reality for many oil and gas companies. Some of them are ahead of others in this journey: Saudi Aramco has led the way on accelerating this convergence, through their digital transformation agendas. To gather additional data and provide more insights for predictive maintenance goals, more industrial IoT sensors will be implemented. That creates a far greater risk of those sensors to be hacked or tampered with, thus, the need for IoT visibility (an area NetWitness has been innovating around for quite some time). Major players in this industry realize that visibility into threats such as OT ransomware attacks is gaining traction, too.

6. Why is the NetWitness Platform also well-suited to the security needs of government operations?

It's no surprise that governments are extremely security-sensitive because historically they're so often targeted. Like other organizations, they want to get far ahead of their threat landscape. They seek investigative and forensics tools that provide a breadth of data to help them capture, analyze, and efficiently respond to threats. It's a matter of national security.

Working with governments or any industry for that matter, a key differentiator for us has been the combination of the tool and the expertise. If you provide the tool for the customer but not the team behind the tool, then you're not giving customers the true value of your product. The technical expertise of our incident response and threat hunting teams has been able to prove to clients the true value of NetWitness.

7. Let's talk strategy. How can these industries, governments, and infrastructures build a strong threat management strategy—where does it start and what are essential steps?

Great question. There's no one size fits all, as every organization starts at a different point of time in their journey.

For an effective roadmap, it should start with a proper risk-based assessment: What's most important to my business? How do I protect our most valuable assets? Where's my customer data and intellectual property?

After these questions, identify various risks that could affect those assets. What are my business' functions day-to-day? Assess with both a top-to-bottom and bottom-to-top approach. What is risky to my business? If we are breached, what's the cyber exposure? Who are our third parties, contractors, customers? These are the absolute questions to start with.

It depends upon industry and it differs dramatically from one organization to another, but I think it's equally important to understand the organization's wider threat landscape, too. Identifying first the "crown jewels" and then asking the question: "What could our enterprise be targeted with from a threat management point of view?"

Next up, build the capabilities needed to identify security vulnerabilities, and identify the right people, processes, and technology required for a proper threat detection and response strategy. Then the strategy can begin to form, encompassing visibility, enterprise-wide analysis and investigative capabilities, remediation, orchestration, and automation. Obviously, there are different ways to look at strategy, as some customers start looking at global frameworks to start their strategic journey.

8. Last question, Karim. Looking ahead, what does cybersecurity of the future look like?

The growth of smart cities. The technology drive of these cities, as well as the sophistication of adversaries in a complex yet fascinating region, will mean an even more diligent approach to threat detection and response. This will require essential visibility platforms.

These smart city projects are at the center stage of almost every government organization providing services to its citizens, so the use of IoT will become more prominent in this part of the world—and with that comes more IoT-specific hacks. The digitalization of the META region is gaining steam as a key priority for governments, and they'll need the technology to protect and secure their countries' futures.

The threat landscape will get more aggressive. Threat-wise, the usual opportunistic suspects will always be on the increase: phishing and commodity malware. You may also see an uptick in targeted supply chain attacks and ransomware. That will be a unique challenge, because here in the Middle East, so much of the digital agenda is pushed by the government rather than the private sector.

To counter the sophisticated threat actors, Extended Detection and Response (XDR) technology should provide analysts and threat hunters with a far superior and more accurate detection capability, as well as automated orchestration and response.

Here at NetWitness, we are focused on continually adding value to our patented network and endpoint detection capabilities. These efforts should help reduce the time needed to detect a panoply of targeted zero-day attacks, multi-staged ransomware attacks, encrypted attacks, and lateral movements. We are heavily investing in researching techniques and tactics adversaries are using. We're also looking to provide more threat detection curated content leveraging different sources: our own research, our world-class incident response team findings, our technology partners, and the cybersecurity community.



Karim Abillama
Presales Director, International Business
NetWitness, an RSA Business

Karim Abillama serves as the Presales Director of NetWitness, an RSA business, running teams of cybersecurity professionals, trusted advisors, and leaders across both Europe/Middle East/Africa (EMEA) and (Asia/Pacific/Japan) APJ.

Karim has spent 15 years in the cybersecurity industry, helping organizations address their cybersecurity challenges in various disciplines. Among those disciplines are network and web application security, threat detection and response, and identity and access management.

Karim holds an MS degree in network and systems security from the engineering faculty of Saint Joseph University in Lebanon.



Ransomware: A Beginner's Guide to Threat Detection

By Darren McCutchen

If you have followed the news over the first half of 2021, you've certainly been bombarded by the term "ransomware". Almost every week, another large company publicly discloses being impacted by this type of attack. Due to the increased awareness of ransomware, one may think that this is a new phenomenon. But it's not. (The first widely distributed ransomware attack, the AIDS Trojan, was delivered via floppy disk in 1989.)

