CASE STUDY

Customer Success Story: A Leading Media/ Entertainment Company

A Media/Entertainment Company Identifies Potential IP Theft and Proactively Fortifies its Security Perimeter

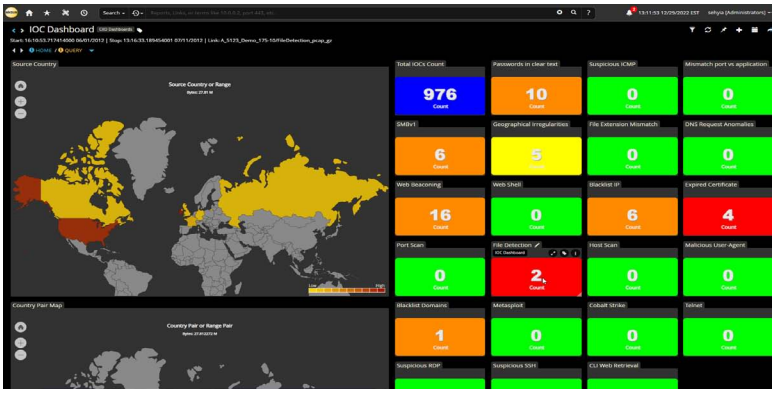
OVERVIEW

Challenge & Result

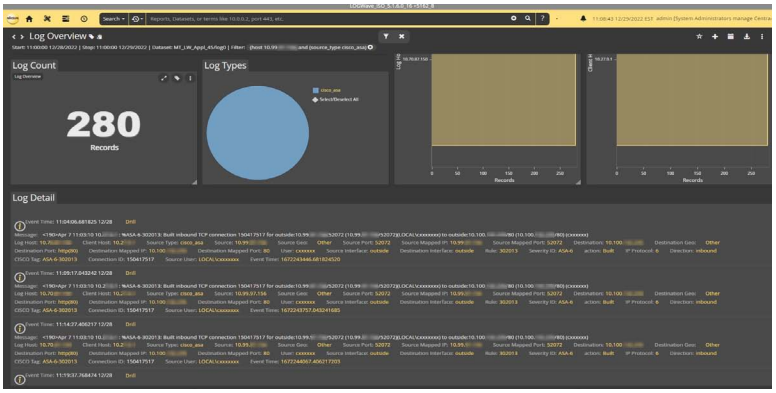
- *A leading M&E company wanted to ensure that it would be able to safeguard its IP property against theft*
- *Deploying NIKSUN's powerful NetDetectorLive Network Detection & Response (NDR) solution and next-generation LogWave SIEM allowed them to identify a case of attempted IP theft in real-time*
- *With NIKSUN, the M&E firm's SOC team was able to complete an end-to-end investigation of the incident in mere minutes and save a complete forensics trail of evidence for law enforcement*

NIKSUN Solution

- *NIKSUN NetDetectorLive™ Advanced for real-time content-based alerts*
- *NIKSUN LogWave® for proactive network, application, and services alarming and event management*
- *NIKSUN NetXperts™ using NIKSUN AI for application security, automated and optimized workflows*



NIKSUN's "IOC Dashboard" report showing content alarm alerts based on confidential files being transmitted to an external recipient



NIKSUN's "Log Overview" report shows details about the source IP address and username using cross-correlated information

For more information on Niksun products, applications and services, please contact Red Helix
Tel: 01296 397711 | Email: info@redhelix.co.uk
Web: www.redhelix.co.uk

Challenge

Today's Media and Entertainment (M&E) industry is diverse, digitally advanced, and covers a whole gamut of organizations including movie / TV production and distribution, newspapers, magazines, book and online publishers, streaming services, radio, music, video and audio recordings, video games, and many more businesses. The global M&E industry is worth approximately $2 trillion, with the U.S. having the largest market share at around $660 billion.[1]

In many instances, content is created, processed, edited, and disseminated using a distributed ecosystem that leaves it exposed to cyber threats. With its large attack surface, the entertainment industry is one of the most targeted by cyberattacks. The 2014 cyberattack on Sony Pictures was a giant wake-up call and was followed by similar-size attacks on Netflix and HBO in 2017 as well as a flurry of other incidents since then.[2, 3, 4]

The most invaluable asset for any media and entertainment company is, unquestionably, its content. The IP of any M&E firm is hugely critical to its profitability, making it an attractive target for cyber criminals looking for monetary gains. Threat actors are cognizant of this and are constantly looking for ways to infiltrate digital infrastructure of studios and access files related to upcoming movies or TV shows. If this high-profile content is stolen, the company suffers both lost revenue and reputational damage that may affect future returns in an extremely competitive industry. A TV show or movie released on the dark web before its official release date could spell doom for a studio and cost it millions of dollars.

