CRAWL, WALK, RUN:

A Growth-Oriented Approach to Maximizing SIEM Deployment

Many organizations aggressively roll out SIEM or log management based on sales promises that "it will do everything for you." While these promises are mostly true, they may represent an organization's end goal, not their realistic starting point.

The reality is that SIEM functionality is limited to where the organization is and what it has in place…and that's 100% okay.

To take full advantage of SIEM technology, an organization must evolve to meet a certain set of conditions. For example, an organization may adopt SIEM so that when a violation is identified, a ticket can be automatically opened and the virtual CERT (Cyber Emergency Response Team) gets notified. But this presumes the organization has a ticketing system, an emergency response team already in place, and a process for what needs to happen when the ticket is received.

Many organizations believe they can spend their way to the functionality they want. That's only true for things that can be purchased, such as systems and tools. Things like skillsets, knowledge, and processes need to develop over time. An organization can bypass only so much of its growth and maturation by paying for it. The rest needs time to evolve organically through strategic direction and focus.

Successful SIEM deployment should be approached from a growth perspective. There's a saying in security sales that security isn't a technology. It's a system that includes technology, business process, and personnel. Taking this perspective helps organizations avoid the frustration and disappointment of feeling like they didn't "get what they paid for" that can result in managers blaming their teams or vendors or the technology itself.

Crawl, Walk, Run is a three-stage, growth-oriented SIEM deployment method that maximizes ROI on intellectual and actual capital of SIEM deployment. It focuses on the continuous evolution of

four elements in an organization's security ecosystem: sources, skillsets, knowledge, and tools. It also reflects the natural evolution of SIEM in organizations of every size, providing a customizable roadmap to increasing security outcomes and value.

This white paper explores each of the three stages of SIEM growth: Crawl, Walk, and Run. While some recommendations in each stage may seem obvious, organizations that don't follow them pay the price. But the advantages of Crawl, Walk, Run's growth-oriented approach is two-fold. First, you can avoid moving faster than is beneficial. Second, you can steer clear of "throwing out the baby with the bathwater" by disregarding a potential solution that can't yet deliver what you want because the organization—not the technology—isn't ready.

STAGE 1: CRAWL

The Crawl stage is about starting exactly where you are today and trusting that wherever that is, it's completely okay. Your first try will never be as good as your second. So it's important to embrace the idea that every organization has to start somewhere, minus the judgments about whether you're behind or ahead of the game. In a growth-oriented approach, moving forward by building on what you've learned is the key to success.

Each stage looks at four distinct elements that catalyze successful SIEM deployment and evolution. These elements are event and data sources (from which you will collect data), skillsets (the employable skills of you and your team), knowledge (what you and your team collectively know), and tools (the resources you wield to get things done).

In the Crawl stage, most of the focus should be on taking stock to establish your baseline.

SOURCES

Start with the data sources currently available to you and begin collecting there. Take an inventory of the devices and applications currently present in your environment and identify a few of those you want to start with. Some common examples include logs from firewalls, antivirus software, and Windows servers. If you don't currently have a specific source that you're interested in, don't worry about it yet. Just make a note of it at this stage.

Resist the urge to do too much at first. Remember, just because you have a source doesn't automatically mean you need to collect it (such as printer logs). Start with sources that you believe will provide useful and actionable information. By the same token, just because a device has a debug or informational level of logging available, that doesn't automatically mean you should collect those logs. At this stage, if a source can log more than it's currently logging, stick with the default logging levels.

SKILLSETS

Work with the skillsets available to you. What do members of your team already know how to do? Who are your experts? Examples of skillsets include formalized log monitoring and response, incident response, or security analysis/investigation. When you've uncovered available skillsets, document them in some way.

KNOWLEDGE

Knowing your environment is key. Catalog security resources as well as assets (routers, switches, and servers) and gather this information together.

TOOLS

Uncover all available tools. Gather your team and answer these questions collectively: What's your existing toolkit? Did you inherit security tools to enhance or support your efforts? Do you need to research open-source alternatives? Do you have people experienced in using these tools?

NEXT STEPS

Once you've completed your inventory, you can start collecting and analyzing based on your current limitations. In the beginning, this could look like batch processing instead of real-time alerts. For example, if you have firewalls, Windows servers, endpoints, and administrators without a security background, you can generate automated reports, send them to a designated "owner," and review the information every 24 hours.

It can be tempting to generate real-time alerts at this point, but if you don't have the skillsets and processes to do anything with them, you're just filling up an inbox. Batch reports reviewed at a regular cadence can be a good way to start building your knowledge foundation by training your team on what to look for.

The bottom line is to do the best you can with what you have right now. It gives you a manageable starting place to build on your people, processes, and technology. Again, it's important to be okay with wherever you are at this stage—it's all part of healthy growth.

