NETWITNESS

Make Way for the Intelligent SOC

Will Gragido of NetWitness on the SOC's Evolution From Traditional to Intelligent

ISMG
INFORMATION SECURITY
MEDIA GROUP

NETWITNESS

Will Gragido

Gragido started his journey in technology when he joined the U.S. Marine Corps. He has been a leader in the cybersecurity industry's most outstanding services, product, threat research and intelligence organizations, including but not limited to ISS, Cassandra Security, TippingPoint DV Labs, RSA, NetWitness, FirstWatch, Digital Shadows, Hyas and Prevailion.

The evolution of security operations centers is resulting in major shifts in cybersecurity management. Traditional SOCs, often overwhelmed by the sheer volume of data and alerts, are making way for the intelligent SOC. **Will Gragido**, head of product management and intelligence at NetWitness, called it a "highly enriched contextual value that's highly actionable and ultimately drives decisions in a confident fashion."

The intelligent SOC is not just a technological upgrade but a paradigm shift toward more strategic, informed cybersecurity practices. This new model integrates various intelligence sources, including geopolitical and socioeconomic data, to enhance decision-making and operational efficiency.

"What we envision for the future is a revolution wherein the SOC becomes much more than just an analog for SIEM and other comparable technologies, but much more integral to all cybersecurity decision-making," Gragido said.

In this video interview with Information Security Media Group at RSA Conference 2024, Gragido also discussed:

- Why and how the traditional SOC has run its course;
- What the intelligence fusion center approach is and how it works;
- How NetWitness is helping customers develop and refine the intelligent SOC.

"Providing an intelligent approach to that, by introducing disparate sources of intelligence that provide depth and breadth from context, allows you to prioritize events in a more real-time fashion and drive toward more actionable and confident ends."

The Intelligent SOC

TOM FIELD: When you say "the intelligent SOC," what do you mean, and as opposed to what?

WILL GRAGIDO: The intelligent SOC represents a new motif and a new iteration on an era of SOCs that tended to be less driven by intelligent diffusion concepts. What we envision for the future is a revolution wherein the SOC becomes much more than just an analog for SIEM and other comparable technologies, but much more integral to all cybersecurity decision-making – that it's driven by disparate sources of intelligence, whether they're geopolitical, socioeconomic and other.

Thank you for your question. The NetWitness Intelligent SOC Initiative represents a paradigm shift in the way Security Operation Centers and intelligent decision-making processes are viewed in modern businesses, enterprises, and organizations across both public and private sectors.

This initiative is centered on the integration of diverse types of intelligence - including threat, social, economic, psychological, philosophical, statistical, and geopolitical intelligence. These are combined in a thoughtful and innovative manner using proprietary technology, tradecraft, and intellectual capital. This approach positions the SOC as the hub of all decision-making processes - be it business, threat detection, response, or other areas within the organization that chooses to adopt it.

This unique form of intelligence fusion center capability promises to revolutionize the way businesses and their assets - including human capital, engage and navigate in a world filled with threats and threat actors of all types. It provides them with higher degrees of confidence, capability, and the wherewithal to properly qualify, assess, prepare for, and defend against threats and adversaries across all categories of threat actor groups.

The Intelligent SOC Initiative is set to usher in a new era where intelligence, complemented by the tradecraft, along with bespoke forms of applied data science and threat detection rigor, will coalesce to enhance the value of investments in security technology of all types found within the adopting organization's environment.

At NetWitness, we are at the forefront of this initiative, leading the way in delivering on this promise today and into the future. Our unique approach and commitment to innovation set us apart, ensuring that we can provide unparalleled value to our customers.

FIELD: So, something that's not just spewing out alerts without any real discrimination?

GRAGIDO: That's correct. You have a highly enriched contextual value that's highly actionable and ultimately drives decisions in a confident fashion.

Indeed, the NetWitness Intelligent SOC Initiative is far more than a traditional capability that merely ingests data and generates alerts. It's a unique approach that revolutionizes how we perceive cybersecurity within our businesses. This initiative applies Intelligence Fusion Center constructs across a multitude of sources, offering a fresh perspective on Security Operation Centers (SOCs).

The Intelligent SOC Initiative aims to transform the role of the SOC from a generic cybersecurity hub into a more tailored, structured, and diverse entity. It coalesces various sources of data and intelligence to deliver practical cybersecurity outcomes for truly novel and advanced use cases. The goal is to safeguard the confidentiality, integrity, and availability of the organization while minimizing business-associated risks.

Moreover, this initiative makes it increasingly challenging and costly for adversaries of all types to achieve their objectives. Only NetWitness can deliver on this promise, both today and in the future, thanks to its unique approach and commitment to innovation. The Intelligent SOC Initiative is not just a step forward; it's a leap towards a more secure future.

