Whitepaper

Deep and Lasting Cyber Defense Requires Transformation

Most organizations understand that true cyber defense isn't just about executing tasks; it's about orchestrating a program that evolves alongside the sea of threats lurking below the surface. At the heart of this belief is a fundamental understanding: If you're not actively transforming, you're inevitably falling behind.

Despite this general acknowledgement, organizations often find themselves in the latter situation, operating within a program that lacks the depth and cohesion needed to always keep networks and digital assets safe. In other words, their security operations center – if the organization is fortunate enough to even have one – spends most of their time drowning in alerts.

> "We know threat actors are continually adjusting and changing. We need to as well,"

said Wade Alt, Chief Operating Officer at DeepSeas, a global cybersecurity company that offers advanced threat detection and response solutions. Its employee-inspired name refers to the depth of talent, tradecraft, and technology that empowers its experts to delve deep into complex domains and industries to achieve clarity and calmness like serene deep ocean environments.

Going deeper than traditional threat detection and response

DeepSeas distinguishes itself from other cybersecurity vendors through its focus on a unique service delivery methodology. This approach prioritizes personalization, reliability, transparency, and cost-effectiveness by first working with a client's existing security controls and then enhancing from there. Its crew of cyber defense experts has served in the U.S. intelligence community, Fortune 500 cyber defense teams, and world-class enterprise security consulting firms.

With the rise in cyber threats, the persistent cybersecurity skills gap, and government regulations, mid-sized organizations and enterprises alike are turning to DeepSeas to transform their cyber defense programs.

To demonstrate how the DeepSeas programmatic approach to transformation works, Alt walked through a client engagement with an organization that had only partially implemented a security operations center (SOC) due to higher-priority business goals. When the company was ready to transform its security operations, it recognized the need for outside help.

When DeepSeas began working with this client, it helped identify critical areas in need of improvement, including the following:

- A global environment with limited visibility and endpoint deployment
- Hampered detection and response due to limited threat hunting capabilities
- An incomplete tech stack with partial deployments and key technology integration missing
- A heavy reliance on incident response retainers for remediation, regardless of severity
- Ad hoc processes with minimal intrateam interaction among a loosely federated group

“Our approach wasn't about instant fixes or quick wins; it was about laying the foundation for continuous improvement,” Alt explained. “From day one, our focus was on leveraging tailored intelligence, deploying detection use cases, and collaborating closely with our client to prioritize enhancements.”

The solutions from DeepSeas used to accelerate transformation included the following services.

- **Managed Detection & Response (DeepSeas MDR+)** monitors client networks and endpoints for suspicious activity; analyzes potential threats; and then takes action to contain and neutralize them 24x7x365.

- **Penetration testing from DeepSeas RED** simulates cyber attacks to identify weaknesses in a client's defenses. This helps organizations understand their vulnerabilities and prioritize remediation efforts.

Over the course of three years, a DeepSeas crew helped the client create a solid, sustainable cyber defense program that surpassed industry standards. Alt explained, “We knew from the start that this was going to be a transformative program where we were constantly improving and adjusting.”

DeepSeas kicked off the process of cyber defense transformation by boosting the power and efficiency of the client’s current security tools and leveraging threat intelligence tailored to the organization’s industry. Then, a crew from DeepSeas worked with the company to locate and eliminate IT security blind spots before enhancing capabilities tied to risk and compliance. This immediate improvement carried through for the next 12 months as cyber operations and scalable platforms were built specifically for the client’s business and industry.

Alt noted that the DeepSeas cyber professionals involved key stakeholders from the client’s team as needed and, once a solid foundation was established, implemented “attack surface reduction activities.” Within a year, the client had a proactive, intelligence-driven cyber defense program that both automated necessary threat activities and integrated with the business overall.

> “It’s amazing what you can do in a year if you’ve set out to achieve that mission upfront,”
>
> Alt said of the initial success.

Once the groundwork was done, the focus shifted to introducing additional capabilities to stay ahead of threats and remain in compliance. Additionally, the cyber program needed to remain tightly aligned with business demands, which are always subject to change.