STAGE 2: WALK

In the Walk stage, you begin adding to your baseline operations by enriching your four elements. You now have a working set of processes and technology. You have a good idea of what you know, some idea of what you don't know, and what skills your team can bring to bear. This stage improves on your first iteration and addresses deficiencies you identified in the previous stage.

SOURCES

Identify additional sources you weren't collecting from in the Crawl stage. These sources can include technology that didn't exist in the first iteration (especially if your Crawl period lasted six months or longer). Consider adding to sources that can collect more than they're collecting now to enable new kinds of logging. An easy example is to collect additional information from file servers so you can start auditing contacts with files, not just logins. Also, look for ways to enrich existing sources to make them more useful to analysts. For instance, reverse DNS lookups can enrich logs for analysts that know host names instead of IP ranges.

SKILLSETS

Enhance available skillsets with online sources (IT Pro TV, Lynda.com, and other training sites), conferences and training seminars, and vendor onsite training. Creating incentives (like bonuses) for learning new skills needed by the group encourages faster leveling up of your entire team.

KNOWLEDGE

In this stage, your collective knowledge base increases organically. Revisit things you documented in the Crawl stage such as questions and things your team didn't know it didn't know. Start identifying where the information might be and who the stakeholders are, where the resources are, and what regulatory requirements need to be considered.

TOOLS

Work additional tools you identified in the Crawl stage into regular procurement. And remember, as people add skills, other tools become available to your team. For instance, if you didn't previously have a packet capture tool available and didn't have anyone who could read packet captures, it's not an issue. But if someone attends a class and learns how to interpret packet data, then it might make sense to invest in a license for a commercial packet capture tool.

STAGE 3: RUN

The Run stage focuses more on automation. The goal is to automate the easy tasks so the people on your team can focus on doing more high-value operations. For example, your analyst may perform the same five steps gathering information and performing lookups at the beginning of each investigation. Suppose these steps take two minutes each. If these steps can be automated, the analyst regains ten minutes for each repetition. If the analyst performs six investigations in a day, automation gives you an extra hour of that analyst's time.

SOURCES

Shift the way you acquire technology by evaluating its ability to be monitored via logs and how it will add to your existing security stack. This shift ensures you will continue to approach security monitoring as an ecosystem. If possible, incorporate this shift into procurement of all products throughout the organization and include security teams in procurement decisions and product evaluation to help prioritize these considerations in all technology evaluations done.

SKILLSETS

Manage skills as a set of their own. Hire based on skills you identified you need and incenting people in the organization to acquire desired skills.

KNOWLEDGE

Develop a process to identify changing stakeholders and new assets that can be updated as new things come online outside your purview (such as a new finance or physical security system). This measure also helps keep your security ecosystem in balance and ensures that resources are always applied in the most appropriate areas.

TOOLS

Integrate your toolset. Instead of picking up another tool, focus on integrating more of your existing toolset by teaching the pieces of your toolkit to talk to each other. For example, this is when you can begin integration with ticketing systems, assets management systems, and compliance.

Automate as much as you can of the process itself. Automation keeps you from wasting expensive "people power," and it also means your rules get more complex. More conditions help hone automated responses and avoid exceptions. They also further whittle down events that end up in front of a human and keep stakeholders on board because the security team is better able to communicate business risk to the management team. This benefit is an example of the level of sophistication that develops with the Crawl, Walk, Run iterative method—something the pay-to-play method cannot offer.

If you need to purchase tools, budget ahead of time. Identify capabilities you'd like to have and then work on acquiring them proactively in the budgetary cycle.

PEOPLE

At this point, people become a new element in the system as well as the resource you want to optimize most. People are your most limiting factor due to time (there are a limited number of hours in the workday), money (people are more expensive than technology), and space (you can only hire/add so many people).

The goal is to involve your most expensive people as little as possible in administrative tasks. This approach means they can focus more on high-value activities because they're applying their specialized (and valuable) expertise as much as possible.

CONCLUSION

Just as you would never buy a young driver a Formula 1 race car, toss them the keys, and say "Good luck, kid," you should never believe the earnest promises of those who offer SIEM and log management "turnkey solutions." While growing your security ecosystem in an organic way may take more time than business stakeholders would prefer, it offers capabilities and functionalities that can't be bought. It allows you to cultivate a solution based on the particular set of conditions and needs unique to your organization and takes into account the sources, skillsets, tools, and knowledge available to you.

By employing each of the three stages, your team and your organization will identify more specific objectives and desired outcomes than they ever could by simply paying a vendor to deploy and integrate systems. Without the skills, tools, and knowledge to fully harness those systems, no organization can realize the return on investment that is expected.

The Crawl, Walk, Run method not only empowers security teams, it magnifies the value of their work in and across an organization. It also engenders trust from management and increases organizations' ability to maximize ROI on intellectual and actual capital of SIEM deployment. The secret of Crawl, Walk, Run is using a growth focus to create a stable, customized security ecosystem in a win-win environment.