Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.
Being as prepared as possible to respond to an attack is business critical.

About the author
Tom Hofmann leads the intelligence directorate at Flashpoint that is responsible for the collection, analysis, production and dissemination of deep and dark web data. He works closely with clients to prioritise their intelligence requirements and ensures that internal Flashpoint operations are aligned to those needs. Hofmann has been at the forefront of cyber intelligence operations in the commercial, government and military sectors, and is known for his ability to drive effective intelligence operations to support offensive and defensive network operations.

References
1. Morgan, Steve. '2017 Cybercrime Report'. Cyber security Ventures, Feb 2017. Accessed Aug 2020. https://1c7fab3im83f5gqiwu2qps2k-wpengine.netdna-ssl.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf.
2. Graham, Luke. 'Ransomware can cost firms over $700,000; cloud computing may provide the protection they need.’ CNBC, Aug 2020. Accessed Aug 2020. www.cnbc.com/2017/08/04/cloud-computing-cyber-security-defend-against-ransomware-hacks.html.
3. Yadron, Danny. 'Los Angeles hospital paid $17,000 in bitcoin to ransomware hackers’. The Guardian, Feb 2016. Accessed Jul 2020. www.theguardian.com/technology/2016/feb/17/los-angeles-hospital-hacked-ransom-bitcoin-hollywood-presbyterian-medical-centre.
4. 'Ransomware: How consumers and businesses value their data.' IBM, Dec 2016. Accessed Jul 2020. www.ibm.com/account/reg/us-en/signup?formid=mrs-form-10908.
5. 'The crippling effects of targeted ransomware attacks.’ Flashpoint, Apr 2016. Accessed Jul 2020. www.flashpoint-intel.com/blog/cybercrime/the-crippling-effects-of-targeted-ransomware-attacks/.
6. Ventura, Vitor. 'SamSam – The Evolution continues netting over $325,000 in 4 weeks'. Talos Blog, 22 Jan 2018. Accessed Jul 2020. https://blog.talosintelligence.com/2018/01/samsam-evolution-continues-netting-over.html.
7. Cimpanu, Catalin. 'Here’s a list of all the ransomware gangs who will steal and leak your data if you don’t pay.' ZD NET, Apr 2020. Accessed Aug 2020. www.zdnet.com/article/heres-a-list-of-all-the-ransomware-gangs-who-will-steal-and-leak-your-data-if-you-dont-pay/.
8. 'HMR targeted by cyber criminals’. Hammersmith Medicines Research, 29 Apr 2020. Accessed Jul 2020. www.hmrlondon.com/hmr-targeted-by-cyber-criminals.
9. ‘How ransomware has become an ‘ethical’ dilemma in the Eastern European underground’. Flashpoint, 20 Sep 2017. Accessed Jul 2020. www.flashpoint-intel.com/blog/ransomware-ethical-dilemma-eastern-european-underground/.
10. 'Here’s what went wrong in the Baltimore ransomware attack that cost the city $18.2 million’ Cyware Social, 1 Oct 2019. Accessed Jul 2020. https://cyware.com/news/heres-what-went-wrong-in-baltimore-ransomware-attack-that-cost-the-city-over-182-million-3b6ac1a2.
11. Zelonis, Josh; Lyness, Trevor; Balaloukas, Stephanie; Cyr, Madeline; Dostie, Peggy. 'Forrester’s guide to paying ransomware: paying ransom can be a valid recovery option based on business need and circumstances’. Forrester, Jun 2019. Accessed Jul 2020. www.forrester.com/report/Forresters+Guide+To+Paying+Ransomware/-/E-RES154595.

Data highway and the digital transformation: arguments for secure, centralised log management

Robert Meyers, One Identity

Digital transformation happened all of a sudden, not with a gradual shift towards more sophisticated tools, but with a televised announcement from prime ministers and presidents across the globe asking organisations to do their part in containing the coronavirus outbreak. Almost overnight, companies found themselves having to adapt to a completely new mode of working. Some saw their remote workforce increasing exponentially, others had to swiftly make arrangements as they had previously always worked on-premise.

Faced with this challenge, companies had to put policies and technologies in place to allow employees to continue doing their job as they would have in the office. That meant that all the tools workers...
previously accessed from the corporate network now had to become accessible from outside the company perimeter. Some organisations opted for a VPN, others went for SSL connections through web applications or used Citrix farms.

“The logs that are sent into the SIEM include the logs from external access points such as remote machines, server logs, and things like terminal services and Citrix, as well as application logging”

But as all of this was happening, one thing remained the same: logs. These continued to be collected, regardless of whether users were within the network perimeter or in their own living rooms.

The importance of logs

Logs are collections of data about the activity and the performance of applications, systems and users. These are very useful from a security perspective, but also to monitor the overall performance of certain applications and tools. Normally, logs are fed into the organisation’s security information and event management (SIEM), which ultimately helps identify activity that shows signs of compromise or is potentially suspicious.

Interestingly, most companies don’t archive all the logs from their workstations, but favour storing just the ‘important’ logs. These traditionally include server logs, remote access logs, multi-user system logs, security logs and web application logs. Collected in a SIEM, these are used to provide real-time analysis.

Archiving only the more important logs helps SIEM vendors such as Splunk to control their costs. The model has generally worked well, especially given that the price of maintaining a SIEM is usually based on either the number of gigabytes of logs per day, or on the total amount of storage a customer requires.