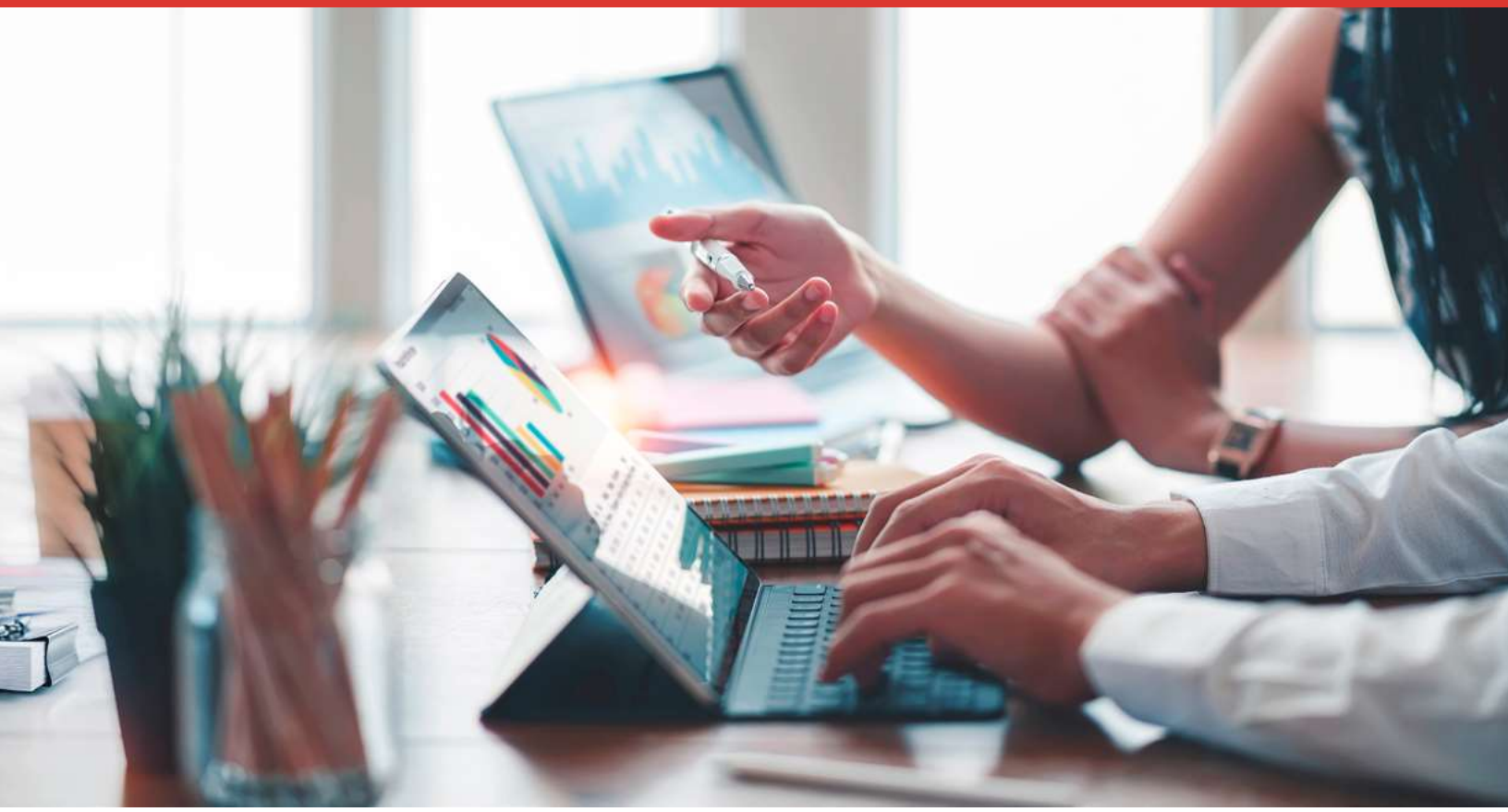
Drawbacks of the Traditional SOC

FIELD: Why and how has the traditional SOC run its course? A lot of security leaders run it down, and a lot of that's because of the overwhelming amount of data that gets released that no analysts reasonably can get through.

GRAGIDO: The volume of data, the volume of alerts, alert fatigue, understanding how to approach the data that you're dealing with on a minute-by-minute basis and how to prioritize that data in a meaningful fashion from events to incidents and actionable ends is really a concern in traditional SOCs. Providing an intelligent approach to that, by introducing disparate sources of intelligence that provide depth and breadth from context, allows you to prioritize events in a more real-time fashion and drive toward more actionable and confident ends.

Traditional Security Operation Centers (SOCs) are facing a multitude of challenges that have led to their diminishing effectiveness. One of the primary issues

"We're looking at a future that relies upon bespoke and tailored intelligence being combined with applied data science … taking a broad-spectrum approach to select applications of algorithms in addition to advancing threat detection capabilities."



is manpower overload, with SOCs struggling to staff adequately experienced personnel to address, analyze, and respond to an ever-expanding threat landscape and attack surfaces.

