

— CASE IN POINT | DATADOG + ONEZERO

Maturing Security Operations at oneZero Financial with RapDev's Managed SOC

Delivering ROI through 19 remediation tickets filed, 17 exposed repos surfaced, and zero successful credential attacks

Turning Cloud SIEM signal into weekly, tracked remediation

Challenge & Technical Solution	Business Impact
Tuned suppression rules to filter known-benign dev and backup tooling from the SIEM	28% of signals closed benign before reaching the client
Scanned GitHub weekly for disabled guardrails and leaked secrets, ticketing each case in Jira	17 exposed repos surfaced, 25 alerts triaged, zero leaked
Tracked every anonymous logon on legacy NTLMv1 hosts and ticketed the remediation weekly	7 consecutive reviews tracking hostile logons from 5 countries
Investigated every phishing and credential attack across five correlated log sources	5 hostile IPs and 1 phishing chain, zero compromise

"RapDev just comes in and becomes a part of the team. RapDev's implementation has helped make troubleshooting and getting to the bottom of incidents much, much faster."

— Alex Sullivan | SVP of Information Technology

