Processing DMCA notices

You work for a university at which students, and sometimes faculty, use the network to distribute content illegally. By law, you are required to pass on notification of infringement of the Digital Millennium Copyright Act (DMCA) to the end user in violation. If you don’t pass on the notices, the university might become liable for the copyright infringement and owe damages to the reporting party. However, identifying the end user can be a challenge due to network authentication and network address translation. You want to use Splunk software to speed up the processing of DMCA notices. When provided with the date, time, and public IP address of the violation, your investigators can use Splunk software to determine which network user committed the violation.

Required data

- DHCP data
- Authentication data

How to use Splunk software for this use case

You can run many searches with Splunk software to determine who violated the DMCA and serve notice. Depending on what information you have available, you might find it useful to identify some or all of the following:

- Machine leasing an IP address at a particular point in time
- Device owner identified using a MAC address

Next steps

Measuring impact and benefit is critical to assessing the value of security operations. The following are example metrics that can be useful to monitor when implementing this use case:

- Time to investigate request: The average time it takes an analyst to complete the investigation stage of the notification process
- Monthly requests processed: The total number of requests that were fully processed within a month
- Monthly monetary value of risk avoided: The number of requests processed per month x average $$ of risk for notice

In addition, these two processes commonly impact success with this use case and should be reviewed for efficacy:

- Communicating the notices to the investigator
- Notifying the violator after an identity has been established

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
You might also be interested in the capabilities provided by the Campus Compliance Toolkit for NIST 800-171 app.