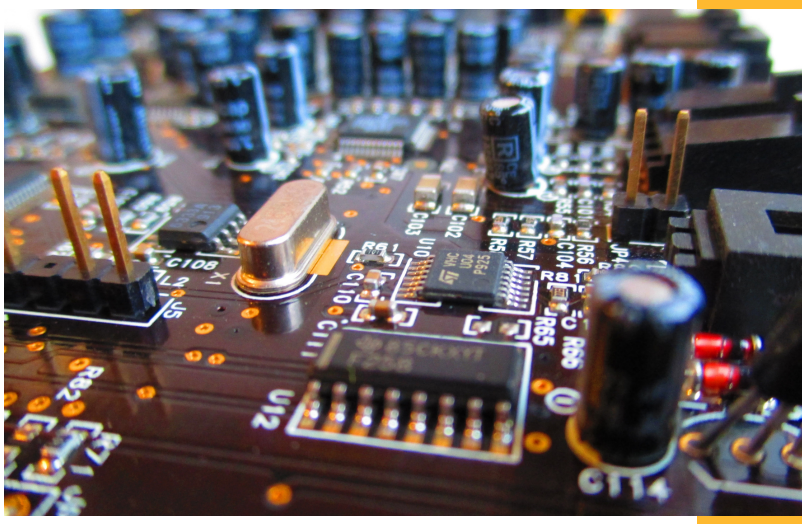
NETWORK BOX USA PRESENTS

SIEM BEST PRACTICES

A Security Incident & Event Management Checklist



KEY POINTS TO TAKE NOTE OF

Start Slow

Begin by defining the scope of your SIEM deployment. Next, identify and isolate your goals and objectives, taking stock of existing security protocols as you go along, and evaluating how these will fit into the prospective SIEM implementation plan. And then, roll it out and test it piecemeal, in phases. This way, your organization eases into SIEM.

Consider Compliance Requirements

Compare your list of compliance requirements against the list of SIEM vendor contenders you're reviewing, not only will that narrow down the number of candidates to evaluate, it will also force you to be more mindful of log data needs.

SIEM BEST PRACTICES

Adjust Correlation Rules

Customize each set of correlation rules and set thresholds according to what works best for you. A SIEM is designed to detect and uncover connections between events that would otherwise go unnoticed so start with the pre-set configuration rules of a particular SIEM solution you're reviewing, and work your way backwards, disabling and enabling (striking off and keeping) parameters according to what is needed and what isn't.

Imagine your SIEM to be somewhat like a big brother, keeping vigilant watch over your network. All day. Every day. 24/7/52/365.

Collect Security Log Data Efficiently

Strike a happy medium between collecting enough data to create a comprehensive view of your network but not so much that the sheer volume is overwhelming,

Key log data to collate should include, but mustn't be limited, to:-

>> authorization successes and failed attempts
>> changes to user privileges
>> application errors and performance issues
>> opt-ins like terms and conditions
>> all actions undertaken by users with admin privileges

Data you may not need to collate likely pertains to:-

>> anything that's illegal to collect
>> banking or credit card info
>> encryption keys
>> passwords
>> any PII

A SIEM collects logs, metadata; and not actual data.

SIEM BEST PRACTICES

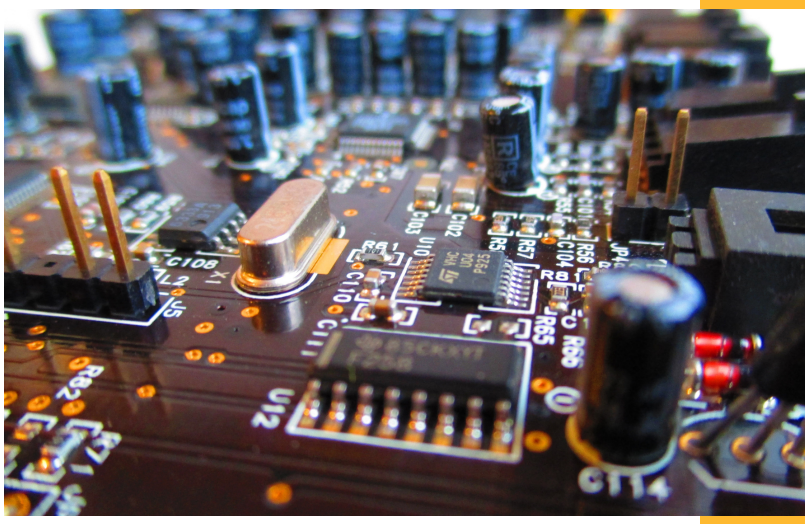
Have A "Post Threat Detection" Plan In Place

Deploying the right SIEM and adopting best practices is only half the battle won. It is imperative to have an Incident Response Plan in place to act upon what the SIEM uncovers, with pre-designated roles for every security personnel.

These include:-

>> who does what during a data breach or other information security event?
>> how do you prioritize and document security events?
>> how will a breach be reported to your incident response team @ via email or text or phone?
>> who is responsible for communicating with, say, clients, stakeholders, partners, law enforcement?
>> are appropriate backups and disaster recovery solutions ready following a compromise?

You should also have a "sensitive data" recovery plan on hand.



SIEM BEST PRACTICES

Continuously Refine Your SIEM Deployment

Having a SIEM does not mean that you can operate on a “set and forget” policy.

Pre-implementation planning and management are essential but a culture of continuous refinement and improvement must also be cultivated.

The mere use of a SIEM gives you access to a wealth of useful feedback, yes, allowing you to tweak and fine-tune everything so you can form an improved protection posture against threats on an ongoing basis.