The case for continuous penetration testing

By Oliver Cromwell, OccamSec

Knowing your risk

In an ideal world, risk management for an organization would be based on complete knowledge of all the factors involved in calculating the risk to an organization, namely, complete knowledge of all your systems or assets, and the data residing on those systems or assets, as well as knowing all related:

- Vulnerabilities or security problems affecting those assets,
- Threats, that is, actors attempting to exploit those vulnerabilities, and
- Knowledge of the attacks or exploitation events, that is, the exploits

![Fig 1: The threats](image)

While complete knowledge of any of those aspects, and thus their totality, is currently unrealistic, most organizations believe they have a fairly good understanding of the above and hence can come up with an accurate estimation of risk. Unfortunately, given the continuing trend of costly breaches of large organizations, by what are arguably semi-proficient attackers, it seems reasonable to step back and question this belief: are we as far from the “total ignorance” end of the spectrum of knowledge related to attacks on protected assets as we had assumed?

One of the most fundamental problems with most organization’s risk management methodologies is that they work off incomplete and out of date data. At worst, a single snapshot
is taken and presumed to be an accurate representation of an environment that is inherently in
flux, as are most IT departments, let alone organizations. In addition, that snapshot is taken to
be fairly complete. Whilst this may be effective in understanding the impact of a single event or
outbreak, such as that from a worm or a specific piece of automated malware, it does nothing
for:

- Systemic risk identification: for example, is your patching methodology flawed, or are
  your development practices leading to more vulnerabilities

- Risk trends: is the organization becoming more or less secure over time, or within a
  specific time period

- Intelligent adversaries: even a relatively unskilled adversary will probe your infrastructure
  and assets, and attempt to launch attacks over a period of time spanning days, weeks,
  or months

Thus a model that presumes a single, static infrastructure and its behavior in a single incident or
instance is fundamentally flawed.

Even worse, this flawed methodology and model is used in a wide range of activities relevant to
the security posture of an organization, whether it be penetration testing, auditing, or operational
risk assessments. Hence it is no surprise that risk management is working off models that are
inaccurate at best, leading to under or over specification and implementation of mitigating
controls. And thus high-profile breaches.

**Continuous Testing: A Solution**

Traditional penetration testing suffers from two main problems, as discussed previously:

- Generally out of date data for the known assets, vulnerabilities, and threats, but more
  importantly

- An incomplete knowledge of assets, vulnerabilities, and threats

Naively, we can simply suggest performing more testing and striving for greater coverage. The
devil is in the details though: given the cost of penetration testing and the inherent problem of
knowing how much is enough, it is best to treat this as a cost/benefit question.

**Important Lessons from Software Development**

Penetration testing, being a form of testing, we can reference other types of testing
methodologies and see what has been successful, what may be applied, and how. Arguably,
one of the most important aspects of a quality assurance program as part of a complete
software development life cycle is the level of integration of testing with development itself. Of
particular note are the ideas around:
- Continuous testing: every time code changes, before it goes into production, it is tested
- Regression testing: there is a testing baseline (itself modified in a controlled manner, rather than static) against which all testing is done, and against which improvements can be measured

These efforts emphasize the problems highlighted above: given there is no absolute or perfect security, testing within a void, as a once-off activity, has marginal value and speaks more to the idea of perfect security. Security in the real world is a compromise and should reflect the continually-changing and dynamic nature of assets, threats, and controls, and security testing should in turn address real risks, be they systemic, cyclical, or dynamic, and whether they originate from external attackers or internal issues. That is, putting it simply: security, and particularly security testing, such as penetration testing, should be continuous and comparative.

**Fig 2: Continuous penetration testing**

**Penetration Testing: not for the feint of heart**

This leads us to two important questions: how often should continuous testing be performed, and by whom? Even with testing that produces easily comparable results, itself a non-trivial task, the testing takes time and effort - even if it can be largely automated, to replicate the efforts of anything more than the most unskilled attacker, penetration testers need to review the findings and use those to guide their manual penetration testing efforts. In addition, unless there
is complete assurance that your test or development environment exactly mirrors your production environment\(^1\), it is likely that production testing is required. This in turn may generate alerts from monitoring systems which may not be discernible from malicious attempts, increases the load on production applications and infrastructure, and may also cause outages - either through increased load or exploitation of a vulnerability that causes crashes, freezes or other denial of service.

