2024 Case Study

NOPSEC

Media Production Giant Casts in Lead Role for Exposure Management

Executive Summary

Cybersecurity leaders at this multi-national production company opted to streamline its vulnerability risk management (VRM) practice to surface and eliminate digital risk across several major film studios. The team chose NopSec's Cyber Threat Exposure Management (CTEM) platform to automate contextualization and prioritization of threats, drive faster mitigation, and evolve operations toward more mature and proactive risk management. In the process, cybersecurity strategists looked to machine learning (ML), a user-friendly exposure management portal, and advanced analytics to minimize analyst cycles, bridge cyber skills gaps, and gain predictive insight to up-level operations.

Media Company Profile

Markets served	**Worldwide**
Industry	**Media and entertainment (M&E)**
Products	**Feature films, streaming services, stage shows, music**
Annual revenues	**$80 billion**

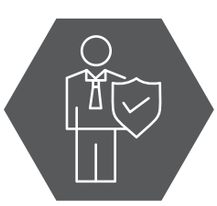
Challenges

Along with security operations at the headquarters in California, each film studio runs its own autonomous vulnerability management (VM) practice led by dedicated analysts—and sometimes artists—onsite. Those responsible for securing multi-million-dollar projects and state-of-the-art equipment battle two formidable enemies: modern threat actors, and time.

> This M&E leader owns the industry's largest franchises and highest-grossing films of all time. This long-standing company operates multiple world-leading production studios, accounting for a significant amount of M&E market share.

The company's CISO devised a plan to catapult the studios' vulnerability management practices to the next level quickly. Objectives for the project include automating delivery of accurate, actionable data to Vulnerability Managers at individual studios and reducing the time it takes to validate, prioritize, and remediate risk.

The team faces a host of logistical and cultural challenges in achieving these goals, including the industry's unrivaled need for secrecy and ceaseless operations.



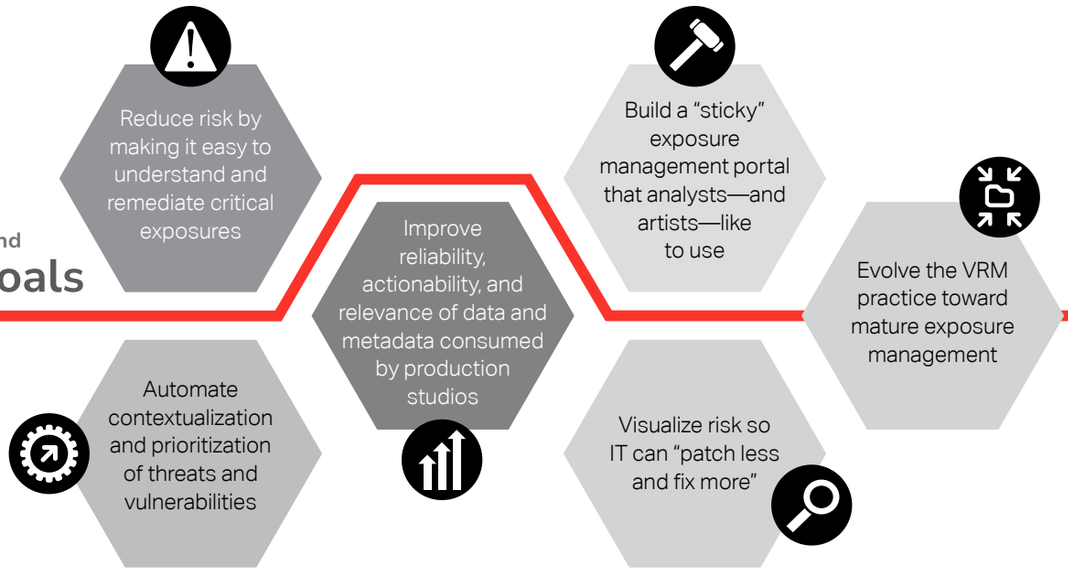
IT can't "Take 5" for security

Producers place a high premium on protecting content during the making of multi-million-dollar movies but assign cybersecurity a lower priority. "When Ryan Reynolds is on site burning $400- 500K a day, nobody's stopping for 15 minutes to patch," the CISO explains. "They'd rather take the risk even if the vulnerability is a Zero Day."

Despite the media and entertainment (M&E) industry's focus on secrecy, data privacy policies vary from studio to studio. While some grant artists inside the building access to everything, others employ such granular controls that editors around the world may not know what movies are about. Cybersecurity workflows need to stay flexible to accommodate each studio's unique culture and technology needs.