Despite efforts to automate, orchestrate, and simplify tasks, many processes within SOCs remain highly manual. This results in delays in threat analysis, detection, response, and mitigation. The pace of detection and response, both manual and automatic, is often slower than desired, further exacerbating the problem.

Another challenge is the siloed nature of many SOCs. Built upon incremental solutions or technologies, these SOCs often fail to foster collaboration across the organization, leading to inefficiencies and missed opportunities for threat detection and response. Moreover, stagnant processes and protocols, ineffective documentation, and the persistence of outdated management processes all contribute to the decreasing effectiveness of traditional SOCs.

In summary, these challenges underscore the need for a shift in our approach to cybersecurity, moving away from traditional SOC concepts towards more integrated, collaborative, and intelligent solutions. This is where the unique value of the NetWitness Intelligent SOC Initiative comes into play, promising a renaissance in how we think about cybersecurity within our businesses.

The Intelligent Fusion Center

FIELD: Your approach is called the intelligence fusion center approach. Define it, and discuss how it works.

GRAGIDO: The intelligent fusion center is a concept that came out of the military and federal constructs wherein you take disparate sources of intelligence and information from disparate sources of study as well as disciplines. You can mine those things to provide distilled, highly enriched, confident results that have meaning to a broad spectrum of audiences.

Our approach is to tap into that same construct and ideology, bringing in the best of breed from a machine-readable threat intelligence perspective, a human consumable intelligence perspective, as well as disparate sources of intelligence – examples being socioeconomic data, philosophical, geo theater-specific data and other. It has more highly attuned and bespoke outcomes for organizations that gravitate toward this construct that have more meaning and drive more value to the business.

Happy to do so. An intelligence fusion center – as I alluded to previously, is simply an organizational model that was designed or conceived for the express purpose of ingestion and sharing information and intelligence. These concepts go back many, many decades here in the United States having their roots in the United States Military and Law Enforcement. Over the years they have enjoyed many iterations, incarnations, forms, and implementations – some with greater degrees of success than others.

When approached thoughtfully, comprehensively, and rigorously, they can and are quite powerful and result in highly confident decision making and action resulting in reduced risk and higher degrees of threat mitigation. This has been observed in the public and private sector – in cyber threat intelligence and intelligence organizations in general. Our approach capitalizes on a bespoke or tailored approach to the creation and development intelligence work products unique to the organization in question. This approach is driven by a combination of recognized subject matter expertise, inter-disciplinary expertise, intelligence tradecraft, and highly tuned experience. Our belief is that through a novel application of the types of things we are discussing here today, we can enable organizations – geographically disparate organizations, to move and adapt to the ebbs and flows in the threat landscape and world at large thus changing the ways in which they conduct their respective businesses through anticipating movements against them in terms of direct or indirect targeting so they can better prepare and defend against such activity.

FIELD: I'm going to assume that predictive and generative AI both play a significant role.

GRAGIDO: They do, in addition to other forms of algorithmic application as it relates to the intersection of intelligence.

Skills Needed for an Intelligent SOC

FIELD: When you put the intelligent SOC fusion center to work here, you're relying on a different set of skills than what we typically have in our Level 1 and Level 2 analysts. What skills are required to make this approach work?

GRAGIDO: Traditional, foundational skills from an internet-working, cybersecurity perspective

will play a role in that. But so too will skills associated with some of those disparate sources of information and intelligence – knowledge in geopolitical, sociological and economic concerns and being able to tie those together to create a cohesive story that will drive a value within that ecosystem and environment. It's an evolution of what a SOC traditionally was known for, driving greater degrees of value within the business.

The Future of Detection and Response

FIELD: How do you envision the near future of detection and response?

GRAGIDO: We're looking at a future that relies upon bespoke and tailored intelligence being combined with applied data science, not necessarily confined to one model or one motif or another but taking a broad-spectrum approach to select applications of algorithms in addition to advancing threat detection capabilities.

The NetWitness Approach

FIELD: How is NetWitness helping its customers develop and refine the intelligent SOC approach? Give me an example or two of how it is different.

GRAGIDO: We're spending a lot of time advancing our innovation expertise as well as investments made in applied data science intelligence and threat detection capabilities. We believe that doing that from a hardware and a software perspective will drive more value to the customer and aid them in addressing modern-day threats. We have a large-scale plan underway that will see our hardware and software mature and also see us introduce more advanced algorithmic capabilities that will help them reduce the burden of events in the SOC and address deficiencies in their staff and their overarching capabilities from a compensating control perspective.

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 36 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® · CU INFO SECURITY® (Just for Credit Unions) · GOV INFO SECURITY® · HEALTHCARE INFO SECURITY®

infoRisk TODAY · CAREERS INFO SECURITY® · Data Breach TODAY (Prevention. Response. Notification.) · CyberEd.io

CIO.inc · DeviceSecurity.io · PaymentSecurity.io · FraudToday.io

CYBER THEORY · CyberEdBoard · Xtra mile LIFECYCLE MARKETING · GREYHEAD

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io