DARKReading

4/11/2019
02:30 PM

Joe Partlow
Commentary
Connect Directly

0 COMMENTS
COMMENT NOW

Tweet Share

In Security, All Logs Are Not Created Equal

Prioritizing key log sources goes a long way toward effective incident response.

Like a triage nurse, security professionals have to prioritize the data that will help them best identify problems and keep the organization, its data, and devices safe from intruders and cyberattacks.

However, logging and monitoring all relevant events from across the IT environment can be challenging. For instance, some common log sources, such as servers, firewalls, Active Directory, intrusion detection systems, and endpoint tools, are fairly easy to ingest and parse. But other sources that are particularly valuable for incident response (IR) are difficult to manage at scale and rarely ingested because of the effort it takes.

In fact, a new 451 Research survey of 150 large enterprises found that enterprise security information and event management (SIEM) platforms are only ingesting logs from about 45% of their organizations' log-producing systems. This means teams risk missing critical information that could indicate a compromise and affect their overall security posture.

To maximize the benefits of logging, organizations must evaluate and adapt existing processes to fit current needs and threats, as well as consider logging additional — often overlooked — sources that are invaluable for IR and threat-hunting exercises. Here are five log sources that should be prioritized.

1. Database Logs

Database logging poses challenges for a number of reasons. Administrators often avoid enabling features, like auditing, that could impact server performance. Auditing databases and tables is very difficult given the large number of database servers resident in the typical enterprise environment. In addition, security teams struggle to gain access and visibility into operations occurring in databases created by third parties that have restrictions on viewing the data or table structures.

To gain sufficient visibility into the databases without enabling auditing functions, consider correlating built-in rules and alerts into your SIEM if database activity monitoring is present. You could also create stored procedures that watch for specific actions, and write an event log with the record ID, date, and time of the violating record entry to trigger an alert.

2. Web Server Logs

Of the major data breach vectors, holes in web applications – which typically have access to highly sensitive customer account information – represent the greatest percentage, according to the "2018 Verizon Data Breach Investigations Report." Unfortunately, security teams have the least visibility into web application logs.

In addition, parsing web server logs is challenging because they are often in a multi-line or custom format and logged in a nonstandard way to a text file or database, as opposed to the native web server log, such as Microsoft IIS or Apache. If you're using standard web server logs, be sure to enable all the relevant fields since the default W3C layout in IIS doesn't capture some critical elements, such as page size and cookie values. Logging events from a web application firewall (WAF) already watches for potentially malicious actions.

3. Domain Name System Logs

DNS server logs provide rich information about what sites users visit, and they show whether any malicious applications reach out to command-and-control sites. However, DNS also is a common tunneling protocol for exfiltrating data since firewalls typically allow the data out. DNS logs are challenging because of the volume of data, their multi-line format, and the difficulty posed in exporting them.

Consider using BIND, Infoblox, or even Microsoft's new Analytical Event Logging method, which uses a more standard logging format rather than the traditional debugging and flat file importing. The new Analytical logs have significant performance gains over the debug method, and the events are stored in the common Windows Event Log format.

4. Cloud Platform Logs

Enterprises are rapidly adopting cloud services, including Amazon Web Services, Google Cloud Platform, Microsoft Azure, Salesforce, and Dropbox, to store data and applications. However, many such services don't have consistent logging formats and require different parsers and methods of logging events from various applications housed on the platform. Building parsers to scale to the number of events is a challenge for most teams, but effectively prefiltering data before ingesting will prevent overwhelming your SIEM or logging tool by handling only the actionable events.

Cloud application security broker (CASB) solutions may not be all-encompassing enterprise

platforms, but they provide granular auditing capabilities at the application or service level and need to have the same logging and monitoring considerations as full cloud platforms. CASB solutions are essential for IR and forensic investigations since alerting on unauthorized access to cloud services can signal potential insider threats.

5. Physical Security Logs

It is extremely valuable to monitor for insider threats logs from camera systems, biometric/card access readers and alarm systems. Combining these with evidence correlated from servers, workstations, firewalls, VPNs, and remote access devices is essential to demonstrate whether credentials were stolen and establish insider location at specific points in time. However, the physical security team and the IT security team tend not to work together, which makes it difficult to gather and correlate the different log sources. Despite that, it's not impossible to ingest logs from the disparate systems. The focus should be on things like unauthorized physical access to remote facilities, visitor/contractor access to unauthorized areas, and after-hours alarm triggers.

Stay Alert

These five log sources are helpful in improving visibility into the entire enterprise security environment, but enterprises need to be smart about how they handle all the new alerts generated by their security products. The 451 Research report found that 43% of enterprises are unable to act on at least a quarter of the alerts, and nearly half said their SIEM, endpoint detection and response, and other data-capture systems were overwhelming their security operations capacity.

A good best practice is to create a roadmap with all of the possible log sources and have IT teams work with affected business units to set priorities, taking into account the level of effort ingesting will require and the potential risks that will be mitigated by doing so. Having security teams work with the data or application owners ahead of time ensures they can review the actionable event types together and disoverer where the source owners might need more visibility.

Related Content:

- Inside Incident Response: 6 Key Tips to Keep in Mind
- Threat Hunting 101: Not Mission Impossible for the Resource-Challenged
- Care and Feeding of Your SIEM
- DNS Hijacking Campaign Targets Organizations Globally

Interop19 MAY 20 - 23 THE MIRAGE, LAS VEGAS

Join Dark Reading LIVE for two cybersecurity summits at Interop 2019. Learn from the industry's most knowledgeable IT security experts. Check out the Interop agenda here.

Joe Partlow is currently the chief technology officer at ReliaQuest, an enterprise cybersecurity company. He has been involved with InfoSec in some capacity or role for over 15 years, mostly on the defensive side. Current projects include mobile and memory forensics, SIEM ... View Full Bio

COMMENT | EMAIL THIS | PRINT | RSS

MORE INSIGHTS

Webcasts

- Becoming a Threat Hunter in your Enterprise
- Building an Incident Readiness & Response Playbook

MORE WEBCASTS

White Papers

- 10 SMB Endpoint Security Problems - Solved
- 2019 Ponemon Report: The Value of Threat Intelligence

MORE WHITE PAPERS

Reports

- The State of Cyber Security Incident Response
- IT Threat Intelligence & How Enterprises Are Using It

MORE REPORTS

Copyright © 2019 UBM Electronics, A UBM company, All rights reserved. Privacy Policy | Terms of Service