Equally as challenging, as knowing what to test and when to test it, is finding the right people to perform the testing. If we are expending any sort of non-trivial effort on testing, it seems reasonable to have fairly skilled testers and analysts. As mentioned previously, if we are trying to replicate the efforts of something more than a completely unskilled attacker, we need a dedicated, full-time team to conduct the testing, analyze results (and conduct further or follow-up testing) as well as liaise with the rest of the organization to ensure that testing does not impact production systems and achieves desired business goals. These testers also need to be able to clearly articulate the results of the assessments to both technical and business teams and have the ability to translate focused technical risks into strategic and business risks. This level of technical and organizational skill in turn implies keeping those resources adequately trained and up to date with the latest pen-testing methodologies, building and maintaining systems to perform the automated aspects of testing and comparison, as well as reporting, and ensuring personnel are kept abreast of the latest attack tools, methodologies, and threats that may impact a given industry or organization. By any measure this is a large and costly in-house endeavor for most organizations.

**External Penetration Testing**

If you are in charge of security testing, risk assessment or management for your organization - that is, responsible for penetration testing activities, you may at this point be asking yourself: what do I do? On the one hand, you need testing, and continuous penetration testing sounds plausible, but at the same time, you don’t have the time or budget to form or maintain a penetration testing team, let alone implement and manage the tools to support them.

As with a number of other areas in IT, specialized organizations that focus on one specific activity can be utilized. Having external penetration testers from reputable penetration testing organizations perform this function has a number of advantages: given the specific, focused task and thus skill set required, a team focused on this task can ensure they have the specific, specialized skills required, as well as the knowledge of systems, vulnerabilities and threats gained from focused research and external agreements with other specialist organizations, and most importantly is constantly refining those skills and knowledge.

In effect, you are getting access to a specialized set of tools, personnel and knowledge base that most organizations not focused on such testing can realistically never achieve. One other

\(^1\)which is unlikely, particularly given the constant change most applications and infrastructure go through, as discussed earlier in this paper
often-unrecognized advantage is that using external penetration testers more closely replicates a real attack and threat: rather than an internal group with prior knowledge of the organization, and in most cases internal constraints, you have a well-defined relationship and can control the exact amount of knowledge about your organization you provide, and the specific activities required of the external penetration testing team. Having an external group with testers removed from your organization also confers advantages in terms of identifying systemic issues, particularly those issues likely to be downplayed or dismissed in the process of being raised due to organizational politics: rather than having to report issues up through normal channels, external testers can highlight those risks that reflect real world weaknesses directly to those most likely to address them.

**Continuous Penetration Testing and the OccamSec advantage**

While we have argued for the feasibility and value in using an external penetration testing organization earlier, we still have the issue of continuous penetration testing to deal with it: specifically, the questions of how often is good enough, and how an organization deals with the mountain of information generated by such continuous penetration tests, particularly their results. Most penetration testing organizations generate a standalone report, so this latter concern is certainly reasonable.

![Fig 3: The OccamSec approach](image)

To that end, OccamSec’s testing methodologies are built around repeated penetration testing, with an inherent comparative aspect, so our testing and reporting addresses this directly. Our reporting is optimized for our base penetration testing package, which is based on changes in
an organization’s threat and vulnerability landscape between two penetration tests - the assessment score delta - conducted however far apart an organization chooses it, and presents those differences concisely.

OccamSec can of course conduct more than one penetration test in an engagement, and in fact, this is encouraged so that an organization gets a better idea of the level of improvement in security over time, without the worry of the recipients of the testing results having to weed through unnecessary information and compare one set of results to the previous one. You also have the benefit of knowing that the testing was performed using the same methodology. This is important due to the fact that differences in testing approach and methodology will likely lead to different results so you will not have a true benchmark comparative analysis.

Given the ease with which comparative results can be produced, we can now answer the question of how often we should perform penetration testing: as often as an organization requires. Ideally, this would be at a minimum, as often as changes affecting the externally visible attack surface, that is, the set of vulnerabilities an attacker may exploit, are made. For organizations where these changes are always implemented in a controlled manner, this may be linked to change management processes, for example, as post-implementation verification or as part of some development process, but in other cases, or where an organization requires a higher level of assurance, suspects that changes affecting external security are being made more often, or would like to identify systemic risks, OccamSec can provide assistance with this scheduling and planning. And for all organizations, we recommend taking advantage of OccamSec’s Vulnerability Assessment and Alerting services to improve the precision of penetration testing results and effectiveness, as well as our other specialized services. For more information, please visit www.occamsec.com