"We have artists and directors using the tools they prefer," the CISO adds. "We have to figure out how to let Ryan Reynolds edit on his iPad with apps that he's chosen and safely move the data through our content security lifecycle."

Business and Solution Goals



Complexity overwhelms traditional VM

With multiple agents running on multiple platforms, the complexity of managing vulnerabilities outpaces today's manual, siloed efforts. The CISO describes the traditional process as a "three-way handshake" that starts with the corporate team analyzing data from every scanner in the company's extended environment and sending lists of potential exposures out to each studio.

IT analysts onsite are then supposed to validate threats and send back business context—like whether assets are Internet-facing or exposed publicly through the production process—for further analysis. After several rounds of sharing insights back and forth, remediation plans get created that might or might not ever get put into practice.

Data lacks context to prioritize

Infrastructure teams at individual studios often complained of receiving too much data with too little guidance on what to do first. Without the resources needed to build and run their own risk calculators, IT experts resorted to exporting data into spreadsheets and scouring tagged data to find what matters to them.

Manual correlation of asset and exposure data consumes an exorbitant number of cycles each week and leaves teams reluctant to trust and act upon conclusions. "Just because CISA in DC says something is a Zero Day, we don't necessarily care because CISA doesn't put context to the asset we're protecting or to our critical production times," the CISO explains. "We need clear data to tell the studios, 'you have an immediate exposure to a celebrity vulnerability and push remediation plans to take care of the risk."

VM warrants a smarter, faster approach

Surfacing digital exposure without proposing mitigation strategies does little to reduce risk—especially when patching isn't an option. Intrigued by the Cyber Threat Exposure Management (CTEM) platform's unique value proposition, the CISO invited NopSec to demonstrate its power to predict risk, automate contextualization and prioritization, and deliver reliable data and action plans to its seven studios.

Solution

The NopSec platform aggregates and normalizes data from vulnerability scanners at every location, global threat intelligence feeds, endpoints, and asset management tools to give the entire Security team a single source of truth. "The platform ingests all the data and tells us what matters upfront," the CISO says. "This way we're all starting earlier in the process with a common set of information."

NopSec automates contextualization and prioritization to deliver the real-time exposure management insights Security Managers at the studios need. The platform applies modern machine learning (ML) to help analysts validate the severity of threats and increase the chances of critical vulnerabilities getting patched to avert serious risk.

ML assigns the right priority

automates the process of understanding and prioritizing which vulnerabilities can be allowed to 'age" and which, left unchecked, might lead to sensitive content and metadata being stolen. Fed by more than 50 threat intelligence sources worldwide, NopSec's machine learning algorithm offloads the time-consuming job of correlating asset data against celebrity vulnerabilities, Zero Days, and high-profile threats.

"In terms of exposure management, we need to know how much time we can buy ourselves," the CISO explains. "When does 'mean time to fix' need to be short and when can it be long because shutting down a particular rendering platform to patch would cost $10M? How long can we sustain without patching?"

To illuminate priorities that warrant urgent attention, the algorithm assesses risk based on critical factors such as:

- Assets running in each environment with known vulnerabilities
- Evidence of active threats or threat actors using known vulnerabilities to steal data or deploy ransomware
- Available controls in place to mitigate risk with or without patching

Context accelerates time to action

By equipping vulnerability managers with reliable business context, CTEM eliminates tedious manual efforts to reach the same conclusions. In surfacing clear priorities, NopSec's automated contextualization guides the team in devising targeted remediation plans—without analysts needing to build their own prioritization models.

"Everybody's conscientious of trying to kill the spreadsheets," the CISO says. "The NopSec platform provides obvious visual charting so there's no need for analysts to 'stare and compare' data across hundreds of rows to find what's relevant to them."

Where risk is high and the likelihood of patching vulnerabilities low, the platform helps to identify other potential shields and controls that can be used to offset exposure.

BEYOND RISK SCORES

Are known vulnerabilities being actively exploit?
Do exposures pose a serious threat to 24/7 operations?
Can we shut down risk without stopping to patch?

Results

Centralizing VM operations around the NopSec platform moves the production studios closer to the CISO's ultimate vision for, "automation and accuracy that create speed." The project met initial key performance indicators (KPIs) for understanding the number and severity of exposures and whether business tagging provided by scanners could be trusted.