At NetWitness we understand how devastating it can be to find yourself impacted by a ransomware attack, so we created this Ransomware FAQ. This intro to ransomware covers key ransomware concepts to equip IT and non-IT professionals with a greater understanding of this growing threat.

What exactly is ransomware?

Ransomware is a class of malware that, once executed on a victim's computer, renders the system and/or its data inaccessible until a ransom payment is completed. This is typically achieved by either:

1. Locker ransomware prevents the user from using basic system functions, making the computer inoperable. The goal of locker ransomware is to prevent system access, not destroy data.
2. Crypto ransomware identifies and encrypts the contents of entire drives and/or specific valuable data on the victim system. Beginning with CryptoLocker in 2013, most modern ransomware attacks involve some form of data encryption.

What does ransomware cost companies?

With improvements in encryption algorithms, the introduction of crypto payments, and easier distribution, the major difference from 1989 to today is financial:

- ◆ In 2019, costs associated with ransomware attacks passed \$7.5 billion. (Source)
- ◆ In 2021, medium-sized organizations paid out an average of \$170,404 for ransom demands. (Source)
- ◆ Over the last three years, requested ransom fees have increased 4,000%, going from \$5,000 in 2018 to around \$200,000 in 2020. (Source)

In 2021 alone, there have been several major high-profile ransomware attacks resulting in hundreds of millions of dollars lost:

- ◆ **CNA.** US-based insurance company CNA paid a \$40 million ransom payment after being attacked with Phoenix CryptoLocker ransomware, created by the group Evil Corp. More than 15,000 devices on the CNA network were impacted by the ransomware, including the systems of remote workers connected via VPN. CNA was forced to take many systems and its website offline for a short period of time. (Source)
- ◆ **Colonial Pipeline Company.** In late April, the DarkSide group was able to deploy ransomware on the Colonial operational network using leaked VPN credentials. As a result, Colonial was forced to shut down the entire pipeline for five days, resulting in massive gas shortages and higher fuel prices. After being threatened with a data leak using 100GB of data that DarkSide was able to exfiltrate, Colonial ended up paying a \$4.4 million ransom. (Source)
- ◆ **JBS USA.** On June 1, meat processing company JBS suffered a large-scale ransomware attack at the hands of the REvil (a.k.a. Sodinokibi) group, forcing the company to shutdown plants in Australia and Brazil. JBS ended up paying \$11 million in Bitcoin as a ransom payment. Post-compromise analysis revealed that REvil was able to conduct a three-month data exfiltration campaign (March 1–May 29, 2021) before any data encryption occurred. (Source)

Over the last three years, requested ransom fees have increased 4,000%, going from \$5,000 in 2018 to around \$200,000 in 2020.

How is ransomware distributed?

From the first widely distributed attacks using a floppy disk, to the use of botnets in the mid to late 2000s, ransomware distribution methods have evolved over the years. The most recent ransomware families and their associated variants most frequently employ the following techniques:

Phishing: Emails containing malicious links or attachments are one of the most common delivery techniques for ransomware payloads. According to Proofpoint's State of Phish report, 47% of successful phishing campaigns resulted in some form of ransomware infection.

- ◆ Ryuk, a ransomware developed by Russian hacking group WIZARD SPIDER, is primarily delivered as a second-stage infection after initial Trickbot infection via malicious email attachments.

Automated recon scans: This method employs open internet scans, using services such as Shodan, to identify internet facing systems with open ports (ex: TCP/3389-Remote Desktop Protocol) or running unpatched exploitable versions of software.

- ◆ CloP, a now defunct ransomware group, was able to exploit two zero-days, CVE-2021-27102 and CVE-2021-27104, which allowed for remote code execution within unpatched Accellion FTA instances.

Ransomware-as-a-Service (RaaS): A newer method of distribution, RaaS outsources the initial compromise of corporate systems (some will even outsource all actions up to ransom collection), with some form of subscription or profit splitting. While there are multiple revenue models for RaaS, some of the larger ransomware families like DoppelPaymer, Maze, and NetWalker are operating under the Affiliate model. In the Affiliate model, a ransomware provider will develop/maintain the malware's code in addition to setting up the associated infrastructure (payment portals, unique IDs, troubleshooting support, data leak sites). These groups will then recruit "affiliates" to deliver the ransomware payload to targeted victims. Once profits have been paid, the ransom group and the affiliates will split the profits.

What are the stages of a ransomware infection?

