Checklist for an Effective Security Operation

Use this checklist of best practices to define an effective security operation, whether you're building your own or evaluating a potential partner.

---

01. Broad Visibility

Your security operation can only measure, and protect, what it can see. Ensure that your security operator or managed SOC provider can make sense of your environment and the technologies that your organization relies on.

- ☑ Data ingest is flexible and includes all sensitive assets. It should also be adaptable to new technologies and security tooling as protection evolves.
- ☑ Monitoring, enrichment, and advanced correlations must span data sources to ensure the most effective and accurate coverage.
- ☑ Security operations technology deployment is available on-premises and in the cloud. Your security must support your architecture.

02. Tailored Threat Intelligence

It's critical that your operation or provider is continually identifying and applying new intelligence to your protection strategy.

- ☑ Threat intelligence is gathered, understood, and integrated on a continuous basis.
- ☑ Data gathering includes less traditional sources, such as active threat hunting and dark web scanning for your private information.
- ☑ Attack simulation results are included. This can be the only means of surfacing bespoke threats where custom software is present.

03. Available Expertise

The breadth of your security operation must be matched by the breadth and availability of skilled personnel. Whether you plan to evolve internal capabilities or gain more expertise with a partner, having the right level and readiness of expertise is critical.

- ☑ Leaders, analysts, and operators must possess a demonstrable breadth of experience across all critical areas of the protected environment.
- ☑ Staffing is sufficient to handle periods of high traffic or the potential for a widespread event.
- ☑ In-house teams can quickly scale to augment during periods of business growth, reorganization, and changing priorities.

04. Communications Cadence and Competence

The difference between an effective security operation and a dysfunctional one is communication. Your operation or partner needs to have clear communication expectations.

- ☑ Communication of security activity, progress, and vision is in business terms, language that non-security, non-technical people can understand.
- ☑ Security reporting is consistent, comprehensive, credible, and relevant to the audiences involved.
- ☑ Security operators are available, and able, to answer direct questions from a variety of stakeholders.

Looking for help building an effective security operation?

Visit www.nuharborsecurity.com to learn more.

NuHarbor SECURITY