Security experts and artists tasked with security functions appreciate the platform's ease of use, accuracy of data, and ability to save time and effort out of the gate.

"Sticky" portal gains rapid traction

The CISO's ultimate vision for managing digital exposure includes building a self-service portal that everyone involved in the process likes to use, and NopSec delivered. "We've been very impressed by the fact that engineers have taken to the portal," the CISO says. "The tool seems to be very 'sticky' and it appeals to the various personalities and various skill levels that have to use it."

Rapid traction allowed the project to progress quickly. After starting the pilot with one engineer working part-time, the team brought several new analysts on board to help scale the program.

Automation puts time on the side of defenders

Understanding Zero Day exposures once meant a "3–4-day fire drill" with analysts working to pull together and validate data from disparate tools in siloed environments. With the CTEM platform, immediate access to reliable data puts time on the side of defenders.

"If the time it takes a Zero Day announcement to progress to a Zero Day exploit globally is going to drop to less than 24 hours, we need prioritization automated and available for analyst consumption in less than 48 hours," the CISO observes. "NopSec helps us understand, 'how big is the fire' so we can have the fire trucks rolling upfront."

Automating asset management, correlation and contextualization saves Vulnerability Managers at individual studios 4-5 hours during the average week. Of even greater value, confidence in the VRM data frees up analysts hired to help vulnerability managers at each location to move onto higher-level projects.

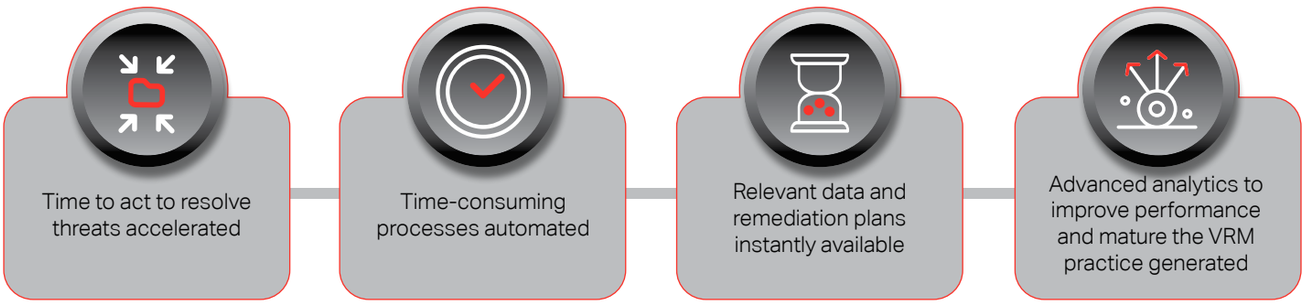
At the end of the day, the production studio teams envision requiring fewer specialized tools deployed at endpoints. Cross-checking data against Qualys and other solutions confirmed the accuracy of NopSec assessments which gives IT teams greater confidence to act upon data quickly.

Impact

As a foundational step toward continuous threat exposure management, adopting the NopSec platform allows the Security team to replace manual, reactive processes with automated, more proactive risk management. The ability to resolve risk without impeding production helps to promote a mature VRM practice to internal stakeholders as an "unburdening technology."

"If we can get this common tagging, categorization, and prioritization of what's important to the studios in place, we'll be asking engineers and artists to patch less, and they'll actually be fixing more," the CISO explains. "Blast zones for ransomware will be smaller and we'll be asking fewer artists to turn off their machines at 6 PM so we can patch."

MAJOR IMPACTS



A pivotal stop on the "maturity train"

Maturity also means leveraging more advanced, forward-looking analytics. The NopSec portal equips cybersecurity strategists to look at multiple types of data in one place and gain new insight into coverage gaps and team performance.

The CISO expects the platform to continue streamlining operations as the project scales and expands beyond agent-based solutions. "The deeper we dig the more complicated it gets and NopSec has taken the whole ride with us," the CISO says. "I give them kudos for being flexible to the problem set and extending themselves to take on strange new challenges. That's all we can ask, and we've been happy so far."

Ready to unlock those same gains?

As a Cyber Threat Exposure Management tool that works seamlessly with any security technology stack, we can empower you to champion change and mature your vulnerability management program. Leading prioritization, security insights, and workflow automation are just some of the ways our CTEM solution experts can help you achieve similar results. Take the first step right now!

Schedule a Demo Today

NOPSEC

Fix Less, Secure More

The World Leader in Exposure Management