But when a company goes from 50 remote workers to 5,000 in a matter of weeks, things change. The logs that are sent into the SIEM include the logs from external access points such as remote machines, server logs, and things like terminal services and Citrix, as well as application logging. This is what happened during the lockdown: organisations that previously only had a fraction of their workforce generating remote access logs and such now found themselves with an exponentially larger stream of logs feeding into their SIEMs.

Nor did this digital transformation happen in a gradual way, allowing for security procedures to be gradually implemented. Instead, it rapidly crushed our external user capabilities. Even companies like Microsoft and network providers are running into issues with so many changes taking place at the same time.

Organisations’ mode of working isn’t the only thing that was transformed rapidly. Privacy laws have continued to be refined to include certain logs in the definition of personal data. By virtue of being personal data, these logs must be kept encrypted and secured.

Centralised management

The concept of log management is often overlooked or unknown. Recently, many organisations simply stashed their logs into their SIEM and considered the job done, which has now been made impossible by the dramatic increase in the volume of logs to be collected.

To address the problem, organisations should consider implementing a centralised log management solution (CLM), which consolidates all the log data and pushes it to one, central data highway. This data highway will collect all the logs and direct them wherever they need to go. Essentially, a CLM is a product designed to make companies’ lives easier and reduce their SIEM costs, as SIEMs are not effective log management tools.

“Using a CLM would lift the burden of having to hire the staff, provide the training and the support for the deployment and the operation of a SIEM. Furthermore, it would reduce the costs that organisations would incur with their SIEM providers”

Dropping all logs into a SIEM means that these are sometimes fragmented or incomplete, thus impacting security monitoring and incident response. Using a CLM would lift the burden of having to hire the staff, provide the training and the support for the deployment and the operation of a SIEM. Furthermore, it would reduce the costs that organisations would incur with their SIEM providers, as well as the risk of endangering the
SIEM infrastructure by storing unmanaged logs.

Fragmented data collection becomes unified data collection. If your SIEM infrastructure was at risk due to the huge volume of data, now you can reduce the costs by filtering that data and delivering only what you need. This can also help with overcoming the age-old strategy of letting IT teams have their own source of data, which could instead be directed to the appropriate team via the data highway that is a CLM.

Cleaning up the data

Once logged, the data then needs to be parsed. Parsing is the process of analysing a string of data or pulling specific items out. In computing, we use parsing to build a structure for the data that we want. In this way, there are a few neat things that can be done to help security teams during this digital transformation.

Before you get to parsing out the specific items you want, let’s filter out the excess. The first way in which filtering can really help a company is by using this concept to remove unnecessary and unwanted information from the logs that are sent to the SIEM. That sounds a little weird, right? With parsing, it is possible to take a log and remove superfluous information, rewriting it on the fly to diminish the storage space it will take up and increase the usability of the data.

What kind of information is superfluous? One example is the timed mark that many applications add into the log of their system to show they are online. If this type of information isn’t something that a security auditor will need to see, then there is no reason why an organisation should be paying to store it in its SIEM. In fact, what about filtering out all the extraneous text that ends up in the log, or going the extra mile and adding parsing for specific events from your logs? As you can see, this could quickly and easily reduce the costs that are likely spiralling out of control during this time.

“Parsing, filtering, masking and other transformation techniques in a CLM will also allow security teams to overcome the privacy issues of log management and filter out personal information that shouldn’t be distributed”

Parsing, filtering, masking and other transformation techniques in a CLM will also allow security teams to overcome the privacy issues of log management and filter out personal information that shouldn’t be distributed. Specific personal data can be matched to a pattern and removed before the log is sent to the SIEM. This data can also be masked or de-identified. Resolving this problem could become crucial as more and more personal data is being collected than ever before, and as privacy laws are becoming stricter.

Efficient team

While not as important to the digital transformation in many ways, always remember that not everyone that is going to be reviewing logs will be utilising the SIEM or be highly skilled as a Linux or Unix administrator (or even be one at all). Or they just might like to have a graphical user interface.

Know that the team that will have to be able to easily operate your new data highway before selecting one, because you don’t want it to become an ornament on a shelf: your team must be able to use it.

Build the data highway

So, in this crush of new technologies spiralling into the new digital transformation age, don’t forget the importance of effective log management. You can optimise the SIEM and increase the likelihood of meeting compliance requirements. It’s possible to log from more places, and easily search them. With that encrypted data store, the compliance officer may even be able to sleep at night. And beyond the SIEM, it’s possible to then send data anywhere, including things like: Kafka, MongoDB, any database, big data systems, or anywhere else you can think of. Don’t just optimise your SIEM, build that data highway, collect those logs once, distribute them where they need to go, and cut costs with centralised log management.

Security teams don’t have to be put in the position where they have to go to the company’s management to say that they have uncontrolled SIEM costs. They can be managed and reduced without losing their effectiveness by simply feeding to the SIEM only the data that needs to be there.

About the author

Robert Meyers is a compliance and privacy professional, as well as the channel programme solutions architect for One Identity. He is a 30-year veteran of the identity and access systems and information security industry, including mergers and acquisitions, and with more than 10 years of that time focused on planning, supporting and managing privacy programmes such as FERPA, HIPAA, the GDPR and CCPA. His experience also includes leadership responsibilities for nearly 100 mergers and acquisitions. Meyers regularly speaks at events about privacy topics. His extensive certifications include IAPP Fellow of Information Privacy, CIPP/E, CIPT and the ISACA CISM and CDPSE.