

SECURE

Managed SOC and MDR

Most security alerts arrive when your team is asleep.

Provate runs your security operations center for you. Our analysts investigate every alert, hunt for what your tools miss and contain threats under rules you agree in advance, day and night.

IN PRACTICE

24x7

The SOC, NOC and service desk we run as one team for a multi-site North American manufacturer.

THE PROBLEM

A security operations center needs people on every shift, including weekends and holidays. Then it needs detection engineers to keep the alerts meaningful and someone senior enough to make a call at 3 a.m. That team is hard to hire and harder to keep.

So most organizations settle for tools that raise alerts and a team that looks at them in the morning. Attackers know this, and plenty of intrusions are timed for nights and weekends.

WHAT CHANGES

01 Alerts are investigated the moment they fire, at any hour

02 Detections are tuned to your environment, so the noise drops month by month

03 Blocked threats are checked for related activity before anyone closes them

04 Security and IT outages share one escalation path if you add our NOC

05 Auditors get evidence that comes straight from daily operations

QUESTIONS TO ASK

Of any provider, including us.

01 Who looks at an alert at 3 a.m., and what are they allowed to do about it?

02 How often are detections tuned, and who decides what to change?

03 When a threat is blocked, does anyone check what else it touched?

WHAT'S INCLUDED

Detect

24x7 monitoring and triage
every alert, enriched with threat intelligence

Threat hunting

for behavior your tools haven't flagged

SIEM engineering

detections mapped to MITRE ATT&CK

Respond

Managed detection and response

containment you approve in advance

Incident response

including post-incident review

Phishing and credential exposure

mailbox clean-up and fast resets

Harden

Vulnerability management
prioritized by active exploitation

Penetration testing

including assumed-breach tests

IAM and compliance

access reviews and ISO 27001, SOC 2 and NIST CSF evidence

HOW IT RUNS

PHASE	WHAT HAPPENS	WHAT YOU GET
Assess	We review your environment, tools, current alert volume and escalation paths.	A list of coverage gaps and a transition plan
Transition	Runbooks are written with your team, and we run in parallel before taking over.	Agreed SLAs, contacts and escalation paths
Operate	Our team works your alerts and incidents around the clock.	Regular service reports
Improve	We tune, automate and clean up as we learn your environment.	Service reviews with trends and recommendations

CLIENT STORY

MANUFACTURING

One team for security and IT operations at a multi-site manufacturer

Security and IT operations were run separately across plant-floor and corporate IT. We took over the SOC, then added the service desk, NOC, identity and security engineering. Threats across endpoints, credentials, email and web are now triaged continuously, and the client's engineers no longer chase telecom carriers when a circuit drops.

“The proactive monitoring has made a real difference, allowing us to identify and address security threats before they impact production.”

Director of IT & Security

24x7

SOC, NOC and service desk

1

team in place of separate vendors

4

threat categories triaged continuously

NEXT STEP

Talk to our SOC lead.

+1 (512) 666-9422 • info@provate.net • provate.net

Usually delivered as Managed Services or Dedicated Services. Also available: Advisory & Consulting for assessments and penetration tests.

United States

7300 State Highway 121, Suite 300, McKinney, Texas 75070

India

5th Floor, Western Aqua, Hitech City Road, Kondapur, Hyderabad, Telangana 500081