Once a target has been identified, the ransomware lifecycle can be observed through the following stages:

1. Initial Access/Distribution

This is the beginning of a ransomware attack.

In addition to the previously detailed methods of distribution, ransomware can infect victims via most well-known malware delivery mechanisms such as drive-by-downloads, mishandling of malicious data, third-party compromise, or as a secondary stage of previously downloaded malware. Due to the wide range of compromise vectors being like other types of malware, it is difficult to categorize an attack as solely ransomware during this stage.

2. Infection

Now that the dropper file is on the victim machine, a malicious executable (or another file) containing the ransomware payload is downloaded.

This can be completed by making a call to a hardcoded URL or as an automated second stage of the initial infection vector. At this point, you may see network traffic to suspicious IPs or domains that hold the malicious files. Once downloaded, the executable is typically placed in a local Windows %temp% directory (may also end up in the root or a subdirectory of C:\ such as C:\Windows), the original dropper file is removed, and the downloaded malicious file is executed.

3. Payload Staging

At this point, the ransomware begins to set itself up for successful execution.

The main goal of this stage is to ensure completion of ransomware attack and persistence through system shutdowns. Some actions the ransomware may take during this stage include but are not limited to:

- ◆ Running checks to see if ransomware has previously been deployed on the system
- ◆ Checking, adding, and modifying Registry values
- ◆ Discovering user accounts and their associated privileges
- ◆ Attempting privilege escalation
- ◆ Identifying mapped network shares
- ◆ Deleting system backups
- ◆ Disabling recovery tools
- ◆ Compiling encryption/decryption keys
- ◆ Adjusting system boot settings (some variants reboot victims in 'Safe Mode')
- ◆ Depending on the malware variant, C2 communication may be established.

4. Scanning

Once the ransomware payload has completed staging the environment, it begins identifying files to encrypt.

This can be completed by using a hardcoded list of files to target or avoid. In certain human operated ransomware campaigns, adversaries may manually identify highly valuable data to encrypt. In other cases, ransomware will encrypt an entire drive (Petya). Using the network mapping data gathered during "Payload Staging," ransomware can remotely identify systems/drives/files to target as well. Some recent ransomware variants will also look to encrypt data on any connected cloud storage providers.

5. Data Encryption

With the target data identified, ransomware will begin encrypting.

Files will be encrypted in one of two ways:

- ◆ Encrypted data will be written over the original data and data will be renamed,
- ◆ A copy of original data will be encrypted, and the original will be deleted.

Different ransomware families may prefer specific encryption algorithms or a combination of many. An example of this is in the Kaseya Supply Chain attack, in which REvil ransomware used a combination of Curve25519 (asymmetric) and Salsa20 (symmetric) encryption algorithms to encrypt target files. At some point either immediately prior, during, or after, encrypted files will be renamed and appended with a ransomware identifying hardcoded or dynamically generated file extension.

6. Ransom Demand. For any systems impacted by data encryption, a ransom note will be generated

This can be thought of as a "calling card" for the adversary. Notes can be dropped into a single directory, every directory that holds encrypted files, or as a "lock screen" on victim desktops. Typically, these notes will include characteristics (ransom note title, specific language, or direct mention of group) that informs the victim who attacked them. Ransom notes for specific ransomware families tend to be the same across many variants. Ransom notes will include the monetary demand in some form of crypto currency, how to access the payment portal, and a point of contact. Once paid, a private key is provided to the victim, however, there is no guarantee that the key will properly decrypt the targeted data. According to Sophos, "92% of victims lost at least some data, and more than 50% of them lost at least a third of their precious files, despite paying."

What are common behaviors of ransomware families?

With numerous ransomware families and their associated variants being actively exploited in the wild, cybersecurity professionals need a set of common criteria to identify, respond, and mitigate attacks more easily.

Some of the methods we've witnessed across multiple ransomware attacks include:

- ◆ Privilege escalation attempts prior to lateral movement
- ◆ Disabling of security tools and the killing of specific system processes
- ◆ Deletion of Volume Shadow Copy (via vssadmin, WMI, or other)
- ◆ Recovery prevention via BCDedit
- ◆ Preference for remote encryption of mapped network drives from 1 or 2 infected hosts
- ◆ Encryption of files (Overwrite vs. Copy/Delete Method)
- ◆ Renaming of files
- ◆ Creation of a ransom note

Not every ransomware variant will display every one of these traits. However some combination of these common behaviors will be present in most ransomware attacks.

How can you better detect ransomware?

Using network and endpoint data, these are the ransomware red flags to look for:

This is not a comprehensive list but should provide a starting point for detection of characteristics associated with a ransomware attack.

