

## Customer: Large Hedge Fund

**Target Application:** Internal Surveillance Monitoring / Policy Violations

**Compliance Applicability:** SEC Compliance

### Overview:

Customer is a large hedge fund whose business relies largely on automated trading through its custom-built trading algorithms. Customer had recently tightened security controls, and had a requirement to ensure that these security controls were not being violated. In addition, the customer was faced with routine regulatory audits by the Securities Exchange Commission and had to demonstrate that they were securing the environment through consistent monitoring and response. Since their IT controls were under scrutiny, the customer wanted to build a central monitoring solution that would detect and alert upon activities such as:

- Access to critical files (trading models, development code, etc.)
- Access to databases that house customer specific information.
- Privilege user access to production computer systems (especially during trading hours.)
- Unauthorized access attempts to multiple computer systems.

### Environment:

The customer's operating system environment is heterogeneous, composed of servers and desktops running Windows, Linux, AIX, and Solaris. The production databases are Sybase and Microsoft SQL Server. Critical files are stored on NetApp's Filers and EMC SAN devices.

### Solution:

Vigilant created a custom set of correlation rules and reports, driven by requirements summarized above.

### Custom Rules:

- **Correlated Login Failure** - An authentication event where a single source fails a login attempt across multiple technologies.
- **Brute Force Login Activity** - An authentication event where a user, or a source IP Address, has failed to login to a single target at a rate greater than the specified rate.
- **Production Login Violation** - An authentication event where a privileged user successfully performs a login attempt to a production host during trading hours.
- **Privileged Login Event** - An authentication event where a privileged account successfully performs a login attempt.
- **Privileged Login Failure** - An authentication event where a privileged account unsuccessfully performs a login attempt.
- **High Rate of Login Failures** - An authentication event where a single source has failed 5 or more times in a set period of time.
- **Critical File Access Violation** - An event where a user successfully accesses a file that they are not permitted to access.
- **Potential Theft of Intellectual Property** - An event where a user successfully copies a directory tree of files defined as critical.
- **Successful Critical File Access (Audit Rule)** - An event where a user successfully accesses a file defined as critical.
- **Unsuccessful Critical File Access** - An event where a user unsuccessfully attempts to access a file defined as critical.

**Custom Reports:**

- Executive Summary Report – (High level bar/pie chart)
- File Access Violations
- User Activity Violations
- Privileged User Activity Summary
- All Violations by User ID
- All Violations by Source IP / Source Hostname

**Summary:**

The customer's specific requirements for IT control monitoring were met by instituting a central monitoring solution for internal surveillance, and by leveraging Vigilant's consulting team to design and build tailored rules. The customer has peace of mind knowing that their SIM system provides 24x7 automated monitoring of their existing security controls, and that those controls are protecting their critical business assets. In addition, the customer is able to easily demonstrate that they are in compliance with guidelines set by the Securities Exchange Commission through the use of custom audit reports created above.