“Where we are today, we don’t expect to be tomorrow. We think that realization is really important for any cyber program,” Alt said.

Creating immediate uplift with the tools on hand

Though any cyber journey takes time to gain traction, DeepSeas rapidly deployed a series of curated and vetted use cases to boost threat detection across the client's IT infrastructure. By supplementing personnel and optimizing tools the client's security team had on hand, DeepSeas was able to create an immediate uplift in the organization's cyber capabilities.

This immediate result was only achieved because DeepSeas has a deep bench of experts along with detections and analytics drawn from actively combating threats daily for its global client base. In this case, the client organization improved its cybersecurity posture by maximizing its current technology investments, rather than requiring a rip-and-replace strategy.

While DeepSeas experts have strong professional opinions about certain technologies, they prioritize understanding each customer's unique business needs and accommodating their current tooling, even in greenfield scenarios where no prior tools exist. The security vendor provides expert guidance on tool selection based on the customer's priorities, industry, size, and other key factors, as different tools offer varying capabilities better suited for different use cases.

Connecting Organization-Wide Objectives to Cybersecurity Transformation

A key challenge that most companies face is an inundation of security data generated from various threat detection solutions. Security teams need a way to synthesize and prioritize this flood of data into a hierarchy of threats, allowing cybersecurity professionals time to focus on their organization's objectives. This integration of security operations with organizational objectives ideally happens via collaborative processes like playbook creation and tabletop exercises. That said, it instead is sometimes a forced function during real-time incident response situations.

The experts at DeepSeas understand the need to bridge organization-wide objectives with cybersecurity transformation. That's why one of the first steps a DeepSeas crew will take with a new client is to learn about the organization's existing capabilities in areas like forensics, intelligence, and incident response. Placing that knowledge in an organization-wide context then allows DeepSeas to make sense of the data signals across the client's systems.

"Our approach centers on tailoring our recommendations to align with the customer's specific requirements rather than forcing a one-size-fits-all solution," Alt said.

Every SOC is different

Alt explained a transformational cyber program accommodates a client's unique needs and cyber maturity level.

"We have not run into a situation where the SOC has been properly staffed and resourced – where there wasn't any need no matter how big or small the company is," he said. "We walk in with an assumption that they already have some sort of capability. We need to make them as efficient and effective as possible."

Some clients need DeepSeas to integrate with their fully functioning internal team, where the DeepSeas crew plays a supportive role as needed. Others leverage DeepSeas as their full security operations center.

“There’s going to be some nuance, some difference that you’re going to need to adjust to and accommodate. It’s incumbent on us to do the adjusting, not the client. I think that’s really important and something that we embrace.”

The Power of Personalized Innovation

A one-size-does-not-fit-all mantra is not just a catchy phrase at DeepSeas. Rather, it is a fundamental principle guiding the next generation of security solutions providers, including those in Managed Detection & Response.

Departing from the conventional approach of delivering standardized solutions to every organization, the DeepSeas approach to personalized innovation is revolutionizing the industry in several key ways:

- DeepSeas crew members are trained to tailor, integrate, and emphasize the uniqueness of each client's organization, environment, operations, and security posture.
- Rather than imposing a uniform set of procedures, DeepSeas prioritizes collaboration and personalization, leveraging the client's own resources and expertise.
- By embracing this client-centric ethos, DeepSeas not only enhances security efficacy but also fosters a symbiotic partnership where threat prioritization aligns with individual risk profiles, and playbook creation becomes a collaborative endeavor.

  This holistic approach signifies a paradigm shift towards agility, adaptability, and effectiveness, dispelling the notion that one size fits all in the realm of cybersecurity.

In essence, the unique focus of DeepSeas is on adapting to each client's distinct environment, integrating their team's knowledge of challenges specific to the organization, prioritizing those challenges based on risks, and collaboratively developing processes. They support the idea that effective transformation must be significantly customized to achieve the outcomes their clients desire.