Case Study

Townsend SECURITY

Boyd Gaming

Collecting real-time IBM i security events with Townsend Security's Alliance LogAgent for IBM QRadar

"Alliance LogAgent for IBM QRadar gives you a clear ROI. It creates time for your security and audit teams to focus on specific incidents that they can act on, instead of wasting resources on un-important data." - Anthony Johnson, IT Security Engineer

BOYD GAMING

Founded in 1975 as a family-owned company, Boyd Gaming Corporation is today one of the largest and most successful entertainment companies in the United States. The company currently owns and operates 22 gaming properties in 8 states – Nevada, New Jersey, Illinois, Indiana, Iowa, Kansas, Louisiana and Mississippi. While Boyd Gaming is a publicly traded company (BYD on the NYSE) it retains the original family influence in the management team. The IT operations are modern in every sense, and the security of their patrons is crucial for their continued success.

THE CHALLENGE

IBM i Log Collection and IBM Security QRadar Integration

Having chosen IBM Security's QRadar, Boyd Gaming needed a way to collect IBM i security and application logs into a coherent strategy for log collection and analysis. IBM i security events are stored in a proprietary format in a system journal that is not compatible with the IBM Security QRadar SIEM solution.

Before Alliance LogAgent for IBM QRadar, Boyd Gaming used a Device Support Module (DSM) that made copies of their journal and sent them out over FTP to a server, where QRadar would go grab them – a very cumbersome and inefficient process.

BOYDGAMING®

NEEDS

- Real-time IBM i log collection and monitoring
- Secure and native DSM support with IBM Security QRadar
- Solution that was easy to deploy and maintain

SOLUTION

- Log collection with Alliance LogAgent for IBM QRadar
- Significant improvements in Boyd Gaming's IT security
- Realized ROI by reducing IT time and resources

Boyd Gaming needed something that could collect IBM i security and application logs, convert them to the IBM log Event Extended Format (LEEF) and transmit them to IBM Security QRadar. By doing this, they brought their IBM i platform into a common strategy for log consolidation and analysis with the security events from other servers.

THE SOLUTION

Alliance LogAgent for IBM QRadar

"Alliance LogAgent for IBM QRadar does exactly what it needs to do. It was built for the IBM i and gives you the data you need," said Anthony Johnson, IT Security Engineer, Boyd Gaming. "Knowing that Townsend Security worked with IBM made Alliance LogAgent for IBM QRadar an easy choice. By being able collect all security events and convert them to the IBM Log Event Extended Format (LEEF) made a seamless deployment."

With Alliance LogAgent for IBM QRadar, logs can be collected from the IBM i security journal QAUDJRN user journals, system operator message queue, and system history file QHST. Log entries are converted from the internal IBM format to the LEEF format and transmitted to IBM Security QRadar for log collection, analysis, and alert management.

Improving IBM i Visibility

"As a security person, the AS400 stands alone, in regards to our IT infrastructure. With Alliance LogAgent for IBM QRadar, I get granularity in reporting and I can get data that I would never have been able to get," said Johnson.

The IBM i is often an enclave within an organization because logs are stored in many difference places in an IBM format, which presents a challenge for security administrators who need to monitor their IBM i logs. With Alliance LogAgent for IBM QRadar, users of this Gartner Magic Quadrant leading SIEM solution can now monitor their security events with a natively integrated solution.

Automatically Collect and Transmit System Security Events in Real-Time

"I love that Alliance LogAgent for IBM QRadar collects logs in real-time and don't have to wait an hour to get actual data. Additionally, by being able to set what I want to log, I don't have to manage an over-abundance of logs," said Johnson.

With Alliance LogAgent for IBM QRadar, Boyd Gaming now has a tool that can automatically collect system security events (QAUDJRN, QSYSOPR, etc.) and database changes, format them into the IBM QRadar LEEF format, and securely transmit them in real-time to IBM QRadar for consolidation with the security events from other servers.

Ease of Use

"By receiving logs in the LEEF format, we know exactly what we are seeing. Alliance LogAgent for IBM QRadar is not complicated, anyone can do it, anyone can manage it, it doesn't take an AS400 master or security person to understand it. It is simple," said Johnson.

For Boyd Gaming, getting started was very simple. With 15 installations of Alliance LogAgent for IBM QRadar, it only took one hour for them to get them to set up, configured, and begin collecting logs from their IBM i platform.

Not only does IBM Security QRadar perform real time monitoring of events across the Enterprise, it learns from the events over time in order to recognize normal patterns, detect anomalies, and better identify attacks and breaches. Combined with this intelligent platform IBM Security QRadar provides a broad set of compliance reports that are ready to use. Townsend Security's Alliance LogAgent for IBM QRadar helps IBM i customers realize the full benefits of the QRadar solution.

"Alliance LogAgent for IBM QRadar fits the bill for everything. It is very simple to set up, minimal maintenance, and once you set it, you never have to make any adjustments – set it and forget it," finished Johnson.

Townsend Security

Townsend Security provides data encryption & tokenization, key management, secure communications, and compliance logging solutions to Enterprise customers on a variety of server platforms including IBM i, IBM z, Windows, and Linux. The company can be reached on the web at www.townsendsecurity.com, or (800) 357-1019.

LEARN MORE

Product Information
Alliance LogAgent for IBM QRadar

White Paper
Making Security Better for IBM i and IBM Security QRadar

Podcast
Monitoring IBM i Logs with IBM Security QRadar