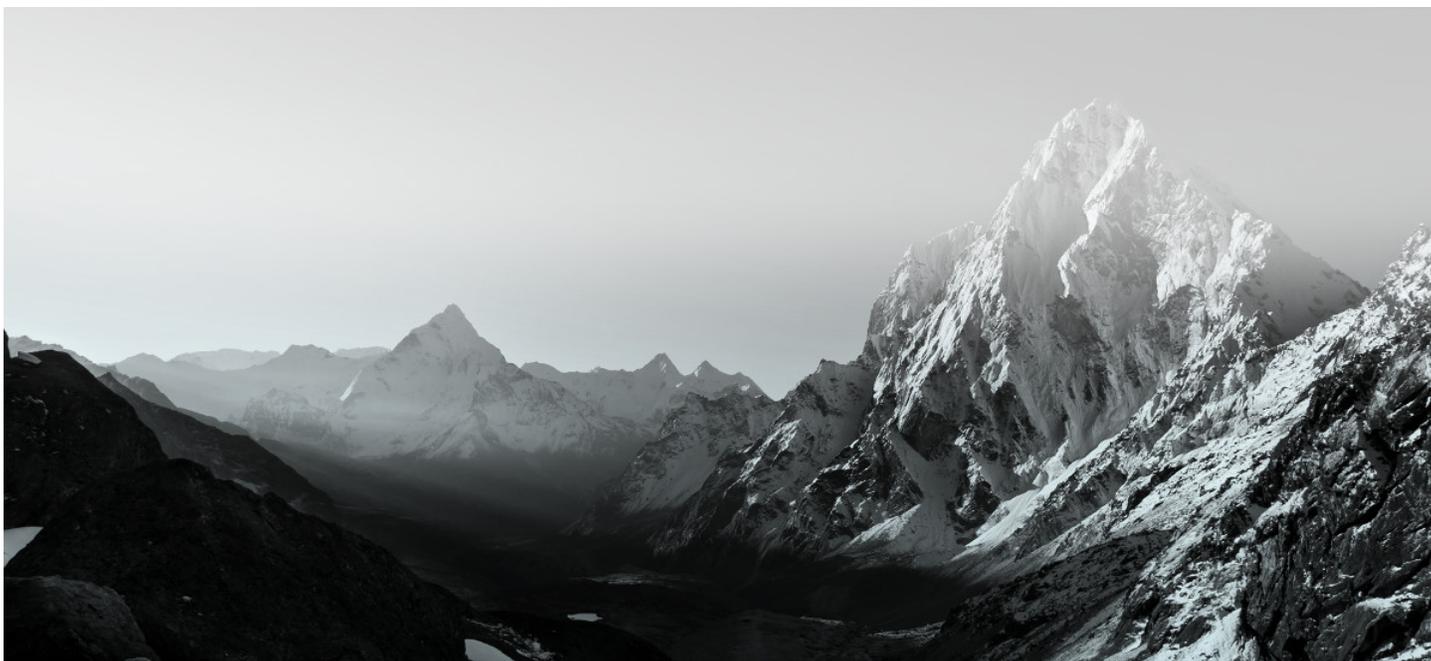


Retained Incident Response and Forensics



Retained Incident Response and Forensics

Incident response is an area that often strains organizations; having just suffered a security incident, your organization is now called upon to carry out a variety of critical tasks to limit its impact, recover from any damage, and prevent a recurrence, all of which must be executed on an aggressive timetable and while maintaining the rest of your business. Leviathan is able to assist this process by evaluating your capabilities, by providing tools, training, and process improvements to aid your staff, and by serving either as extra capacity for your security program during an incident, or as a primary resource for security response. We believe that the process should reflect your organization's needs and priorities, and so at each step, we will work with your staff to make sure that the plan's priorities align with yours.

Initial Assessment

Leviathan tailors security and incident response to your organization; this allows your particular needs and areas of greatest concern to drive the process. It is therefore critical that, to begin, we obtain an understanding of your culture, business drivers, and organizational constraints, along with your current investments. Assessing your current state of readiness to detect, respond to, and recover from an incident allows us to leverage and improve your existing capabilities, rather than enforcing an off-the-shelf methodology which may not be appropriate.

Process, Tools, and Training

We develop a set of process improvements and additions, consistent with industry best practices, which will enhance your security practice generally while also being useful in the context of your organization

EXAMPLE CLIENT:

STARTUP TECH ORGANIZATION

This successful startup needs to build an initial incident response capability to preserve its core business in the face of a security breach. Leviathan will build out an Incident Response Plan that focuses on business realities, and help the startup's staff understand their roles during such an incident. When an incident comes, Leviathan may serve as the business' primary response staff, allowing employees to maintain the company.



and culture. In addition to process improvements, we will work with your organization to find and implement appropriate tools to augment your capabilities. Finally, we will work with your organization to create a training program for your staff that addresses technical, process, or both types of topics as appropriate.

Incident Response Planning

With the information gathered during the Initial Assessment, we will develop a plan documenting how security incidents will be handled. This plan will be high-level guidance, rather than focusing on minute details; this allows it to be useful in a wide range of incidents. Once the plan has been created, we will work with your stakeholders to review and amend the plan to ensure that it focuses on your organization's priorities.

Incident Response Practice

Without proving that an incident response plan works, its value is entirely theoretical. Practice exercises allow the people who will be responsible for managing an incident to walk through the response process, both to familiarize themselves and to identify gaps or inconsistencies in procedures. We find that running tabletop simulations of a security incident is a helpful first step; once stakeholders are comfortable with the new procedures, live exercises—where Leviathan employees will take on the role of attackers, while your team defends your network and its assets—provide valuable experience.

Conclusion

Leviathan combines its breadth of experience with a focus on meeting your organization's actual needs—without simply checking boxes for their own sake. We help your organization protect its information assets, while respecting your time and your core business interests.

Contact us today to see how aligning security with your business can help you achieve your goals.

EXAMPLE CLIENT:

LARGE ORGANIZATION

This large organization needs to be able to respond not just to a security breach, but to other challenges that threaten its continuity of business. Leviathan will identify process improvements that can help the business weather issues, train its staff on how most effectively to respond to incidents, and assist the organization in practicing its incident response capabilities. When an incident comes, Leviathan's deep subject-matter expertise will augment the organization's own capabilities.





Leviathan Security Group, Inc.
3220 1st Ave S, Suite 100
Seattle, WA 98134

p: 866.452.6997

f: 206.225.2004

e: contact@leviathansecurity.com

www.leviathansecurity.com

©2015 Leviathan Security Group Incorporated. All Rights Reserved.