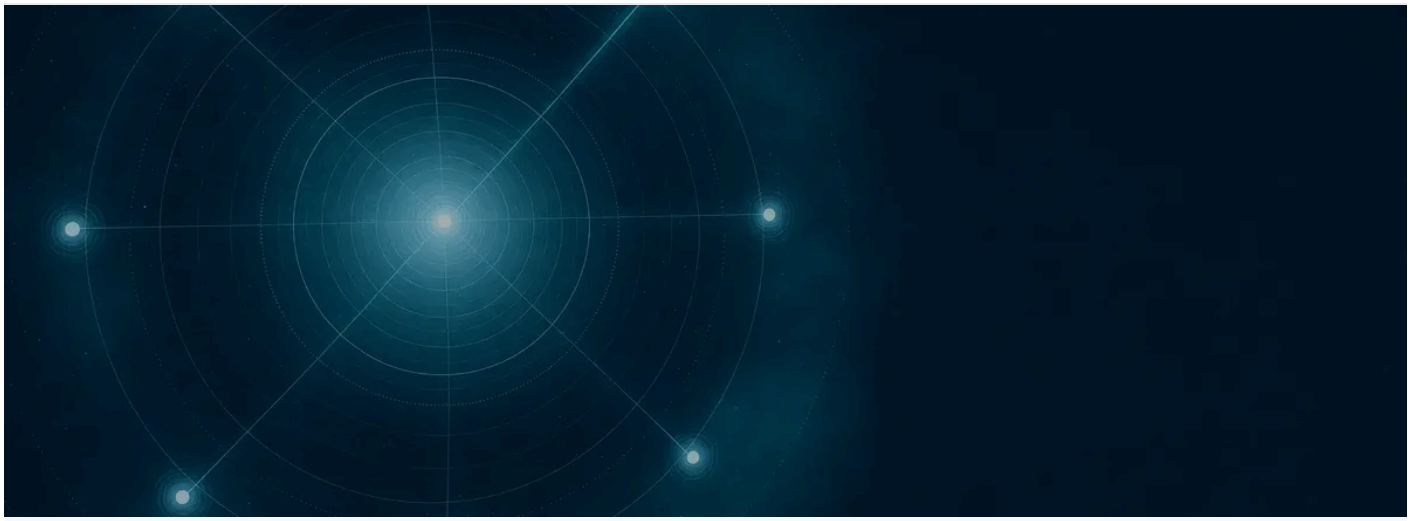

MDR Operations Playbook for SaaS

Erik Jones April 15, 2026

Executive Summary

Most SaaS companies discover they need **24/7 detection and response** after the first close call — a phishing attempt that almost worked, an exposed S3 bucket caught by a security researcher, a suspicious login from a developer's compromised laptop. By the time those signals reach a security team operating 9-to-5, dwell time is already measured in days. This playbook describes the operational discipline of running effective managed detection and response (MDR) for cloud-native SaaS — what to detect, who answers the page at 3 a.m., and how to make every detection event also satisfy a SOC 2 control requirement.

Why MDR Matters Now

The 2024 Verizon DBIR put median time-to-detection at **207 days** for organizations without dedicated 24/7 monitoring. For cloud-native SaaS, where customer data sits in S3 buckets, RDS instances, and SaaS subprocessors, that's the difference between an isolated incident and a regulatory disclosure obligation. Enterprise procurement teams now ask vendors for *"24/7 SOC coverage"* in vendor questionnaires; "we have logs" is not a satisfactory answer.

Most SaaS companies start with a hybrid model: AWS-native detection (GuardDuty, Security Hub, CloudTrail) feeding into a SIEM, with an in-house security team handling business-hours triage and a managed partner handling overnight and weekend coverage. The challenge is keeping the two halves of the rotation talking to each other.

Core MDR Discipline

Detection layer

Detection is built in three concentric circles:

> **Cloud-native services:** AWS GuardDuty for cloud-trail anomaly detection, Security Hub for unified findings, Inspector for vulnerability scanning, Macie for sensitive-data discovery.

Equivalent stacks on Azure (Defender for Cloud, Sentinel) and GCP (Security Command Center).