Large number of files renamed in short period of time

Accessing and disabling of services/processes/applications that could detect execution of ransomware payloads

System backups, recovery partitions, and volume shadow copies deleted

System event logs disabled or deleted

Example Command-Line Arguments:

- ◆ "C:\Windows\System32\wevtutil.exe" cl Security
- ◆ "C:\Windows\System32\wevtutil.exe" cl System
- ◆ "C:\Windows\System32\wevtutil.exe" cl Application
- ◆ "C:\Windows\System32\wevtutil.exe" cl Setup

Ransom note naming conventions
(only effective in stopping ongoing attacks)

Want to dive deeper on ransomware/NetWitness solutions?

If you want to learn more, check out these NetWitness resources or submit a demo request.

- *Managing Risk Amid Spike in Ransomware Attacks on Critical Infrastructure*
- *Using NetWitness to Detect Ransomware Attacks*
- *Detecting and Responding to Kaseya Ransomware with the NetWitness Platform*

How Useful Are Your Threat Intelligence Feeds?

By Brian Robertson

In the constant battle against threats, up-to-the-minute threat intelligence (TI) is critical. TI can guide your security operations team toward better decisions, but those security operations teams are also the source of some of your best native TI.

We find that many operations teams have tools that are good at ingesting and leveraging TI, however, they significantly lack the ability to provide guidance when it comes to utilizing that TI. There's a difference between security tools that simply ingest TI and those that are smart enough to present information to security analysts in a way that they can use to make informed decisions that help during analysis, investigation, and response.

How do security analysts make better informed decisions?

It is no secret that new and more sophisticated threats are emerging at a faster pace than ever before. However, new accompanying TI is also becoming available just as fast to help security analysts make better-informed decisions. Yet having all that intelligence available doesn't make security analysts more effective, if they have no shared context between the incidents they are investigating and how TI is consumed.

The security tools they use must be able to accomplish the following:

1. Present contextual TI to security analysts from where they are performing analysis, by linking TI and the cases together.
2. Validate the trustworthiness of specific pieces of TI to determine which feeds offer high-quality intelligence. This enables security analysts to focus their time and efforts using the most accurate sources of relative intel.
3. Deliver additional context around the artifacts or evidence within a case to quickly determine how critical the case is and if it is likely associated with a false positive.

Fortunately, there is a security orchestration and automation solution that can check all these boxes: NetWitness Orchestrator built on ThreatConnect version 6.1.

NetWitness Orchestrator can help

Since we introduced NetWitness Orchestrator almost two years ago, we have strived to empower security analysts with orchestration and automation capabilities to make better decisions while saving time, minimizing frustration, and improving collaboration across the security operations team and technologies- all while ultimately driving down risk.

In our latest NetWitness Orchestrator release version 6.1, we are delivering key functionality that reinforces our ability to make your security operations work at peak performance.

1 Linking Cases and Intelligence

Analysts want to be able to understand if there are previous or open investigations related to the case they are currently working on. We now make it possible to see all cases that the team has investigated related to an adversary to understand if it's something that has been seen before within the organization.

Users can understand relationships, whether defined by users or automatically made by NetWitness Orchestrator, across cases and intelligence within the system. This is done from the same page that the initial adversary analysis is executed, which saves time and frustration caused by constant context switches imposed by multiple screens and interfaces.

We find that many operations teams have tools that are good at ingesting and leveraging TI, however, they significantly lack the ability to provide guidance when it comes to utilizing that TI.

