— CASE IN POINT | **DATADOG**

Securing 55 Hospitals in Four Weeks at AdventHealth

RapDev's migration of AdventHealth's SIEM and infrastructure monitoring to Datadog secured 55 hospitals and 100K+ endpoints in just four weeks, with zero gaps in detection coverage and zero disruption to patient care.

Four decisions that made the four-week timeline work

Challenge & Technical Solution	Business Impact
Migrated SIEM and infrastructure monitoring off LogRhythm, SolarWinds **across 55 hospitals in four weeks**, under ServiceNow change control	**189** **hours of patient and caregiver impact avoided** during cutover
Translated **452 legacy detection rules into 350 purpose-built rules** mapped to MITRE ATT&CK and deployed as detection-as-code	**55%** **of events contained before escalation**, thanks to cleaner signal and fewer false positives
Standardized deployment with Ansible, PowerShell, and Helm to reach **100K+ endpoints, 10K+ network devices, and 5K+ servers**	**3hrs** **mean time to resolution, down from 7 hours,** with zero change-related incidents
Built tagging, RBAC, and PHI data classification into the pipeline **before the first source went live**	**50%** **fewer major incidents**, with every event auto-routed to ServiceNow carrying team, priority, and CI context

> "I didn't need speed alone. I needed disciplined execution inside our operating constraints. **RapDev and our team brought the horsepower. Datadog gave us the wheels.**"
>
> - *Hector Castaneda, Director, Intelligent Operations Center, AdventHealth*

T. +1-855-857-0222
e. sales@rapdev.io
www.rapdev.io

CONTACT US