SIEM: Datadog Cloud SIEM for AWS-native operational simplicity, Splunk Cloud for organizations with existing Splunk investment, Elastic Security for self-hosted preference. Detection rules tuned to your application stack — generic rule libraries miss SaaS-specific attack patterns.

EDR: CrowdStrike Falcon, SentinelOne Singularity, or Microsoft Defender for Endpoint on the workforce side. Deployed through Jamf, Kandji, or Intune.

Response layer

Response wired into the same PagerDuty rotation that handles application reliability incidents. **One on-call rotation, two skill sets.** Pre-written runbooks for the high-frequency scenarios:

AWS account compromise (root credential exposure, IAM access key leak) — isolation playbook, credential rotation, forensic preservation

Endpoint compromise (malware, suspicious lateral movement) — EDR isolation, identity rotation, scope assessment

Data exfiltration alerts — packet capture, S3 access log review, customer notification timeline

Phishing-driven account takeover — Okta/Google Workspace audit, MFA reset, downstream system review

Practical Implementation

Tooling stack

A reasonable starting stack for a mid-stage SaaS:

SIEM: Datadog Cloud SIEM (~$2-4/host/month) with detection rules tuned to your AWS account hierarchy

Cloud detection: AWS GuardDuty (enabled across all regions), Security Hub aggregating findings, AWS Config for drift detection

EDR: CrowdStrike Falcon Insight ($8-15/endpoint/month) deployed through Jamf or Intune

Identity threat detection: Okta ITP, Microsoft Defender for Identity, or third-party IdP threat-detection

Response orchestration: PagerDuty for paging, Slack for collaboration, Atlassian Statuspage for customer communication

Coverage targets

Aim for **70%+ MITRE ATT&CK coverage** of techniques relevant to cloud-native SaaS — Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Exfiltration. 100% coverage is not the goal; some techniques are operationally infeasible to detect at acceptable false-positive rates. Document your coverage gaps explicitly so leadership can make risk decisions.

Common Pitfalls

Generic SOC vendor: A managed SOC that doesn't know your application can't tune rules. Findings come back as "unusual API call" with no context. Solution: pick a partner that operates your infrastructure, not just your alerts.

Alert fatigue: Untuned rules generate hundreds of low-quality alerts per day. On-call ignores or auto-closes; real signals get lost. Solution: monthly tuning reviews, target <5 high-fidelity alerts per day per rotation.

No threat hunting: Detection rules find what they're written to find. Threat hunting (hypothesis-driven investigation against MITRE ATT&CK) finds what rules missed. Skip it and you're blind to novel techniques.

Compliance evidence afterthought: Treating MDR as security-only and compliance-collection as a separate workstream doubles the effort. Solution: detection events feed directly into the SOC 2 / HIPAA evidence library.

Tabletop never run: An incident response runbook that has never been exercised is a hypothesis. Quarterly tabletop minimum; annual full live-fire exercise for high-trust customers.

Measured Outcomes

Programs we run typically deliver:

Sev-1 acknowledgement under 5 minutes via PagerDuty, 24/7/365

Median dwell time under 4 hours from initial detection to full containment

MTTR for sev-1 incidents under 60 minutes for routine compromises (account takeover, EDR endpoint isolation)

SOC 2 CC7.2/CC7.3 evidence package auto-generated from detection event data and incident records

Quarterly threat hunt reports documented against MITRE ATT&CK with coverage analysis

How Jacobian Helps

Our SREs and security engineers operate the same infrastructure they monitor — detection rules are written by the people who know your codebase, not by analysts reading runbooks for the first time during an incident. We integrate MDR with your existing PagerDuty rotation rather than running a separate vendor portal. And because Jacobian's roots are in audit and compliance work, every detection event lands in the SOC 2 / HIPAA control library automatically — monitoring as compliance evidence, not separate from it.

Resource Details

Author: Erik Jones

Published: April 15, 2026

Categories:

Security Operations SaaS

Download

Full Document

About This Resource

A practical playbook for SaaS companies running 24/7 managed detection and response operations — SOC integration, MITRE ATT&CK coverage, SIEM/EDR tooling, and continuous monitoring evidence that doubles as compliance evidence.

Categories:

Security Operations SaaS