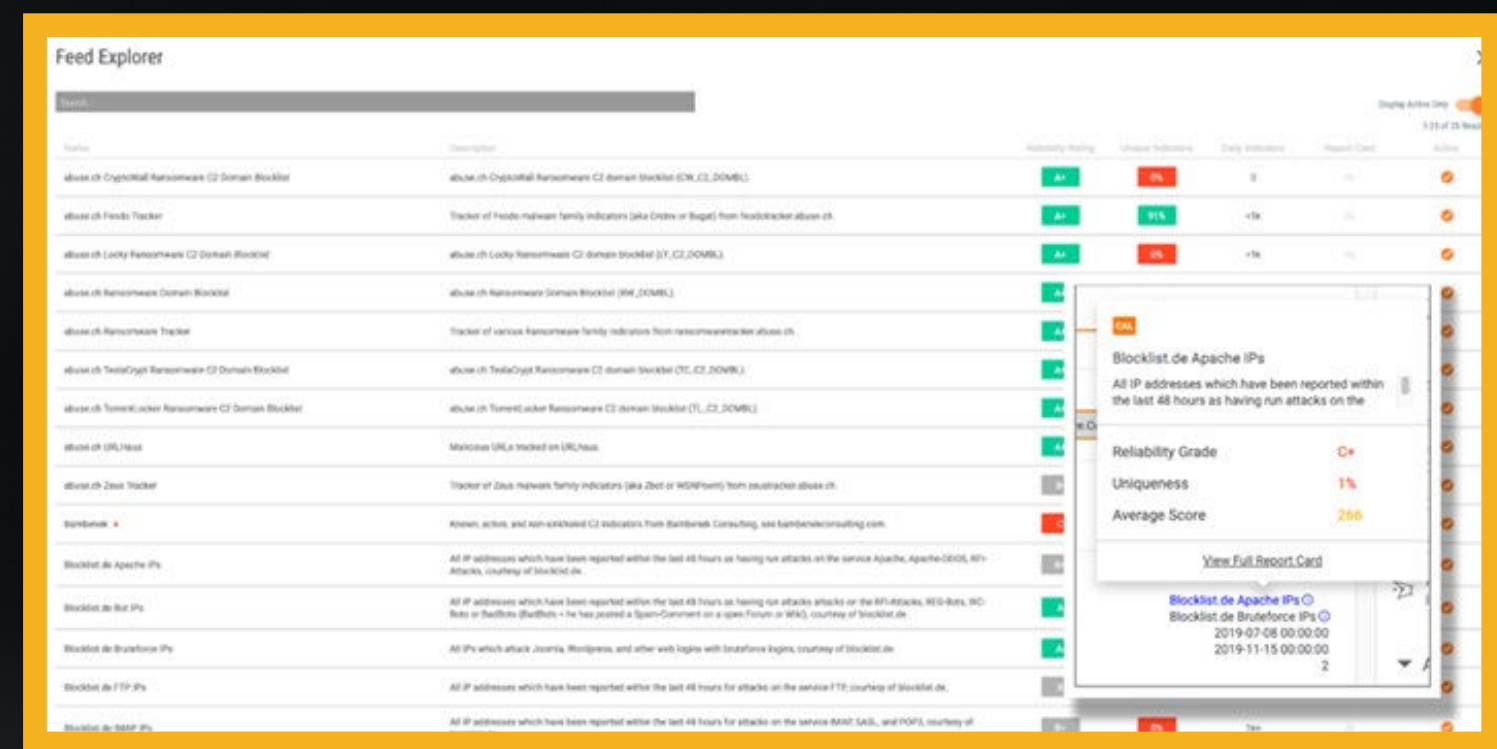
2 Report Cards Everywhere

Analysts want to be able to gauge the trustworthiness of a particular piece of TI. This requires the ability to determine which feeds are providing high-quality intelligence so that analysts can focus their time and effort on the most accurate sources. NetWitness Orchestrator delivers the ability to get immediate access to the information needed to make better strategic and tactical decisions during analysis or investigative processes.

With report cards everywhere, all users have access to the feed explorer that shows reliability and uniqueness for TI feeds. This helps evaluate the efficiency and accuracy of open and subscribed feeds, and uses that data to determine how to move forward with specific intelligence during the analysis or investigation process.

It can answer questions like:

