7 PITFALLS OF USING SIEM TOOLS

BitLyft

There are no perfect SIEMs, and all have their pros and cons. Deciding which tool fits best with your organization depends on your needs and outcomes. Researching and validating cybersecurity tools isn't always easy, that's why we compiled a list of the most common pitfalls to avoid when deciding to use a SIEM tool.

1. No Scalability

It's important to determine if the underlying platform is scalable and cloud based. No one wants to babysit boxes or be stuck with hardware or software limitations. If your Network Security team isn't free to spend time utilizing the tool to investigate and remediate threats, your organization is vulnerable. Your team can get frustrated, bored, and leave for a more equipped and security focused organization.

2. Hidden Costs

The vendor must provide price protection. No one wants to get stuck with the upsells after you buy a solution that isn't fully what you need or what you thought it was. The cost should be defined deliverables for the set cost of the term of the contract. Ensure you talk through the specific use cases you need to address and if that's fully included and not add-on features with more costs.

3. Partial Coverage

The accompanying services from an authorized manufacturing vendor should provide 24/7/365 coverage. Keep in mind more than 75% of the vulnerability time is off hours (weekends and holidays). Make sure you're not purchasing a 9a-5p team, leaving you exposed the majority of the day.

4. Configuration Fatigue

Understand what's involved in configuration for the solution and what your ongoing commitments will be for optimal operations. Any SIEM is going to take significant investment to tune, test, and optimize. Discover if the promised solutions, like automation and playbooks, require coding and configuration on your part in order to work, or if the solution sold provides a guarantee of operability. Review the vendor's support and documentation process to see if they provide a path for learning their tool and getting tickets resolved.

5. No Way Out

Never sign a multi-year deal until you are sure the solution will meet your needs. When you do sign a multi-year deal, leverage discounting for loyalty and build in appropriate opt outs to protect yourself. If a vendor doesn't agree to an opt-out, ask why. Many vendors sell multi year deals knowing full well the solution will struggle and they have trapped you. Do not fall for it!

6. Scope Creep

Watch out for professional services scope creep driving up costs. If source integrations are professed during the business capture process, they should be included. Get follow-up documentation for a digital paper trail and ensure the MSA and SOW list what you've been promised. Being asked to pay for custom PS engagements to deliver basic and professed functionality is deceptive and is a major red flag. Be sure to protect yourself by negotiating any maintenance contracts up front and have it in writing.

7. All Sizzle

Be on guard when speaking with manufacturers directly. Remember they are trained to sell you the greatest thing since sliced bread. Do your due diligence independently and lean upon trusted advisors. Discover the qualifications of who you're talking to in the procurement and demo process. Controlled demos and POC's are "controlled" to limit throughput rates, which tend to be the problem of most platforms. Ask for client references to better understand how the solution performs in real life to avoid buying the marketing and sales sizzle.