To protect viewership and revenues, entertainment companies need to safeguard content from being leaked before an official release. As online streaming of shows and movies grows, this distribution of pirated content is also harmful to the bottom-line of entertainment companies. Thus, a robust security perimeter is critical for the protection of intellectual property (IP) content.

Solution

A well-known serial Director for a major television network and her team of screenwriters had come up with an artistically original screenplay for the pilot episode of a new TV show. The show's premise could prove to be groundbreaking and had the potential to generate immense revenue for the network. After bringing the screenplay to the television network executives, they received the go-ahead to produce the pilot. If the episode was received favorably by the TV audience, the network executives would approve funding for the first season of the new series.

Due to the recent major leaks at HBO and other firms, the network executives were extremely wary of the original screenplay falling into the hands of the public prior to its scheduled release. Given the commercial potential of the new show, they wanted to ensure that it remained under wraps until the pilot episode was released to the public.

Based on their requirements, the company's IT Director drew up a Request for Proposal (RFP) and received responses from multiple vendors. After evaluating the solutions offered, they decided to purchase NIKSUN's® NetDetectorLive™ and LogWave®. NIKSUN's NetDetectorLive is a full-suite network detection and response (NDR) device that supports the quick and efficient reconstruction of a wide range of network content. Its content-based alerts are extremely useful for detecting if key intellectual property resources are leaving the network. NIKSUN's LogWave is a highly scalable platform capable of ingesting and analyzing logs and events for deep analytics and use as a SIEM. Combined with the NetDetectorLive's content-based alerts, a single click of this next-generation SIEM allows users to see the relevant indexed metadata of any and every alert to provide complete context for every event.

NIKSUN's NetDetectorLive provides its users with the ability to perform precise content matching on files. Sensitive documents such as the screenplay can be uploaded to the NIKSUN platform so that precise content matching of network traffic can be done against the uploaded file to detect any leakage of the confidential information. If the screenplay appeared as an attachment to an email, for example, NetDetectorLive would immediately generate an event that would be displayed in NIKSUN's **IOC Dashboard** report. The information associated with the event, including the users involved, information exfiltrated, and whether it left the network is available in one-click, providing the complete, undeniable context of what happened.

1 https://www.trade.gov/media-entertainment
2 https://www.reuters.com/article/us-sony-cybersecurity/sony-pictures-computer-system-down-after-reported-hack-idUSKCN0J920720141125
3 https://www.bloomberg.com/news/articles/2017-08-11/hackers-are-threatening-the-way-that-hollywood-does-business
4 https://www.nytimes.com/2017/08/02/business/hbo-assesses-damage-from-cyberattack.html

After learning the system, the database security team charged with protecting this firm's IP created a new **Content** alarm. Using the **Actions** drop-down menu, they configured the **Create Files Detection** feature to upload the screenplay to NetDetectorLive. The result was that, if this script was detected leaving the network, a critical alarm would be triggered which can immediately be viewed in NIKSUN's out-of-box **IOC Dashboard** report. Taking advantage of NIKSUN's NetXperts feature, they enabled it to highlight specific data in the report (Severity levels: Red - critical, Orange - severe, Yellow – warning). Enabling NetXperts for the **IOC Dashboard** report immediately highlighted the alert.

At one point, an email containing the script as an attachment was sent from an apparently disgruntled internal employee to an external recipient. An email alert to the IT Director and network executives was instantly generated, identifying the attempted IP theft.

From this critical alert, they were able to pivot to the out-of-box **Log Overview** report, carrying over all contextual information, and immediately discovered the source IP address string in the log messages. NIKSUN automatically correlated the IP with the exact username of the disgruntled employee's IP address using firewall logs. Within a few minutes, they were able to conclusively demonstrate that the screenplay was being illegally exfiltrated, a clear indication of attempted IP theft. Because of NIKSUN's 100% accurate, zero-packet loss database, they were able to assemble a breadcrumbs trail of evidence which can stand up in a court of law. It was forwarded to HR, who were able to leverage the NIKSUN report to terminate the employee immediately, with cause, and to their legal team for next steps.

The powerful content monitoring of NIKSUN's NetDetectorLive and the SIEM capabilities of NIKSUN's LogWave now provides this team with the ability to monitor all their IP in real-time and easily access a complete forensics accounting of every alert triggered. It ensures this team can sleep easy knowing their IP is safe and provides a strong deterrent to their employees for mishandling their content. And, because NIKSUN's NetDetectorLive and LogWave act as one seamless product and can run together on one appliance or virtual appliance, deployment and investigations are easier, faster, and significantly less expensive versus any other tool.