tyler
technologies

833.895.3783
info@tylertech.com
tylertech.com

# Cybersecurity: User Monitoring and Response For New World ERP

### DIRECT INTEGRATION

Direct integration with New World ERP program and authentication logs

### ENHANCED ANALYTICS

Enhanced analytics identifying suspicious user behavior

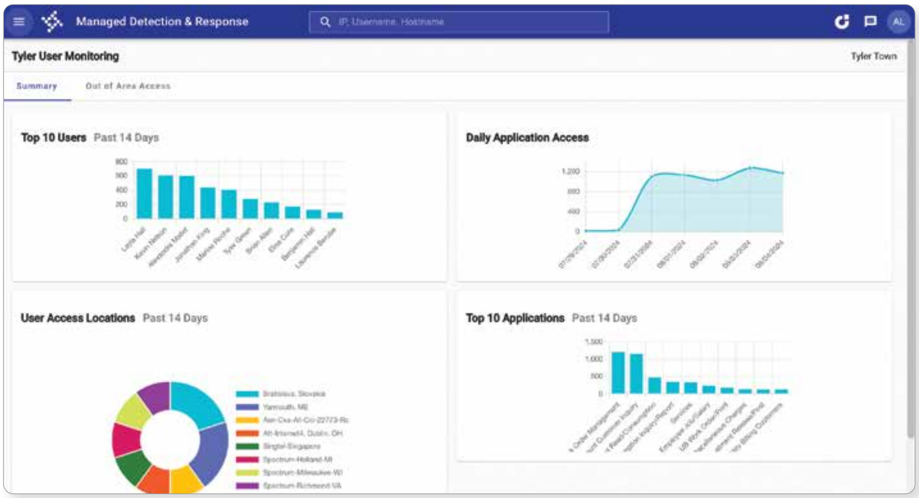
### 24/7/365 ALERTS

24/7/365 alerts from Tyler's Cybersecurity analysts

## IDENTIFY AND RESPOND TO SUSPICIOUS NEW WORLD ERP ACTIVITY

Tyler's User Monitoring and Response offers enhanced insights and increased awareness of potential suspicious New World ERP application activity.

Deployed standalone or as part of Tyler's Cybersecurity Managed Detection & Response, User Monitoring and Response identifies suspicious login activity within New World ERP and empowers clients to actively drill down from point of login to uncover what was accessed throughout the application and by whom.



Tyler's User Monitoring and Response provides enhanced analytics identifying suspicious user behavior within New World ERP.

## NEW WORLD ERP MONITORING AND ALERTS

User Monitoring and Response has a direct integration with New World ERP program activity logs to monitor and issue alerts of possible suspicious activity, including:

- Unsusual events for non-workflow mitigated events, such as mass updates and deletion of data
- Payroll/HR changes, such as deletion of payroll and duplicate check runs
- System administration changes
- Banking changes for vendors and employees
- Additional user behaviors

...continued on back

**For more information visit tylertech.com**

## USER MONITORING AND RESPONSE

User authentication and program activity from New World ERP is collected and monitored 24/7/365. Features include:

- Real-time alerting for:
  - — International logins
  - — Out-of-region logins
  - — Public cloud logins
  - — User-accessed modules within New World ERP
  - — Behavioral analytics alerts for abnormal user activity
  - — Concurrent geographical and anomalous login times alerts
  - — Customizable alerts
- Serverless deployment for SaaS clients. (No additional servers are required for on-premises clients.)

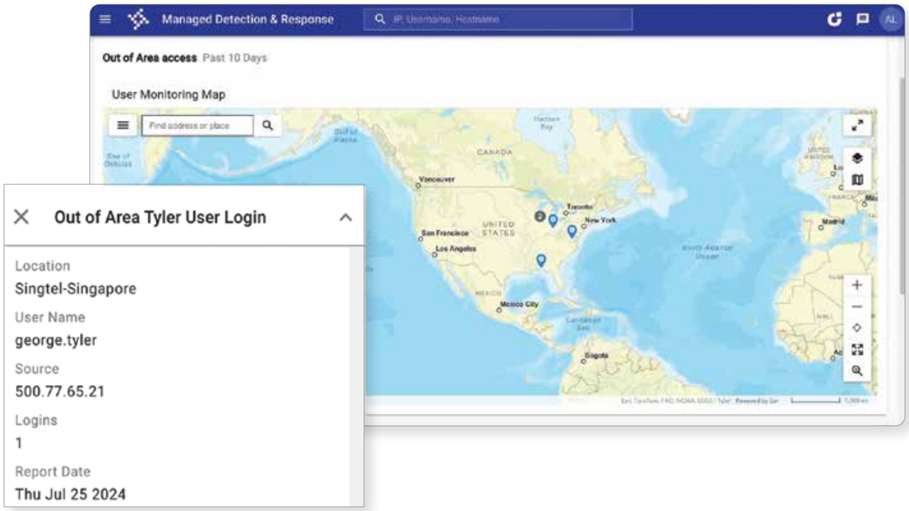
## 24/7/365 MONITORING AND RESPONSE

Tyler's User Monitoring and Response solution provides valuable insights by combining the logs from authentication and program activity. This extends the value of typical authentication solution monitoring. Logs are brought to life through enhanced analytics, and real-time alerts.

When suspicious activity is identified, Tyler's Cybersecurity Services 24/7/365 analysts respond immediately via text, email, or phone. Access activity can be viewed directly in client reports or in real-time via a secure, dedicated client portal.

To provide powerful insight into suspicous activity User Monitoring and Response:

- **Detects brute force/password spraying attacks** and provides transparency and customization of what is blocked. Logs are actively reviewed, and client alerts are generated.
- **Generates alerts for malicious attempts from large-scale/macro attacks** and will disable medium criticality login attempts by contacting the client via phone and email.
- **Provides enhanced log access.** Review the translated logs in the portal, search using a power-search feature, and review login sources on the map.
- **Provides 12 months of access/log retention.** Keeps all authentication logs, not just alerted events, for 12 months, which conforms to common compliance standards such as PCI, CJIS, NIST, CIS, and more.
- **Provides Security Incident and Event Management (SIEM)** for query and review of logs, custom alerting, and retention of logs to adhere to compliance frameworks.



Out of Area Tyler User Login

Location
Singtel-Singapore

User Name
george.tyler

Source
500.77.65.21

Logins
1

Report Date
Thu Jul 25 2024

View detailed information about users on a map, including who they are, when they log in, and where they're located.

Empowering people who serve the public®