VULNERABILITY AND PATCH

CYBERKOMBAT

CyberKombat is a brand new experience designed to replicate a serious cyber attack on an organisation, giving real life SOC teams the opportunity to test their abilities and gain a wealth of new skills in the process.

SOC personnel need a way of gaining real world understanding of how attacks are happening and how to respond to them, as well as keeping current with the latest attack and defence security models. CyberKombat aims to solve some of the biggest problems SOC teams face today.

MANAGED SERVICES

Our managed service is one of the most flexible in the industry, we make no pre-defined 'vanilla' service offering. Our approach is designed in the same way as we like to do business, we spend the time to understand where different organisations require the expertise and if our managed services team are able to bridge that gap.

As an illustration of that, we have customers using our managed service for minor areas, such as backend customer reporting, on things like access to their data right the way through to managing the security programme and technologies around PCI for instance.

CONTACT US

+44 (0) 1582 434320
+44 (0) 1158 243432 (Support)
enquiry@satisnet.co.uk

Satisnet Ltd, Basepoint Innovation Centre, 110 Butterfield Great Marlings, Luton, Bedfordshire, LU2 8DL

IDENTIFY VULNERABILITIES

Organisations typically struggle, or it's an expensive exercise smaller businesses simply can't afford to have the ability to scan the configuration of network devices, as these tools are typically expensive and cumbersome to manage.

Differing types of vulnerabilities to find in the environment include;

- Software (e.g. Adobe)
- Open source software, used within in-house developed applications
- Configuration, like a mis-configured firewall
- Open ports that aren't required
- Zero day vulnerabilities, used by malware

Vulnerability scanners, like Tenable and Black Duck, are seen as a solution to provide the ability to find all of these types of vulnerabilities within the environment, which is only part of the journey once the latest list of vulnerabilities is announced by Microsoft for instance.

CLASSIFY VULNERABILITIES

It's accepted vulnerabilities will exist in all environments, but it's virtually impossible to mitigate all of them, it is therefore important to review all vulnerabilities identified and prioritise them.

A simple way to look at this is; Review all exploitable vulnerabilities to prioritise critical and high vulnerabilities – a good strategy but it is not always the best strategy for the organisation in terms of reducing the attack surface, yes you've removed a lot of vulnerabilities, but are they, in your environment, the most important?

When classifying vulnerabilities it is important to take into consideration your organisations security infrastructure before prioritising the remediation efforts, as the same vulnerability can cause more of an impact in some organisations than others, based on what prevention layers already exist. All of this sort of information needs to be taken into account to ensure that resource is focused in the right area and that the security posture is as high as possible.

As an example, if you can remediate 10 vulnerabilities and reduce your attack surface by 80%, you'd take that action first, rather than working through 100 vulnerabilities that are responsible for the other 20%, right?

REMEDIATE AND MITIGATE

Once the vulnerabilities have been identified in the environment and classified, the remediation steps then require to be defined. We work with organisation to define workflows for each scan that is run, so that remediation steps are clear, if you are running a patch audit scan for instance, the remediation step would be to apply the relevant patch and audit that it has successfully been applied.

For a more complex requirement, like a firewall configuration change, this would require consideration of things like change windows/requests, individuals required to apply the change, and documentation to be completed pre and post change.

The lifecycle is typically then reported to senior management, so we work with organisations to define the automated reports, or templates for individuals to tweak. The typical reports we work to produce with organisations are for things like;

- Remediation time against SLA
- Number of vulnerabilities (trend)
- Unknown devices detected on the network
- Number of assets scanned in any particular 30 day period, where the requirement is that all assets are scanned at a minimum every 30 days for instance

TECHNOLOGIES USED

BLACKDUCK

IBM BigFix

Radar Vulnerability Manager

shavlik

SOCautomation

tenable network security