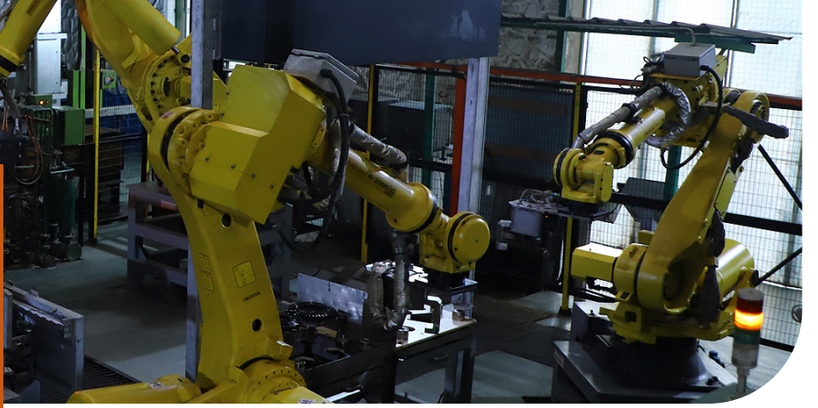
BRISK
TECHNOVISION LIMITED



Case Study SOC

Incident Response, IT Governance & Compliance Visibility Enhancement

Most cybersecurity conversations focus on the future future threats, future risks, future compliance requirements. But real security failures don't happen in the future. They happen in the present.

- A firewall rule that exists but isn't enforced.
- An alert that looks minor but exposes a hidden gap.
- Logs that seem available — until an audit asks the critical question.

This is where modern organizations struggle.

Security tools are deployed. Policies are defined.
Yet visibility, validation, and enforcement gaps quietly remain.

OVERVIEW

For a leading automotive manufacturing organization operating across multiple locations, cybersecurity required a centralized approach to monitor and validate security controls across sites

Through our **Managed SOC** approach, the focus moved beyond traditional alert monitoring to continuous validation of their real-world security posture.

Through our proactive approach, the **SOC team** uncovered critical gaps that would have otherwise remained unnoticed highlighting the difference between having security controls and having effective security governance.

SECURITY CHALLENGES

Like many growing **manufacturing enterprises**, the organization had siloed approach to security - involving firewall controls, endpoint protection, and audit control with policies.

On paper, the environment appeared secure.

However, during continuous monitoring and validation, we identified several hidden operational gaps:

- Security policies existed but enforcement was not always validated in real time.
- Limited visibility into administrative actions created governance blind spots.
- Compliance monitoring relied on multiple log sources .
- Independent oversight was required for stronger control validation.
- A growing multi-location environment increased the risk of unnoticed misconfigurations

These were not failures of security tools.

They were validation and governance gaps, the most common reason incidents occur despite technology investments.

By acting as an independent security layer, we continuously verified whether controls were functioning as intended — not just configured.

This proactive validation led to the identification of critical gaps, two of which are listed below.

> The controls were deployed. The policies were defined.
> But only continuous validation revealed what was silently missing

Case 1:

Incident Response & Firewall Enforcement Remediation

Situation

A real-time alert from our deploy SIEM tool identified outbound traffic to a website listed in the global threat intelligence feed.

Although the website was configured to be blocked in the firewall, it remained accessible from the endpoint.

- **Root Cause**
- Firewall block rule existed in configuration.
- Rule was not properly enforced in active policy set.
- Traffic was not effectively blocked due to enforcement gap.
- This was a governance and validation issue not a tool failure.

Managed SOC Action

1. Detection & Validation
   - Alert validated at endpoint level
   - Confirmed legitimate access to blacklisted site
2. Escalation & Coordination
   - Escalated to Firewall Team
   - Coordinated with Client IT Team
   - Reviewed enforcement status
3. Remediation
   - Firewall policy corrected and enforced
   - Configuration validated with OEM to verify if any existing vulnerabilities
4. Post-Fix Validation
   - SOC re-tested endpoint
   - Confirmed site successfully blocked
   - Continuous monitoring enabled

Business Impact

- Hidden firewall enforcement gap identified
- Potential malware exposure prevented
- Strengthened firewall governance
- Zero operational disruption
- No data compromise observed

Case 2:

Compliance & SIEM Log Visibility Enhancement

Situation

During routine monitoring, SOC identified incomplete log visibility from Endpoint Security tool integrated with SIEM.

Logs Missing:

- Admin login activities
- Policy modifications
- Configuration changes
- Console-level actions

Logs Received:

- Website access logs
- USB activity
- Endpoint security events

Risk Identified

- Incomplete audit trail
- Compliance visibility gap
- No tracking of administrative changes
- Governance accountability risk

SOC Recommendation

Upgrade Endpoint Security tool version in order to:

1. Enhanced administrative logging
2. Complete audit trail visibility
3. Improved compliance readiness
4. Better SIEM integration

Business Impact

- Proactive compliance gap identification
- Strengthened audit posture
- Improved governance transparency
- Enhanced SOC monitoring effectiveness

Key Outcomes

Through Managed SOC services, the organization achieved:

- 24/7 proactive threat detection
- Policy enforcement validation
- Compliance visibility improvement
- Visibility into real world security posture
- Improved overall cyber resilience

Conclusion

This combined case demonstrates that Managed SOC is not just about alerts it ensures:

- Continuous validation of security controls
- Enforcement of firewall policies
- Compliance audit visibility
- Cross-team coordination
- Independent security oversight
- A proactive approach that prevents incidents before they escalate.

If your organization's security posture hasn't been independently assessed, you may be relying on assumptions instead of real protection.
Let's verify your security posture today.

enquiry@brisk-india.com
+91 -9594713513
brisktechnovision.com