HAVE YOU OUTGROWN YOUR SOC?

A practical self-assessment for organizations that need security operations aligned to business priorities, critical operations and real-world risk.

Most organizations already have security monitoring, alerts and reporting. The challenge is rarely a lack of information. More often, the challenge is understanding which risks matter most, how they affect critical operations and what actions should be prioritized first.

Organizations operating critical infrastructure often manage interconnected IT and OT environments, complex operational dependencies and increasing regulatory requirements. In these environments, cyber incidents can affect more than information systems. They can impact safety, availability, operational continuity and essential services.

This self-assessment is designed to help you reflect on how well your current Security Operations Centre (SOC) supports your organization's operational reality, business priorities and risk management objectives.

Rather than producing a maturity score, the assessment highlights potential strengths and gaps across five key areas. Areas with multiple Partly agree or Disagree / not sure responses may indicate opportunities for further review and discussion.

How to use the assessment

Answer each statement honestly. Then review the pattern of responses within each category. There are no right or wrong answers. The goal is to identify areas where your security operations are well aligned and areas where further review, discussion or improvement may be beneficial.

ASSESSMENT OVERVIEW

Area	Core question	What it tests
Prioritization	Are you getting clarity or just alerts?	Whether the SOC manages alert volumes and focuses attention on the events that present the greatest risk.
Context	Does your SOC provide meaningful context about your operations?	Whether SOC outputs reflect IT, OT, critical assets, dependencies and operational reality.
Decision support	Does your SOC support better decisions?	Whether SOC insights support risk-based operational, security and management decisions.
Continuous improvement	Is your SOC improving your security position over time?	Whether the SOC contributes to reducing exposure and improving security over time.
Governance and collaboration	Does your SOC work as an integrated part of your organization?	Whether roles, escalation paths, ownership and collaboration are clear.

1. PRIORITIZATION

Are you getting clarity or just alerts?

Use these questions to assess whether your SOC helps the organization cut through alert volumes and focus attention where business or operational risk is greatest.

	Assessment statement	Agree	Partly agree	Disagree / not sure
1	Our SOC helps us prioritize the security events that present the greatest risk to operations.	☐	☐	☐
2	Alerts are prioritized based on business impact, not technical severity alone.	☐	☐	☐
3	We know which assets, systems or operational processes require immediate attention.	☐	☐	☐
4	We spend limited time reviewing alerts that do not lead to meaningful action.	☐	☐	☐
5	Our SOC helps us focus internal resources where risk is greatest.	☐	☐	☐

Category indicator

If several statements are marked Partly agree or Disagree / not sure, the indicator is likely alert noise, inconsistent prioritization or unclear focus on business-critical risks.

What effective security operations look like

Effective security operations help teams focus on the threats and exposures that matter most Alerts are prioritized according to business impact, critical assets and operational consequences, helping internal teams spend less time on noise and more time addressing meaningful risk.

2. CONTEXT

Does your SOC provide meaningful business and operational context?

Use these questions to assess whether SOC outputs reflect your IT, OT, operational dependencies, critical assets, regulatory obligations and business reality.

	Assessment statement	Agree	Partly agree	Disagree / not sure
1	Security events are prioritized based on our critical assets, systems and operational dependencies.	☐	☐	☐
2	Security events are explained in the context of our critical assets and business priorities.	☐	☐	☐
3	Recommendations reflect our business, regulatory and operational realities.	☐	☐	☐
4	Security events are assessed in the context of their potential impact on critical operations, production or service delivery.	☐	☐	☐
5	We do not need significant internal reinterpretation before action can be taken.	☐	☐	☐

Category indicator

If several statements are marked Partly agree or Disagree / not sure, the indicator is likely missing context or a gap between security operations and the operational reality of the organization.

What effective security operations look like

Effective security operations connect security events to what matters most: critical assets, operational dependencies, business priorities and regulatory obligations. Security events are assessed and communicated in terms of potential business and operational impact, not technical severity alone.

3. DECISION SUPPORT

Does your SOC support better decisions?

Use these questions to assess whether SOC reporting and insights help security, operational and management stakeholders make clearer risk-based decisions.

	Assessment statement	Agree	Partly agree	Disagree / not sure
1	SOC reporting supports operational, security and management decision-making.	☐	☐	☐
2	SOC insights make it clear which risks require attention first.	☐	☐	☐
3	SOC insights help us discuss priorities and risk ownership across the organization.	☐	☐	☐
4	We can clearly explain cyber risk and priorities to business stakeholders.	☐	☐	☐
5	Our SOC provides information that supports governance and investment decisions.	☐	☐	☐

Category indicator

If several statements are marked Partly agree or Disagree / not sure, the indicator is likely that the SOC provides information, but not enough decision support or business relevance.

What effective security operations look like

Effective security operations provide insights that support decisions at operational, security and management levels. Reporting gives stakeholders a clear view of risks, priorities and recommended actions, not simply what activity has occurred.

4. CONTINUOUS IMPROVEMENT

Is your SOC improving your security position over time?

Use these questions to assess whether your SOC contributes to reducing exposure and improving security operations over time, rather than only reacting to alerts and incidents.

	Assessment statement	Agree	Partly agree	Disagree / not sure
1	Our SOC contributes to exposure reduction before incidents occur.	☐	☐	☐
2	Recommendations are practical, prioritized and followed up over time.	☐	☐	☐
3	The SOC helps us address root causes, not only individual alerts.	☐	☐	☐
4	Security operations evolve as our business, threat landscape and operating environment change.	☐	☐	☐
5	We have a clear view of which improvements have been implemented and what remains open.	☐	☐	☐

Category indicator

If several statements are marked Partly agree or Disagree / not sure, the indicator is likely limited follow-up, weak improvement loops or a reactive operating model.

What effective security operations look like

Effective security operations contribute to reducing risk over time. Lessons learned, recommendations and improvement activities are tracked, prioritized and integrated into the organization's evolving security posture.

5. GOVERNANCE AND COLLABORATION

Does your SOC work as an integrated part of your organization**?**

Use these questions to assess whether the SOC is integrated into roles, escalation paths, governance discussions and shared risk ownership across the organization.

	Assessment statement	Agree	Partly agree	Disagree / not sure
1	Roles, responsibilities and escalation routes are clear between our teams and the SOC.	☐	☐	☐
2	Security, IT, OT and business stakeholders share a common view of priorities and responsibilities.	☐	☐	☐
3	Governance meetings focus on risk, exposure, business impact and improvement, not only service performance.	☐	☐	☐
4	Appropriate stakeholders are involved quickly when security events require action.	☐	☐	☐
5	Collaboration reduces pressure on internal teams rather than creating more follow-up work.	☐	☐	☐

Category indicator

If several statements are marked Partly agree or Disagree / not sure, the indicator is likely an operating-model gap: unclear ownership, weak governance or collaboration that creates additional work for internal teams.

What effective security operations look like

Effective security operations operate as an extension of the organization rather than a standalone service. Roles, responsibilities, communication paths and governance processes are clear, enabling effective collaboration and shared ownership of risk.

NEXT STEPS

Use the patterns from this self-assessment to identify where your current SOC setup is working well and where further review may be valuable.

- Validate your current SOC setup.
- Identify gaps and improvement areas by category.
- Define practical next steps to improve prioritization, context, decision support, continuous improvement and governance.
- Explore whether a SOC maturity or scoping conversation would help clarify the right operating model.

Your risks are not generic. Your SOC shouldn't be either.

https://www.dnv.com/cyber/