

# CASE STUDY



*“With the guidelines set forth by the Governor’s Office as it relates to Information Security, we needed a fast, automated, cost-effective method for capturing log data and providing sufficient analysis capabilities. Log data from our networked devices is a primary source of unimpeachable information.”*

**Bryant K. Young**  
Chief Information Officer  
Ohio Department of Developmental Disabilities (DODD)

*“I especially like the Device Summary. Currently, we have many different devices being monitored within our equipment network, and CorreLog helps us specifically pinpoint and identify issues from an informed standpoint. The customer service aspect also has been excellent – very helpful in the training phase, as well as with day-to-day questions that may come up.”*

**Aaron Austin**  
Data Security Analyst  
Information Security  
Ohio Department of Developmental Disabilities (DODD)



## Customer

### Ohio Department of Developmental Disabilities

## Objectives

- To enhance confidentiality, integrity, availability, assurance and accountability (CIA) across the Department of Developmental Disabilities Information Technology Systems
- Improve means to both quickly know about and respond to adverse events within the Department’s IT systems
- Provide a higher level of assurance to their constituency that their information is being protected

Greater reliance on IT systems requires the protection of the confidentiality, integrity and availability of those systems and the data they contain. As such, the Department of Developmental Disabilities (DODD) had a growing need to utilize information security products and services to protect the data entrusted to the department. The department sought to implement better centralized log management and event correlation both as internal processes and by implementing new technical approaches.

## Challenge

To obtain systems, software and professional services to achieve the following:

- Ability to log Microsoft Exchange mailing access
- Offer a willingness to extend or expand capabilities within the log aggregation/event correlation solution per customer request
- More effective means of gathering logs from disparate systems and software
- Aggregate logs on a centralized server; and effectively correlate events, visualize threats and research related events on disparate systems
- Provide real-time event correlation and alerting, with the ability to customize alerting rules and policies
- Effectively visualize logging activity
- Provide flexible reporting, both canned and customized
- Provide IT/log/event searching capabilities
- Encrypt agent-based log collection
- Scale upwards as needed
- Onsite staff training

## Solution

The DODD found that the ability to effectively monitor systems through their various logging and event/configuration reporting mechanisms resulted in quicker response to and handling of security incidents. Implementation of a centralized log management and event correlation system mitigated security risks that could otherwise go unrecognized for a significant amount of time.

## CorreLog Benefits Include:

- Understanding and pinpointing security risks throughout the network
- Supporting regulatory compliance, including Sarbanes-Oxley, HIPAA, PCI/DSS, NERC, GLBA, FISMA, FERPA and others
- Providing efficient event and syslog analysis; whereby reducing system downtime, increasing network performance, and tightening security policies
- Reducing data management complexity
- Avoiding security attacks with in-depth incident responses
- Determining unauthorized access attempts and other policy violations
- Honing in on applications that cause performance and security problems
- Identifying trends in user activity, server activity, peak usage times, and more
- Automating compliance and auditing reporting
- Detecting insider threat/fraud
- Responding to security incidents
- Obtaining useful event, trend, compliance and user activity reports



### CorreLog, Inc.

311 Conners Ave.

Naples, Florida 34108

1-877-CorreLog

239-514-3331

info@correlog.com

www.correlog.com

© 2010 CorreLog, Inc. All rights reserved.

## Results

The DODD found CorreLog's centralized log management and event correlation solution to most effectively remediate security risks. The capabilities of the software allowed for higher system and data integrity and reliability, less down time and higher productivity, better resource utilization in staff and system usage, better outcomes for adverse events, more accurate information regarding an adverse event, and the ability to quickly respond in an effective manner.

## Free, 30-Day Evaluation

Download a free evaluation of CorreLog for Windows 200x, XP and Vista systems at [www.correlog.com/download.html](http://www.correlog.com/download.html). Installation is easy and can be performed in less than five minutes.

## About CorreLog, Inc.

CorreLog, Inc. delivers security information and event management (SIEM) combined with deep correlation functions. CorreLog's flagship product, the CorreLog Security Correlation Server, combines log management, auto-learning functions, neural network technology, proprietary semantic correlation techniques and highly interoperable ticketing and reporting functions into a unique security solution. CorreLog automatically identifies and responds to network attacks, suspicious behavior and policy violations by collecting, indexing and correlating user activity and event data to pinpoint security threats, allowing organizations to respond quickly to compliance violations, policy breaches, cyber attacks and insider threats.

Visit [www.correlog.com](http://www.correlog.com) for more information.

## About the Ohio Department of Developmental Disabilities

The Ohio Department of Developmental Disabilities (DODD) is a cabinet-level agency reporting directly to the Office of the Governor, and is responsible for overseeing a statewide system of supports and services for people with developmental disabilities and their families. The Mission of the DODD is continuous improvement of the quality of life for Ohio's citizens with developmental disabilities and their families. The DODD Vision is that Ohio's citizens with developmental disabilities and their families will experience lifestyles that provide opportunities for personal security, physical and emotional well-being, full community participation, productivity, and equal rights. Our five goals include:

- Create less complex service delivery, with fair and logical payment systems that are federally compliant
- Continue to be good stewards of limited resources
- Provide quality outcomes through a combination of people and processes
- Design service delivery models in response to choices made by the people served, in alliance with community supports
- Develop a system-wide vision and long-range strategic plan by listening to our funding partners, constituents and stakeholders