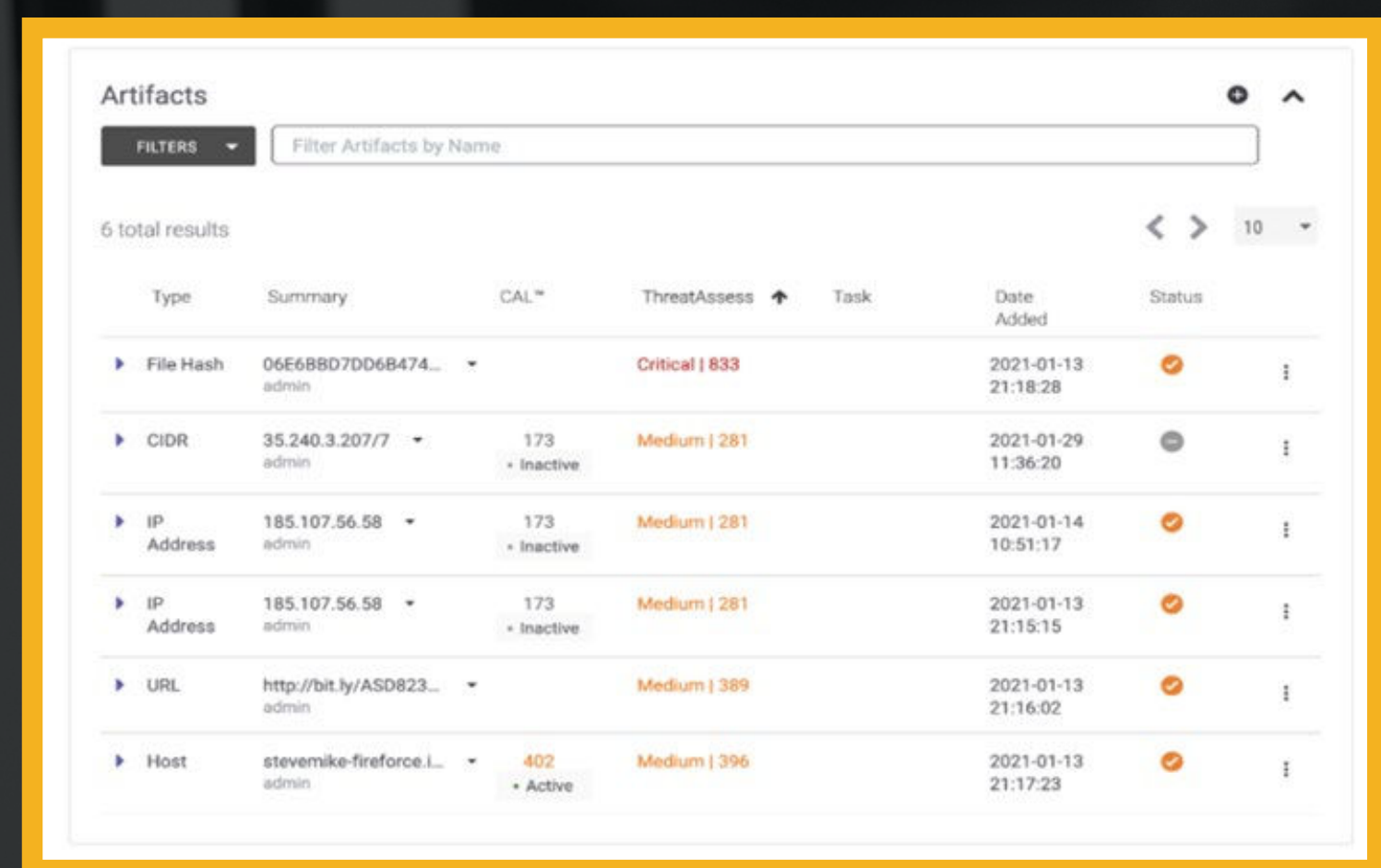
- How often does this TI feed report a false positive?
- How timely is this feed compared to other available feeds?
- Does this feed provide a breadth of information that expands beyond a single topic?
- Do the indicators in this feed tend to be more critical/malicious than others?



Feed Explorer allows users to view information like reliability and uniqueness of particular feeds. You can click and drill down into more detail when needed.

3 Actionable Artifact Context

When looking at artifacts or evidence of a case, analysts need to understand additional context. Simply knowing it exists and that it is related to the case is not enough. Analysts may need to consider hundreds of artifacts of a case, making it difficult to understand which artifacts carry the most weight. NetWitness Orchestrator has expanded the amount of context provided when viewing case artifacts. Now, security analysts are armed with the relevant TI they need to make more informed decisions by seeing which task added the artifacts, any crowd sourced details of the artifact, derived indicators, and much more. All artifacts are sorted so the most critical artifacts are presented at the top of the list.



Users are presented additional context about a particular artifact directly from the case screen, allowing them to come to faster conclusions about the potential criticality of an investigation.

These new capabilities are designed to make security operations more efficient. NetWitness Orchestrator merges TI and orchestration and automation into a single platform, empowering security analysts to fully exploit the value that the vast TI system provides.

For more information about NetWitness Orchestrator or to request a demo, click [here](#).

How NetWitness Protects against Ransomware Attacks

A recent report found that 70% of enterprise ransomware victims have paid ransoms and estimated that ransomware attacks could net cybercriminals \$20 billion in 2021.

From video games to healthcare to auto parts distributors to municipal governments, ransomware attacks are a major security issue for nearly every type of organization.

The attacks – which encrypt, block access to, or leak IP and other company information until a victim pays a fee – were already a challenge before the pandemic.

But as more people and businesses spend more of our time online than ever before, the impact of ransomware attacks is growing worse with the pandemic. Different outlets have reported that the total number of ransomware attacks is increasing, ransomware attacks are becoming more targeted, ransomware payouts are becoming steeper, or some combination of all three.

Wherever you look, the news isn't great: a recent report found that 70% of enterprise ransomware victims have paid ransoms and estimated that ransomware attacks could net cybercriminals \$20 billion in 2021.

Another troubling trend? Cybercriminals are increasingly using double extortion ransomware attacks, in which they threaten to “sell or even auction the encrypted data.”

