Using Baselines & Behavior Profiles

Baselining refers to the recording and profiling of what is considered to be "normal" on a system or in a network. This can include network utilization, protocol field values, active hours, user activity, port numbers and any factor that could change and thus indicate an imminent threat or attack. This baseline can be consistently compared to the current state of the network to identify any anomalies which could potentially suggest a security or performance issue. This process of identifying potentially malicious events or performance issues using differences between the status of the current network and the baselined network is categorized as anomaly-based detection.

For example, suppose a network has been baselined to be extensively using ports 22, 25, 80, 443 and 3389 with very little traffic on other ports. If there was a significant increase in Telnet traffic on port 23, the anomaly-based detection system would identify this event as an anomaly. This anomaly could indicate that there may be malicious remote command and control occurring through Telnet, or it may just be that the network has started implementing Telnet as a way to allow employees to remotely access internal systems. In order to narrow down this wide range of interpretations on a single anomaly to a single cause or a small range of possibilities, further analysis is required.

ANOMALY-BASED DETECTION

Take a look at this image:

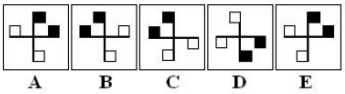
I'm sure you can notice the odd one out quite easily from this image. But what do a bunch of apples have to do with network security and threat detection mechanisms?

Interestingly, the process of picking the "odd one out", in this case, a red apple from a bunch of green apples, is exactly what anomaly-based detection is all about! Except, in this case, the green apples become the normal set of network, system, application, or user behaviors, and the red apple becomes a malicious threat.

Baselining and anomaly-based detection is an effective defense mechanism against new and unprecedented attacks and threats. Unlike signature-based detection which is based upon factors such as file hashes, where any variants of malware cannot be detected, anomaly-based detection allows detection for malicious activities and network behavior, which are hard to discretely define. Signature-based detection is ineffective against threats that are not recorded in its signature base, providing somewhat limited flexibility. Furthermore, detecting anomalies in network traffic allows for an excellent detection mechanism against DoS/DDoS attacks and attacks through an encrypted channel. Anomaly-based detection, coupled with automatic or manual analysis, can provide excellent network and system monitoring.

However, anomaly-based detection does have its shortcomings. Since network, system, or application behavior is abstract, unpredictable, and highly dynamic, many false positives are generated – especially in large-scale enterprise environments that have a complex network architecture. With so many activities and events occurring, the chances of encountering a "false anomaly" significantly rises. Additionally, baselining networks can take a substantial amount of time which grows with the complexity and scale of the network, causing implementation delays. The baselining process should be repeated after time intervals and after significant changes to the network, and finely adjusted to provide both an updated picture of the network and reduce false positives. Lastly, the analysis process can be time and resource-intensive with the number of false positives to sift through, especially with manual analysis.

Now take a look at this image:



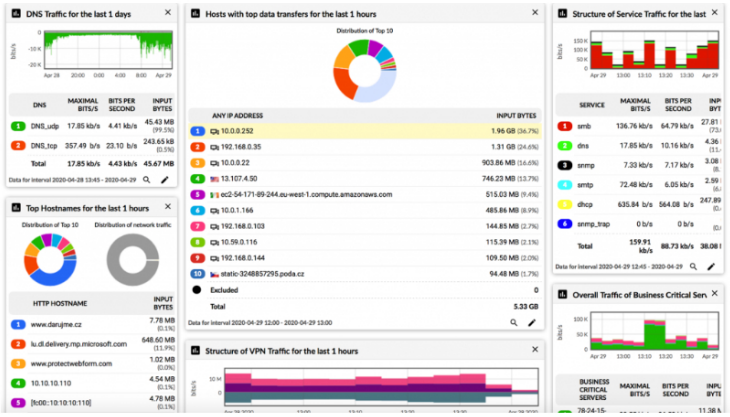
Did you find the "odd one out"? (If you didn't, the answer was A). How long did it take for you to find the anomaly? How long did it take for you to notice that all the figures except A were reflections or rotations of a single figure? That is, how much time did it take for you to 'baseline' the figures? And how long did it take for you to 'analyze' each of the figures? How many 'false positives' did you sift through to find the anomaly? This may not have been the best example, but it captures some of the downfalls of anomaly-based detection – the long baselining time and resources wasted on analyzing false positives.

ENHANCED DETECTION

Baselining and anomaly-based detection can be incorporated into a wider group of security controls, systems, and procedures in order to improve the organization's overall security posture. Anomaly detection systems allow for quick detection of potential attacks or threats and can thus alert the Incident Response Team and the CSIRT in order to further investigate or stop an attack early in its tracks.

Anomaly detection systems can also send its logs to a centralized SIEM which can aggregate data from the ADS and a variety of other sources, such as network activity logs, in order to provide the Incident Response team with a clear understanding of the events prior to, and during an attack.

Anomaly-based detection allows an organization to be ready for unknown threats with its flexibility and its reliance on deviations from normal network behavior rather than a signature database. There are many tools available to collect, analyze and display network statistics and alert on anomalies, including Cisco Stealthwatch, IBM QRadar and Flowmon ADS.



Flowmon ADS Dashboard

Previous Topic

Mark Complete

Next Topic

Back to Lesson