Blumira

NSA Best Practices For Logging & Detection

GUIDANCE ON ATTACKER TECHNIQUES USED TO EVADE DETECTION

The NSA (National Security Agency) and the Australian Signals Directorate's Australian Cyber Security Centre have released Best Practices for Event Logging and Threat Detection to help organizations protect against malicious actors.

*"**Quality log data helps in building a comprehensive picture of your environment**, drives detection and alerting systems to discover issues quickly, and helps incident responders understand what went wrong if you do suffer a cybersecurity incident."*

– Scott Gee, AHA deputy national advisor for cybersecurity and risk, IndustryIntel

EVENT LOGGING POLICY

Take into consideration any shared responsibilities between service providers and the organization.

Policy should include:

- Details of the events to be logged
- Event logging facilities to be used
- How event logs will be monitored
- Event log retention durations
- When to reassess which logs are worth collecting

*"**Ideally, logs should be stored for a period of one year**, subject to storage space constraints. In the middle of an incident is not the time to find out that you were not logging useful data, or that you were not retaining that data for long enough to thoroughly investigate the incident."*

– Scott Gee, AHA deputy national advisor for cybersecurity and risk, IndustryIntel

EVENT LOG QUALITY

Consider logging the following to help detect malicious actors using LoTL techniques:

- **Linux**: Logs capturing the use of curl, systemctl, systemd, python and other common LOLBins
- **Microsoft Windows**: Logs capturing the use of wmic.exe, ntdsutil.exe, Netsh,cmd.exe, PowerShell, mshta.exe, rundll32.exe, resvr32.exe and other common LOLBins. Capture command execution, script block logging and module logging for PowerShell, and detailed tracking of admin tasks
- **Cloud**: Log all control plane operations, API calls and end user logins. Capture read and write activities, admin changes and authentication events

EVENT LOG RETENTION

Retain logs for long enough to support incident investigations; default periods are often insufficient.

- Log retention periods should be informed by risk assessment
- In some cases, it can take up to 18 months to discover an incident, with malware dwelling on a network from 70-200 days
- Review log storage allocations -- insufficient storage is a common obstacle to log retention
- **The longer logs can be kept, the higher the chances of determining the extent of an incident**

Blumira

ENTERPRISE NETWORK LOGGING

With a wide variety of native tools to exploit, enterprise networks should prioritize logging:

- Critical systems and data holdings likely to be targeted
- Internet-facing services, including remote access, network metadata and their underlying server operating system
- Identity and domain management servers
- Any other critical servers
- Edge devices, such as boundary routers and firewalls
- Administrative workstations
- Highly privileged systems such as configuration management, performance and availability
- Monitoring (in cases where privileged access is used), Continuous Integration/Continuous Delivery
- (CI/CD), vulnerability scanning services, secret and privilege management
- Data repositories
- Security-related and critical software
- User computers
- User application logs
- Web proxies used by organizational users and service accounts
- DNS services used by organizational users

PROTECT LOGS

To avoid or delay detection, malicious actors are known to modify or delete local system event logs. Logs should be aggregated in an event logging facility that can protect them from unauthorized modification and deletion.

Best practices include:

- Limit access only to personnel that need to have permission to delete or modify logs, or view logs
- Store logs in a separate or segmented network with additional security controls to prevent tampering
- Back up event logs and implement data redundancy practices

*"In the event of a cyber security incident, **an absence of historical event logs will frequently have a negative impact** on cyber security incident response activities."*

SECURE STORAGE & EVENT LOG INTEGRITY

They recommend organizations implement a secure, centralized event logging facility for log aggregation; forwarding their logs to analytic tools like security information and event management (**SIEM**) and extended detection and response (**XDR**) solutions.

The goal is to prevent the loss of logs once a local device's storage is exceeded, as many network infrastructure devices have limited local storage.

*"Organizations are encouraged to harden and segment their SIEM solutions from general IT environments. **SIEMs are attractive targets for malicious actors** because they contain a wealth of information, provide an analysis function, and can be a single point of failure in an organization's detection capability."*

SECURE TRANSPORT & STORAGE OF LOGS

To ensure event log integrity in transit and at rest, organizations should implement secure mechanisms like TLS 1.3 and methods of cryptographic verification.

Securing and restricting access to logs is also important to prioritize (enacting least privilege to grant access only to those that need it to do their jobs).

Blumira

DETECTING LIVING-OFF-THE-LAND TECHNIQUES

They recommend implementing analytics capabilities to enable automated detection of behavioral anomalies on networks, devices or accounts. They also recommend using a SIEM to detect anomalous activity by comparing event logs to a baseline of business-as-usual traffic and activity.

EXAMPLES OF ANOMALOUS BEHAVIOR

These are examples of actions to detect:

- A user logging in during unusual hours
- An account accessing services it doesn't usually access
- A user logging in using an unusual device
- A high volume of access attempts
- Any instances of impossible travel or concurrent logins from multiple geographic locations
- Downloading or exporting large volumes of data
- Network logins without defined computer access or physical access log validation
- A single IP address attempting to authenticate as multiple different users
- The creation of user accounts or disabled accounts being re-enabled (especially admin accounts)

*"**The increased prevalence of malicious actors employing LOTL techniques**, such as LOTL binaries (LOLBins) and fileless malware, **highlights the importance of implementing and maintaining an effective event logging solution**."*

MORE EXAMPLES OF ANOMALOUS BEHAVIOR

- Netflow data indicating one device talking to other internal devices it normally doesn't connect to
- Unusual script execution, software installation or use of admin tools
- Unexpected clearing of logs
- An execution of a process from an unusual or suspicious path
- Configuration changes to security software, such as Windows Defender and logging management software

BLUMIRA REVIEWS

*"**It's like having that extra person working for the city to help us with security**. It makes it a pretty easy choice. Automation is huge, especially with Blumira. It's ingesting billions of logs over the past six months. We don't have a dedicated person to actually look through and make determinations on that. **It'll save time.***

– Chris Lewis, Information Security Manager
NetSource One

*"**The interactions I've had with the Blumira team have been fantastic**; they made implementation really easy. The responsiveness to when there's an issue, and how quickly you guys walk us through it is great...I really appreciate that willingness to help us when we need it most, and also when I'm stressed out."*

– Jayme Rahz, CEO, Midway Swiss Turn

BLUMIRA'S BEST PRACTICES

- SIEM aggregates & analyzes logs
- XDR automates response to contain threats
- Detection rules identify attacker behavior
- 1 yr log retention for investigation & compliance
- Encrypted logs & secure access to log database

Users Love Us

SIEM + XDR TRIAL

Blumira's platform detects early signs of an attack and helps you respond faster to reduce its impact to your organization, preventing a data breach.

Visit blumira.com/xdr-trial