CRITICAL SECURITY: LOGGING, DETECTION & RESPONSE

What is it?

Setting up logging of your data across your entire environment and retaining those logs are critical for incident detection and response. The next step is centralizing those logs, correlating them, analyzing them for threats, and sending you alerts on possible security threats so you can respond quickly

Why it's important

01 **Security** - Without deeper visibility into your systems with log monitoring in place, threats can go undetected for too long, resulting in possible ransomware infection or data breaches.

02 **Compliance** - Many compliance frameworks (like CMMC, NIST, PCI DSS, HIPAA) require logging, audit trails and data retention for incident detection and response. They also require daily log reviews to help identify suspicious activity and threats.

03 **Cyber Insurance Claims** - Without the proper logging for digital forensics in place, you may not be able to get a cyber insurance claim paid out by your insurer, resulting in wasted spend and costly damages in the event of a security incident. Centralized logging and monitoring is becoming a requirement and obtaining an affordable policy without it may become a challenge.

Best practices

01 **Integrate broadly** - Start with systems that are already delivering security logs, such as IPS/IDS and endpoint protection. Then add on Windows, DNS, application and database logs for a deeper look into your infrastructure.

02 **Retain data** - Compliance regulations often require at least one year of log data retained and accessible for investigation and forensics, with another three months of additional data available for immediate analysis. Accurate time synchronization is also key for proper event correlation and to provide legally admissible evidence, in the event of a breach.

03 **Ensure integrity** - Make sure your logs are encrypted in transit and in storage, and access to them is limited to only those that need it to do their jobs. Store raw log files separately from your network for forensics in the event of a compromise, since attackers often try to cover their tracks by altering or deleting logs.

Contact us if you'd like to learn more about how to get started with Blumira's detection and response platform, including which plan is right for your organization to help you meet security best practices and compliance requirements.

Resources: Log File Monitoring & Alerting: Best Practices Guide