FRESCHE SOLUTIONS

Solution Brief

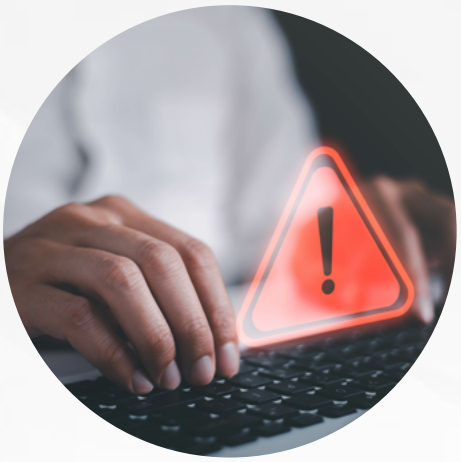
Detect

Security solutions you can trust.

Monitor IBM i Security Events

PROBLEM: There are numerous sources of security event data on IBM i and never enough time to review everything.

SOLUTION: Detect monitors numerous sources of security event data on IBM i and allows you to control how you want to be alerted on that data. QHST, Message Queues (including QSYSOPR), QAUDJRN, and Sensitive Command Monitoring are all covered.



Real-time Security Alerts

PROBLEM: Security threats are real. You need to know a problem is happening when it's happening. The longer it goes undetected, the harder it is to fix and clean up after.

SOLUTION: Detect alerts you to potentially critical security events as they are occurring so you can take remediation action quickly. Also, Detect alerts help you guard against potential security breaches by alerting you of suspicious activity as it's happening so you can take action.

See What's Important to You

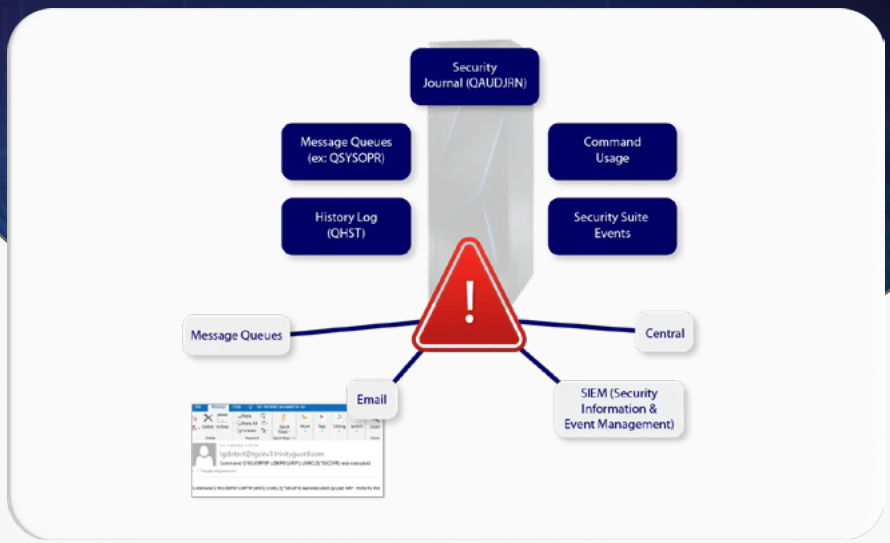
PROBLEM: A high volume of system events makes it difficult to differentiate critical security events from acceptable usage.

SOLUTION: Detect has incredible customization available so you can filter alerts based on what is important to you. See things like failed sign on attempts for specific powerful users and real-time journal events. Also use Security Suite message alerts for events like attempted remote connections, questionable user profile changes, and production library authority issues.

Key Benefits

Detect is a security event monitoring solution that provides flexible alerting capabilities for IBM i. Complete with a fully customizable rules filtering engine, Detect gives you the quick system activity insight you need to ensure you are protected against security breaches.

- Monitoring for major security-related event data including History Log, Security Journal, Message Queues, and Sensitive Commands.
- Funnels critical security events to the top
- Saves you time - no need to review endless records of event data
- Integrated with Security Suite
- Easy to install and configure
- Alert forwarding to Email, SIEM, MSGQ



Security Alerts for Your IBM i

The amount of security-related data on your IBM i can often be overwhelming to manage. Compliance regulations and auditors have vast logging requirements and report criteria. How do you know what security events to focus on? Detect alerts you to critical security events as they are happening so you do not need to spend hours reviewing audit data. With its robust monitoring and flexible alerting capabilities, you can simplify the process of identifying suspicious behavior on your IBM i.

Key Features

- Real-time alerts for suspicious system activity
- Save valuable time reviewing audit reports
- Receive alerts for critical security events as they are happening
- Easily escalate critical security events
- Use your existing SIEM solution to receive alerts and journal data

Benefits

- IBM i security alerts delivered to your inbox
- Monitoring for major sources of security information, including QHST, QAUDJRN,
- Command Usage, and Message Queues
- Integrated to efficiently work with and receive alerts from Audit and Secure
- Integration with any SIEM, including Splunk, Graylog, ArcSight, QRadar, and ELK Stack

About Fresche

Pioneers in IT modernization, Fresche manages, modernizes, and maximizes the value of IBM i business-critical systems. Our winning IP and proven solutions in Modernization, Cloud, Software and Application Services, and Strategy have earned the trust of global leaders from 2500+ companies.

Transform your IT challenges into future growth and innovation with Fresche Solutions.

FRESCHE SOLUTIONS
freschesolutions.com

Montreal, Quebec
995 Wellington, Suite 220
Montreal, QC H3C 1V3
+1 800-361-6782

Asheville, North Carolina
20 Fall Pippin Lane, Suite 202
Asheville, NC 28803
+1 800-669-7076

info@freschesolutions.com
support@freschesolutions.com