Nemertes

Better data. Better decisions.

The Journey to MDR and Managed SOC

Leverage expertise, ease the talent crunch, improve cybersecurity

By John Burke, CTO

Nemertes

May 2024

Table of Contents

1. XDR is Crucial…and Hard

Extended Detection and Response (XDR) solutions aim to complete the journey begun decades ago with the creation of log management systems. Log managers were the first class of product intended to provide a clearinghouse for logging information across systems, so IT and cybersecurity teams could go to one place for the information instead of dozens. Log managers evolved into SIEM systems – Security Incident and Event Managers. SIEM layers onto log management more sophisticated analysis of the log data, with the goal of helping cybersecurity teams more quickly and consistently detect cybersecurity events so they can then contain threats. SIEM systems also provide reporting capabilities, often with preconfigured reports conforming to the requirements of specific regulatory or compliance regimes, like PCI-DSS or HIPAA.

After SIEM came a more focused and still more sophisticated type of tool: endpoint detection and response (EDR). EDR systems brought the logic of SIEM to the systems to which SIEM was generally not applied: enterprise endpoints. Collecting data from endpoint protection platforms (themselves the descendants of the antivirus software of decades past), EDR systems use endpoints as a far-flung network of cybersecurity sensors, sensitive to the anomalous behaviors that indicate an attack in progress. And the "R" is important: EDR platforms provide the means not just of detecting but of responding to attacks, e.g., by requesting more data on processes being executed on the endpoint, or isolating a compromised PC by turning off its network interface, or simply shutting it down.

Evolving up from such roots, XDR ties together all the threads of monitoring, event assessment, and response. An XDR system can pull log data from endpoints, security systems like firewalls, and network devices and controllers, as well as from servers and applications, can ingest configuration files and non-log data from other sources; and do so across sites, data centers, and clouds. It applies analytics across data streams to search for patterns that older forms of log analysis would miss, and can leverage a broader array of responses, since its reach is not limited to the endpoints.

XDR is essential to the evolving enterprise cybersecurity environment. But, deploying it is not simple or easy. In any enterprise cybersecurity environment there will be all those aforementioned data sources to monitor. And, crucially, in a typical environment, there will be a steady churn in the list of applications feeding in, the services/systems/data being protected and the risks they are being protected from, as well as in the policies the overall environment is managed against, and the regulations it must comply with. Implementing XDR is complicated; maintaining it is a huge investment of time and energy. Many organizations deploying XDR never get very far down the road—they don't apply it to all the systems they should—so they get less value from the analytics features. Many also don't leverage automated responses beyond further data acquisition.

2. Make XDR Manageable By Making It Managed

Managed detection and response (MDR) is a natural solution to the challenges of deploying XDR: outsourcing as much operational complexity as possible.

As the first line of response and investigation, MDR solutions can vastly reduce the number of events that in-house cybersecurity teams must respond to, while making sure those teams have solid information to work with on unfolding security incidents. MDR providers can also implement quick initial responses to limit potential harms.

MDR providers can also take on the burdens of adding, maintaining, and dropping integrations, for example, as well as being responsible for maintenance of the XDR platform itself. A good MDR provider will have experience generating reports for auditors and regulating agencies.

Taking advantage of MDR for low-level XDR maintenance, routine monitoring, and initial response mechanics, in-house cybersecurity staff can focus elsewhere. They can improve both policy development and policy implementation. They can devote more time to preventing incidents through full implementation of key cybersecurity strategies like zero trust. They can devote more time to security assessments of new applications and platforms and secure the configuration and deployment of them. And, internal cybersecurity response and operations teams can focus more fully on robust incident response and resolution, since the MDR provider is still performing normal monitoring in the background.

3. Outsourcing the SOC

Having gone this far in outsourcing monitoring, maintenance, and initial response, fully outsourcing security operations is a natural next step. Cybersecurity teams that establish a comfort level with handing off these duties via MDR, and learn to integrate the efforts of internal staff with service provider staff, can see their way clear to handing off more. They also have experience integrating external providers and services into their policies and processes.

With the goal of both improving security outcomes and making the best use of in-house resources, a managed SOC is a sensible option. MDR is not the only stepping stone, of course; there are multiple paths to this destination. For example, cybersecurity leaders might decide they can jump right from XDR to a managed SOC that includes MDR services, or even decide that implementing XDR at all is better handled as part of a SOC outsourcing arrangement.

In Nemertes’ 2024-25 Network and Security Operations research study, all of the organizations most successful in cybersecurity have an outsourced SOC.