Using NetWitness, an RSA Platform to prevent ransomware attacks

Cybercriminals who use ransomware want to infect as many endpoints as possible. To do that, they need to infiltrate the network, set up backdoors, harvest credentials, move laterally between users, and exfiltrate data.

Each of these steps represents a key point where defenders can identify and stop an attack before it does significant damage; it's critical that security analysts and engineers be aware of this process, as it can only take a few hours to move from one step to the next and launch an attack.

Each of these steps represents a key point where defenders can identify and stop an attack before it does significant damage; it's critical that security analysts and engineers be aware of this process, as it can only take a few hours to move from one step to the next and launch an attack.

Organizations can use NetWitness, an RSA Platform at each of these points to protect their IP and stop a ransomware attack before it starts.

The following resources explain how:

- ④ How to Begin Looking for Malware with NetWitness – four-minute video detailing manual malware analysis and binary identification using NetWitness 11.4
- ④ Using NetWitness to Detect Ransomware Attacks – our step-by-step guide detailing how businesses can use the solution to identify anomalous behaviors and prevent successful attacks
- ④ Detecting and Responding to a Ransomware Attack – see our infographic for steps on how to safely detect, investigate, and respond to an attack

Looking ahead

Ransomware isn't going away: Security Boulevard reported an average 139% year-over-year growth in ransomware attacks in Q3 of 2020 compared to the same period in 2019. Cybercriminals are becoming more targeted and more sophisticated in their approach as they aim their campaigns to encrypt the highest valued assets across all sectors. The good news is that we're still thinking of better, faster, and smarter ways to automatically respond to security incidents.

Source:

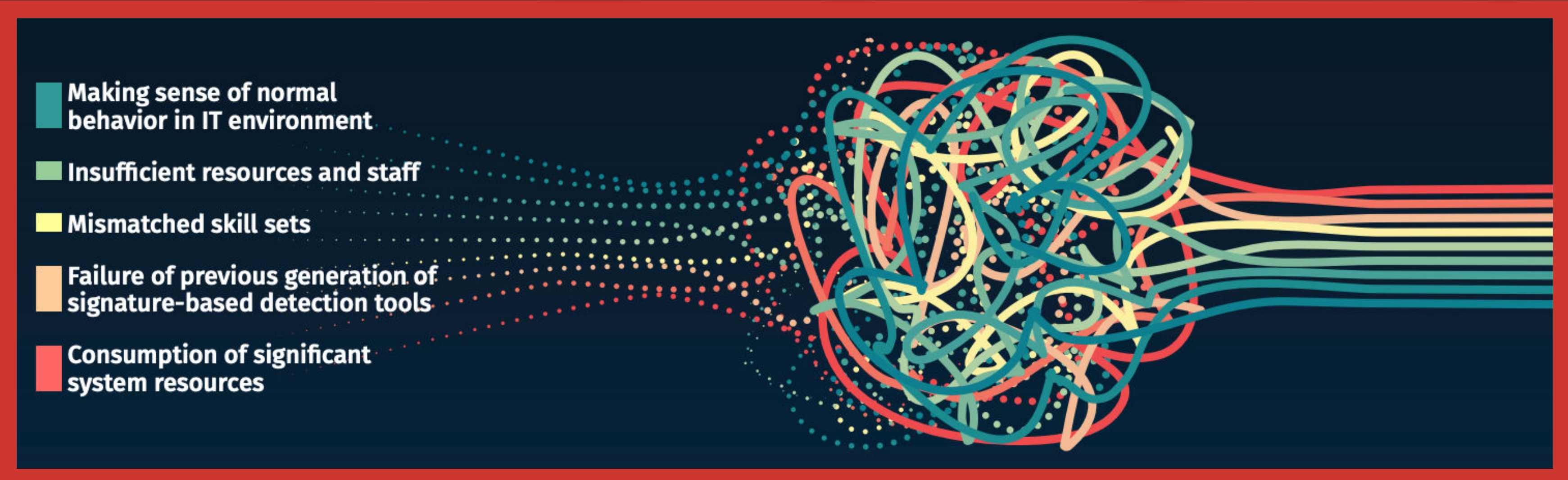
<https://www.netwitness.com/en-us/blog/2021-02/how-rsa-netwitness-platform-protects-against-ransomware-attacks>

Detect and Track Security Attacks with NetWitness

By Dave Shackelford, Sans Institute

Today's threats to our networks, applications, and data are not at all like those of the past. The attackers are getting smarter, the attacks are stealthier than before, and the sheer size and complexity of today's computing environments make the discovery of attacks, as well as the response efforts, much more complicated. Security teams have relied on log management, event monitoring, and correlation tools (usually SIEM platforms) to help aggregate security and other data, correlate events, and monitor activity within their environments. Now, however, security event monitoring and correlation tools are being taxed far more because many organizations are generating and storing much more data. In turn, more data is involved in security event management and monitoring.

