Foundational Coverage

Introduction

SolCyber™ is here to help customers protect their businesses from modern security threats. Businesses large and small are hit by the same sophisticated adversaries. So how do you defend against nation state attackers without a Fortune 500 security budget? By partnering with SolCyber. We help businesses make smart decisions about defending their organizations most effectively and efficiently against an attack. Using the right combination of tools, services and people, we're able to deliver big business security that everyone can afford.

With SolCyber, our managed security program, delivered as a subscription service includes everything you need to immediately raise your security posture and stay resilient. This includes amazing humans running our 24x7 detection and response SOC and a minimum effective dose of technology that provides protection across the kill chain.

When we detect threats, our analysts not only triage, investigate and respond to confirmed threats, but they also work with you to:

- Understand your current posture and associated risks
- Increase your security posture and level up your employees
- Harden your environment and improve your defenses

Foundational Coverage

Making customers choose between different service levels doesn't make sense these days. When cyberattacks are more sophisticated and difficult to understand than ever, why would we put the onus on the customer to determine what level of capability is sufficient? We believe every business needs a foundational set of capabilities.

With SolCyber's Foundational Coverage, you get everything from a set of curated cybersecurity technologies to 24x7 coverage.

Amazing Humans

Every service starts with great people. At SolCyber, you'll be assigned a crew you get to know and rely on. They will be available not only during business hours but also late at night if you need help. These folks will be your go-to partners to help keep you secure.

Ransomware Readiness Assessment

At the start of every engagement (and every subsequent year), we will conduct a health check for your environment. This includes 17 unique controls (aka your vitals) from backup processes to admin sprawl to vulnerable AD configurations. Like a good doctor, we'll also help you improve quickly.

24x7 Detection and Response SOC

Attacks can launch anytime. Hackers don't take weekends or holidays off. We continuously analyze telemetry from your security technologies; and, when something suspicious arises, our expert analysts will investigate and validate the incident before escalating it to you. From there, they'll lead the response activity to stop the bad guys from completing their mission. However, our work is not finished there, each incident comes with valuable lessons on how to improve your defenses and how we can work together more effectively in the future.

In addition to monitoring across all the technologies in our curated stack, Foundational Coverage also includes support for Active Directory, Office 365 and G Suite.

Our service goes beyond waiting for a red light to flash. We'll periodically comb your systems for signs of compromise. This can be triggered by a large global hacking campaign or something suspicious found by our analysts at another customer. It's one more way we help keep you safe.

Curated Tech Stack

You don't have an infinite budget to buy, implement, and manage every new security tool. Yet trade-offs leave gaps the bad guys can exploit. You've purchased several security technologies, but how much do you really need? Are they effective? How can they work together better? We don't just work to answer those questions for today but we do that continuously to ensure you're protected with a described and ever evolving set of technologies to defend against modern threats:

- **Phishing Simulation and Training:** Humans are vulnerable; and, unfortunately, they can't be patched. We keep it fun by offering bite-sized training that takes minutes to complete.

- **Practical Vulnerability Management:** Patching is important but its impossible to patch everything. We recommend the most critical only.

- **AD Assessment and Hardening:** Attackers need to increase their privileges before they can access more systems and complete their mission. Reduce the attack surface of your Active Directory

- **Advanced Email Protection:** 95 percent of attacks start with a phishing attack. The more attacks we can stop at this point in the kill chain, the better. If an email is stuck is quarantine, we'll help with that too.

- **Endpoint Detection and Response:** Endpoints are the new battleground. Not only do they need to be protected, they are critical in response and recovery.

- **DNS Protection:** Other than email, the web is the best way for attacks to get in and get out. Protection wherever you work.

- **User Behavioral Analytics:** What if the attack doesn't contain malware? Know when accounts are being abused.

Yes, we include all these licenses in our Foundational Coverage.

> "We were immediately impressed with SolCyber's unique approach and how they've integrated a curated technology stack into their MSSP service. That combined with the company's 24X7 support made it an easy decision to work with SolCyber."
>
> *Jose Michelen, Senior Partner Alpha,*
> *AFP Crecer, Seguros Crecer, Gam Capital*

Bring Your Own Technology (BYOT)

If you have existing security investments but want to continue to own manage? No problem! We'll integrate the telemetry into our platform for analysis just like the tech we provide. Moreover, we'll also back out the management costs so it's win-win.

For more information about our Foundation Coverage, visit **www.solcyber.com**