3.1 Mitigating Staffing Challenges

The scope and complexity of the SOC expand as the enterprise’s IT environments do. This means SOCs always need more (and more experienced) staff. Unfortunately, SOC teams (as with cybersecurity generally) must deal with high rates of staff turnover. New staff are constantly being trained, diverting the attentions of more senior staff from actual

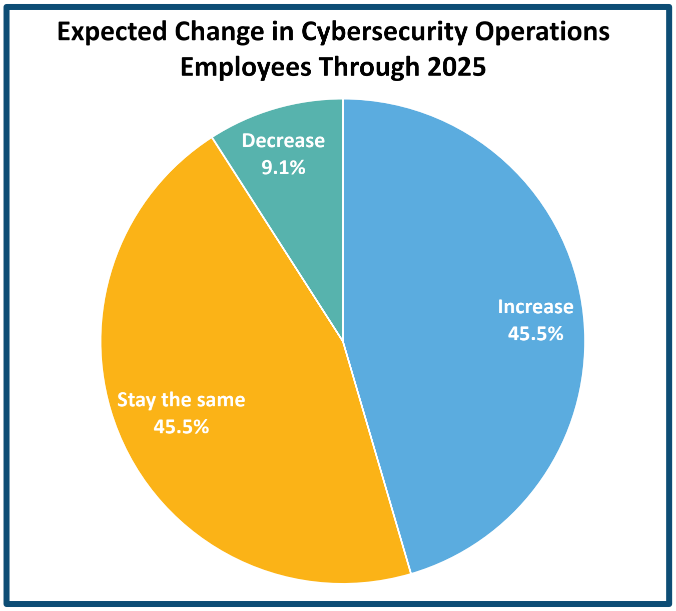

Figure 1: Cybersecurity Operations Teams Growing

security work. More experienced staff leave, taking their higher level of expertise and their familiarity with the environment with them.

In outsourcing the SOC, cybersecurity leaders reduce their need to be constantly hiring staff in a tight cybersecurity labor market—another distraction from actual security work. They also shift to the provider the burden of keeping SOC staff appropriately trained, and of retaining skilled staff.

3.2 Shifting Costs

Enterprises are still engaged in shifting IT spending from capex to opex, mirroring their ongoing shift of workloads into various cloud solutions.

Outsourcing is another way of shifting spending, in this case payroll dollars, into parts of the operating budget that the organization can more easily adjust as conditions change. Having staff on the payroll carries all the added overhead of a benefits package, associated benefits management, and the costs of recruiting and onboarding and training in new staff and there is a lot of hiring, whether to expand cybersecurity operations teams or to replace staff that leave. With nearly half of organizations expecting to increase security operations staffing by 2026 (see Figure 1), outsourcing may become more appealing.

3.3 Leveraging Partner Scale and Scope

A SOC provider will have scale most organizations can't (or choose not to) match.

They can have a deeper bench of experts to bring to bear in a crisis, beyond the ones that normally work on day-to-day operations for any given client. They can also typically manage to have both experts in more distinct areas of cybersecurity and more cross-training amongst staff.

An enterprise is also likely to be able to find a SOC provider with staff holding whatever relevant technology-, vendor-, practice-, or industry-specific certifications their environment dictates, be it a CISSP or a Cloud Security Alliance Certificate of Cloud Auditing Knowledge or a GIAC Security Operations Certificate. SOC providers are also likely to have an array of organizational-level certifications (ISO 27001, for example) and to be familiar with multiple cybersecurity frameworks such as those from NIST and MITRE.

And, a SOC provider can maintain more SOC facilities, and larger ones, than any one client could or would, spreading work across geographies and time zones to provide the best possible support match for a customer's staff and facilities wherever they are.

3.4 Buying Agility

Outsourcing the SOC makes it easier to make major changes in SOC services going forward, should needs change radically. It is easier to shift from one outsourcer to another than to swap out or retrain the internal staff wholesale, while also retooling and rewriting processes. It is easier to scale up a relationship, or add a vendor, than to double or triple the size of an internal SOC in the face of a major acquisition. It is similarly easier to add outsourced coverage in new geographies.

Finally, outsourcing the SOC insulates it from radical changes in the internal cybersecurity organization. It will continue operating serenely no matter what kind of re-org or change in leadership happens within the organization. That is, the internal organization gains a degree of organizational agility by decreasing the inertial mass of the organization: it is easier to change course in a lighter ship.

3.5 Not All Or Nothing

Of course, outsourcing doesn't have to be all or nothing. In Nemertes' 2024-25 Network and Security Operations research study, a third of the organizations most successful in cybersecurity have an internal SOC as well as an outsourced one.

Partial outsourcing allows a strategic separation of duties between an internal SOC and an external one. For example, an internal SOC might focus solely on core customer-facing systems at an e-tailer, while an outsourced SOC watches over everything else. Or, an internal SOC might cover operations in the continental US, with an outsourced SOC for operations in other geographies.

3.6 Focusing on Strategy and Prevention

In most organizations, cybersecurity staff working on operations have to divide their attention between that work and other duties. (Scarce, expensive) cybersecurity architects and engineers are putting on an operations hat as needed, to help identify and respond to incidents. Cybersecurity operations staff are sidetracked into non-operations work such as code reviews, or writing documentation, or helping to vet applications for potential deployment.