Many organizations feel they still can't understand and baseline normal behavior in their IT environments, and the majority of organizations have insufficient people and dedicated resources—preventing progress in security operations. Security teams also can't find people with the right skill sets to manage SIEM and analytics tools, because these are notoriously complex. Another critical challenge is the way the previous generation of signature-based detection tools are failing us more often. Many attacks don't leverage malware at all—attackers are using memory-resident techniques, compromised credentials, and built-in system tools such as PowerShell to avoid detection by many of the traditional endpoint security platforms. Many endpoint tools also consume significant system resources.

- 
- Making sense of normal behavior in IT environment
 - Insufficient resources and staff
 - Mismatched skill sets
 - Failure of previous generation of signature-based detection tools
 - Consumption of significant system resources

The next generation of security event management and monitoring tools is focused on analytics and large datasets. They are based on the idea that by incorporating more data into our analysis, we will be able to perform more predictive analysis for baseline development as well as correlate more diverse information that could potentially help discover needles in the proverbial haystack.

The SANS Analyst team recently reviewed NetWitness®, an RSA Platform, one such security analytics tool, focusing specifically on:

- ④ Scalability and performance across massive and distributed datasets
- ④ Ease of use
- ④ Rapid searching, analysis, and incident correlation
- ④ Automated response tools

NetWitness includes many advanced features that are focused on reducing detection and response time for security operations and investigations, and processing large quantities of data from numerous sources in real time. One of the primary goals of the platform is to help overcome today's security skills gap resulting from a major lack of experts and not enough time to train tier 1 analysts on the job. By emphasizing ease of use, built-in intelligence and search tools, rapid event triage, and highly capable hunting methods, NetWitness is a capable intelligence-driven system that many security operations center (SOC) teams could leverage immediately to prevent or analyze attacks more quickly.

NetWitness Key Aspects: SIEM + NDR + EDR (XDR)

As a security analytics platform, one of the more powerful features of NetWitness is deep visibility into many types of events and data within an environment. Today, however, it's not enough to focus only on network data such as flow information and packet capture or endpoint events—we need all of it. In recent years, a newer model of detection and response has emerged, called extended detection and response (XDR), that combines network detection and response (NDR), endpoint detection and response (EDR), and SIEM. The goal of XDR platforms is to extend NDR and EDR to incorporate deep correlation and analytics to create an analysis capability more holistic than one of these technologies alone.

With this approach, SOC analysts, incident responders, and investigators can all gain access to a variety of insights that save time and facilitate more rapid response. Any primary detection and investigation platform used by an enterprise SOC needs to

offer a wide range of investigative tools and forensics artifacts, including network traffic, endpoint processes, files, and events, and the capability to detect behaviors in the environment that can be mapped to specific incidents or alerts of note. Because user accounts are often involved in attack scenarios (whether through insider threats, end user account compromise, or other attacks), analysts will need a strong user and entity behavior analytics (UEBA) capability—one that ties user behavior monitoring into the other types of event and system analyses being performed. Aside from simply monitoring and detecting threats, security operations and investigations teams are looking for remediation capabilities that can be implemented quickly. These capabilities may include but aren't limited to blocking network addresses, flagging assets for follow-up, and quarantining endpoint systems.

Together, these capabilities combine to form the basis for today's XDR model—deep introspection into both network traffic and system behavior, user account behavior monitoring, and capable correlation and analytics with strong visualization and investigative tools.

BOX OUT colored

Extended detection and response (XDR) combines network detection and response (NDR), endpoint detection and response (EDR), and SIEM. The goal of XDR platforms is to extend NDR and EDR to incorporate deep correlation and analytics to create an analysis capability more holistic than one of these technologies alone.

SANS Review Environment - Snapshot

Our review environment was set up with real exploits and malware in a testbed operated by NetWitness, which allowed us to fully analyze numerous examples of the product in action. Our first order of business was to evaluate the product's ease of use. Our priority was to explore the interface because many SOC teams are overburdened with events and investigations—analysts of all types need to rapidly detect signs of potential malicious activity and respond as soon as possible. We started by logging into the platform and viewing the new “Springboard” dashboard that allows analysts to create customized listings of specific areas of interest.

Source:

Extract from RSA Sponsored paper 'Detect and Track Security Attacks with NetWitness' by RSA, written by Dave Shackelford. To read the full paper, please visit [Detect and Track Security Attacks with NetWitness | SANS Institute](#).