13 ESSENTIAL LOG COLLECTION SOURCES

ALERT LOGIC®
Security. Compliance. Cloud.

Log management is an infrastructure management best practice that supports not only performance management but also security incident response and compliance requirements. Beyond its use for after-the-fact forensics, log management can be a key "early warning system" against possible breaches in progress that could replicate onto a disaster recovery infrastructure. Presented here is a list of log collections and alerts that can help support the infrastructure security of an automated log management system.

ANTI-MALWARE SOFTWARE

These logs can indicate malware detection, disinfection attempt results, file quarantines, when file-system scans were last performed, when anti-virus signature files were last updated, and when software upgrades have taken place.

AUTHENTICATION SERVERS

Servers typically log each and every authentication attempt and show the originating user ID, destination system or application, date and time, and success/failure details.

FIREWALLS

These very detailed and informative logs can show what activity was blocked according to security policies.

NETWORK ACCESS CONTROL SERVERS

These logs can provide useful information about both successful/permitted and unsuccessful quarantined network connections.

OPERATING SYSTEMS

Beyond typical log entries, operating system logs can contain information from security software and system applications that can help identify suspicious activity involving a particular host.

VULNERABILITY MANAGEMENT SOFTWARE

Scanning and patch management software log entries such as configuration, missing software updates, identified vulnerabilities, and patch/scan currency downloads.

WEB PROXIES

Web proxy logs record user activity and URLs accessed by specified users.

APPLICATIONS

Logs can include account changes, user authentication attempts, client and server activity, and configuration changes.

CLOUD-SPECIFIC SOURCES

New sources of log data from specific public cloud environments such as Amazon Web Services (AWS), Microsoft Azure, and Rackspace Public Cloud must be considered for collection. (Example: CloudTrail logs in AWS)

INTRUSION DETECTION & PROTECTION

These systems record detailed information about suspicious behavior and detected attacks as well as actions taken to halt malicious activity in progress.

NETWORK DEVICES

Logs from network devices like routers and switchers can provide information on network communication activity and what types of traffic were blocked.

VIRTUAL PRIVATE NETWORKS (VPNs)

VPN logs record both successful and failed connection attempts, date and time of connects and disconnects, and the types and amount of data sent and received during a session.

WEB APPLICATION FIREWALLS

WAFs generate "deny logs" which identify blocked application requests, useful in identifying attempted attacks that included applications as a possible attack vector.

LEARN MORE ABOUT LOG MANAGEMENT
http://alrt.co/LogManager

ALERT LOGIC®

4 LOG MANAGEMENT FUNDAMENTALS

Effective log management will help you achieve a holistic view of your data flows and more important, alert you to anomalies that could indicate security breaches. Stay ahead of potential threats by utilizing the following four components in your security strategy:

INCLUDE LOG MANAGEMENT IN THE INCIDENT RESPONSE PLAN.

1

Log management is most effective as an infrastructure security measure if it is included as a component of the incident response plan and not a second-thought measure during the chaotic hours after the incident. Specifically, consistent collection and analysis of multiple sources of log information from all data sources is the core process.

STORE LOG DATA SECURELY OFFSITE TO ENSURE AVAILABILITY.

2

Log information can be an attractive target for malicious hackers. Maintain log data securely offsite just as you would your core data to ensure its availability and integrity during a disaster incident.

SET ALERTS ON KEY ACTIVITIES TO GET WARNINGS OF UNUSUAL ACTIVITY.

3

Beyond its use for after-the-fact forensics, log management can also be a key "early warning system" against possible breaches in progress that could replicate onto a disaster recovery infrastructure. In addition to typical log types covering logins and administrator actions, an automated log management system can support infrastructure security by including log collections and alerts from sources such as anti-malware software, applications, web application firewalls, and more.

HAVE EXPERIENCED ANALYSTS REGULARLY REVIEW LOG DATA.

4

Warnings of possible threats to the infrastructure are embedded in all of the log data flowing through the above systems. Regular log analyses can reveal them and trigger preventive action. Few companies can afford the time and cost to have in-house IT staff sift through thousands of log entries per day and detect anomalies.

The breadth of log-generating servers, operating systems, databases, applications, and network infrastructure components is vast, but the powerful analytic engines in today's automated log management systems, combined with the expertise of live security analysts in a Security-as-a-Service environment, can quickly collect and analyze log data to deliver actionable results. Learn more about log management at http://alrt.co/LogManager.