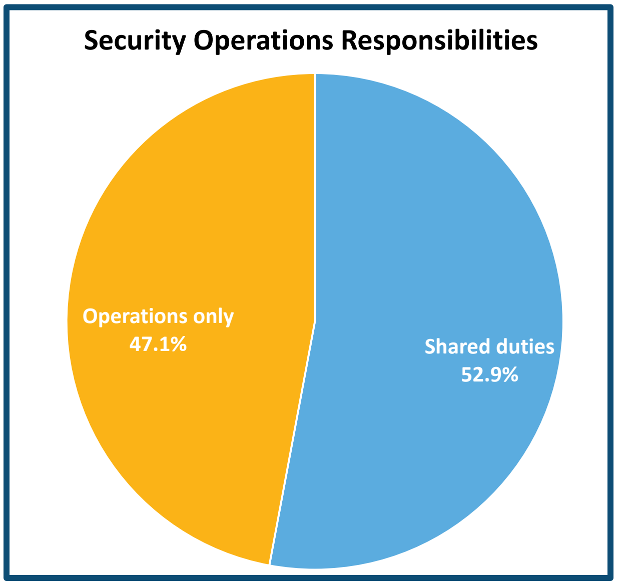

Figure 2: Most SecOps Teams Divide Their Attention

Cybersecurity leaders, in adopting an outsourced SOC, create a clear dividing line between the operations staff and in-house engineering and architecture teams. This allows in-house staff to focus on more strategic efforts, which too often get short shrift when there is no clean division, because the urgent demands of incident identification and response take precedence. These efforts include refining cybersecurity policies in the aftermath of both actual incidents and well-run tabletop exercises; updating cybersecurity architectures as the application portfolio and hosting environments evolve; and improving baseline practices across the organization to boost the overall security posture. By focusing in-house staff on prevention of cybersecurity incidents rather than detection and response, an organization can mature from being mainly reactive in cybersecurity to being more anticipatory.

4. Conclusion and Checklist: What to Seek in a SOC Partner

A managed SOC is a natural next step for anyone engaging MDR, and an important option for anyone contemplating the challenges of creating and maintain a proper SOC. Cybersecurity professionals and IT leaders should be examining their current SOC strategy and ambitions and assessing the ways in which an outsourced SOC might better achieve their organizational risk and cybersecurity goals.

Here are some common criteria that should be on every organization's SOC-provider shopping list:

- **Expertise and Breadth of Experience:** The provider will have some history serving the security needs of companies your size, ideally of your configuration (similar mixes of on-premises and remote work, similar geographic footprint, for example), especially (but not exclusively) in your industry.
- **People:** Provider staff should all be well-trained, including possessing relevant cybersecurity certifications. Provider should also have an established practice of pairing newer staff with seasoned professionals as mentors. Look for a solid mix of experience levels in the staff.
- **Process:** Provider processes should be rock solid around incident identification and response, and the provider should always be refining them in the wake of incidents, red-teaming exercises, and table-top wargaming, whether with you (your incidents etc.) or with other customers.
- **Technology:** Providers should have a portfolio of rock-solid cybersecurity and incident management tooling that is up to date and kept that way. At a minimum, they should have a robust XDR platform service as their primary detection and initial response platform; more traditional SIEM functionality—even if not wrapped up in the XDR—for reporting and auditing; and SOAR tools to supplement the automation capabilities of the XDR package. Furthermore, SOC providers should be incorporating the best of AI-powered analytics and automation into their toolset to improve false-positive rates and speed incident responses.
- **Speed and Scale:** To meet an organization's cybersecurity needs, the SOC provider should have scale to match the scale of its needs, both now and anticipating how needs will grow as the organization grows. It should have geographic reach to match all the geographies the organization operates in—and plans to grow into—and 24/7/365 coverage that is responsive both to emergent situations and to the organization. Working with a provider should lead to the organization having faster incident resolutions, faster after-action reviews, and faster improvements to protections and processes.
- **Flexibility:** To integrate a new SOC provider into its operations, an organization should seek a provider with a well-defined process for accomplishing that goal. The provider should have a repeatable, well-practiced ability to adapt and integrate with the organization's in-house cybersecurity teams, its internal SOC if it has one, and its NOC, whether in-house or also outsourced. And although it should have its own core technology portfolio, the provider should also have some flexibility on tools, to smoothly integrate with an organization's own toolsets.

About Nemertes: Nemertes is a research-based advisory and consulting firm that analyzes the business value of emerging technologies. Since 2002, we have provided strategic, client-centric recommendations based on data-driven operational and business metrics to help organizations deliver successful technology transformation to employees and customers. Simply put: Nemertes' better data helps clients make better decisions.