DIGITAL MOUNTAIN®

SUMMER 2022 E-NEWSLETTER

At Digital Mountain, we assist our clients with their electronic discovery, digital forensics, cybersecurity, and data analytics needs. For this E-Newsletter, we discuss data exfiltration including prevention, digital forensics and case law.

Preventing Data Exfiltration: Can You Buy an Ounce of Prevention?

The Great Resignation, which saw nearly 48 million employee resignations in 2021 and continues with only a slight slowing in 2022, is changing the way organizations prepare for employee departures (https://www.zippia.com/advice/great-resignation-statistics/). No longer can organizations rely on a relatively stable workforce with only a slow drip of employee turnover. With estimates of workers tendering their resignations continuing at high rates, proactively preparing for turnover is no longer a luxury – it's a necessity that includes preventing unwanted data exfiltration. You don't want your data walking out the door with a former employee, but can you buy an ounce of prevention to stop data exfiltration?

DLP and SIEM: Working Better Together

Data Loss Prevention (DLP) is a process named for its goal: preventing data from being exfiltrated by protecting data on a network. The focus of DLP is the data itself. DLP processes start with understanding what information the organization owns, which information needs protection at what level (not all data is equal), and how the architecture of the network(s) on which the organization's data is created, accessed, and stored influences the security of the data. DLP is also the realm in which data security compliance is addressed.

Security Information and Event Management (SIEM) is a combination of detecting and preventing data exfiltration. SIEM provides automation due to advances in Artificial Intelligence. Unlike DLP's focus on the content of the data, the focus of SIEM is traffic associated with users (authorized and unauthorized) on the networks and the various endpoints. User and Event Analytics employed by SIEM products allow for automated analysis and response to patterns of behavior that fall outside the normal range on a particular endpoint or network. The content of the data on the network is, in and of itself, irrelevant to SIEM. SIEM and DLP products can often be integrated with each other and existing data security products, but care should be taken to ensure that the integration is done correctly and doesn't inadvertently create vulnerabilities or a cumbersome, productivity-robbing data blockade.

Key Elements in DLP Products:

For DLP to work, four processes must be carefully designed and put in place: identification, protection, detection, and remediation. Each process is unique and vital; however, all four elements must work in concert to achieve the best data protection possible.

Identification: By carefully examining the types and sources of the data that the organization encounters, a complete scope of data loss risks can be developed. However, if your organization hasn't performed an analysis of this type, or you have and/or still experienced data loss incidents, it's time to call in a trusted partner, like Digital Mountain, to help your organization develop a complete picture of data risk.

Protection: Is your organization encrypting data at every step of the creation-manipulation-movement-storage cycle? If data isn't encrypted all along the way, your organization may also have a security and compliance issue. Permissions and access need to be carefully controlled, and rules need to be followed with regard to what data is accessible by whom and under what circumstances. The protection aspect of DLP also addresses what can be downloaded, printed/screenshotted, attached to email, transferred off network, or stored on an external storage device. This is especially important if your organization has employees or contractors who may access data through mobile devices and/or remotely.

Detection: No gatekeeper will ever be flawless – at some point, a vulnerability will be discovered or created. That's why detecting bad actors, whether internal or external, matters. Adding a DLP product that will not only report a threat, but immediately respond by locking data down with encryption can save your organization precious time until a trusted team member or professional cybersecurity provider can address the incident.

Remediation: Knowing there's been an incursion into your organization's sensitive data is of little use if you don't correct the problem. This is another step that should be handled with care and expertise. Closing vulnerabilities shouldn't mean that your employees' productivity also grinds to a screeching halt – but may be as simple as making sure that a process is in place to communicate immediately when access permissions should be revoked or temporarily suspended. With certain SIEM products, there's an overlap in this function, which can provide the peace of mind that both the data itself and the access to the network are being monitored for threats.

Essential SIEM Tools:

Most SIEM providers offer the same basic tools: log management, real-time monitoring, automated reporting and alerts, and forensic investigation functions. By knowing which tools provide what information, your organization can decide which you want to prioritize and which to augment.

Log Management: Logs record events that take place from installation, access, event, even keystroke logs can be generated depending on the type of application and its code. To the average user, logs are invisible and provide no assistance or impediment. However, to the team administering the network, controlling access, maintaining storage, and responding to security incidents, these logs provide detailed audit trails of the traffic on the network and the relevant details necessary to piece together the events during a forensic investigation.

Real-Time Monitoring: For SIEM products, this is where AI advancements really shine. As networks grow and traffic increases, a natural by-product of organization growth, remote access, and data growth, the ability of humans to monitor network traffic in real time is eclipsed. By teaching an AI-enhanced application what the rules are for normal versus abnormal activity on a network, the application can oversee the signals sent over the network almost as quickly as they occur and analyze them in comparison to known rules. Additionally, SIEM real-time monitoring can be taught to recognize new endpoints and user credentials with a single instruction and won't forget that your organization's newest contractor isn't a hacker with a stolen login.

Automated Reporting and Alerts: As basic functions, automated reporting and alerts are a must-have. There's no question that every organization wants an immediate heads up when hackers are attacking the network. There's also value in knowing which users change devices often, regularly need password assistance, or are downloading copious amounts of data that shouldn't be necessary to do their jobs. Additionally, with automated alerts, parameters can be set to notify appropriate responders when threatening activity is detected.

Forensic Investigation Functions: In the unfortunate event of data exfiltration, forensic investigation functions in SIEM products can help digital forensics investigators quickly and thoroughly conduct an investigation that will produce courtroom acceptable results, if necessary. The tools offer a way for investigators to preserve the original logs and associated data without concern that they may have been altered or tampered with, that the data collected is accurate, timestamped, and reproduces the events completely, including the complete logs identifying the IP addresses and user identification associated with the breach. While these forensic investigation tools may be available to the onsite administrator, we recommend using the services of professional digital forensics investigators to produce the most reliable, thorough, and admissible evidence from the outset as these investigations can be complex and require specialized knowledge.

Irrespective of the products that an organization chooses to employ to prevent data exfiltration, the administration of the product and the response to alerts is the crux to getting the most out of DLP and SIEM products. No single product can prevent all data exfiltration. When departing employees are determined to find a way, even an old school method like screenshots, printed copies, and photos on mobile devices may not be detected or elevated as threats. The best prevention of data exfiltration may be pre-screening potential employees thoroughly and earning a reputation for zero tolerance of data theft.

Please direct questions and inquiries about electronic discovery, digital forensics, cybersecurity, and data analytics to info@digitalmountain.com.

UPCOMING INDUSTRY EVENTS

BLACK HAT USA 2022
Las Vegas, NV: August 6-11, 2022

DEFCON
Las Vegas, NV: August 11-14, 2022

ILTACON 2022
National Harbor, MD: August 21-25, 2022

PFIC 2022
Nashville, TN: September 6-9, 2022

SEDONA CONFERENCE WG12 ANNUAL MEETING 2022
Reston, VA: September 7-8, 2022

Click here to see more upcoming events and links.

Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at various upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com.

DIGITAL MOUNTAIN, INC.
4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

www.digitalmountain.com

Contact us today!

FOLLOW US AT: