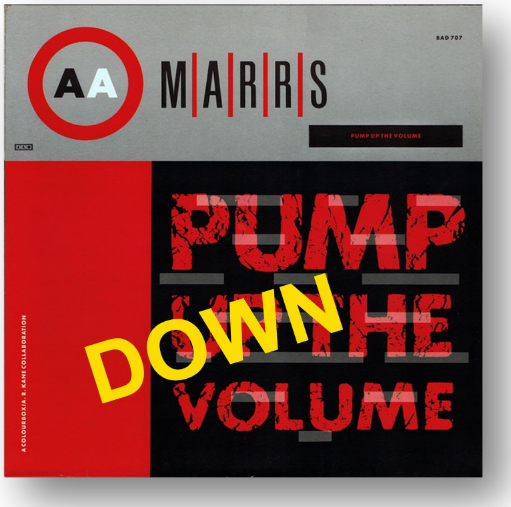
Solution Brief

Pump Down the Volume*



The traditional approach of network security monitoring generates a huge volume of information. The positive side is that almost anything can be found, but proactively hunting for threats in your network is overwhelming at best. This is true whether you're hunting though log files, endpoint, or intrusion detection (IDS) data. In this solution brief we focus on the advanced intrusion detection features of the Stamus Network Detection (Stamus ND) and Stamus Network Detection and Response (Stamus NDR) platforms.

Your Time is Gonna Come

The standard way of reducing the noise created by an IDS is through suppression and thresholding as well as simply removing signatures from the ruleset that identifies potential malicious activity.

The suppression and thresholding methods are the most interesting. The traditional approach allows a suppression by source or destination IP address, which can also be used for Thresholding. This methodology might have been effective in the 1990s, but it is completely insufficient in today's threat landscape.

For example, a lot of IDS rules detect malicious behavior, like phishing attempts, on HTTP websites. If the website is hosted on a set of servers or in a Content Delivery Network (CDN), then we could be contending with multiple addresses making it difficult to discriminate against false positives with an IP address. In this case, you would need to know all the IPs of that particular CDN. This is a complex task given the number of these IP addresses and the fact that they are changing continuously. Worse yet, a real phishing website could be hosted on the same CDN resulting in missing a true positive altogether.

Enjoy the Silence

Stamus Security Platform (SSP) introduces an innovative way to deal with the extraordinary amount of data generated by intrusion detection systems. Instead of limiting filtering capabilities to IP addresses, SSP allows a security practitioner to incorporate any available metadata, over 2,000 fields with over 100 for active filtration, to build powerful filters. Problems like the CDN-hosted website becomes a trivial process addressed with a simple suppression filter combining the phishing signature and the HTTP hostname.

But the Stamus Stamus Security Platform approach goes beyond that. IDSs have evolved from a shell code detection system to a more complex system with, you guessed it, shellcode detection. Additionally, Stamus Stamus Security Platform information from the network that provides context to the analyst. Signatures triggering this kind of behavior should not be seen as alerts but rather security events that can be useful during investigations.

One example of such a signature is the detection of a Debian Linux distribution upgrade. If your IDS monitors a farm of Linux servers, this is essentially useless. But if the signature is firing in your Windows-only desktop network, this may be a problem. As part of the data enrichment process within Stamus Stamus Security Platform, organizational network information is embedded into these events. This additional context makes it possible to suppress the alert for the server network and keep it for the desktop network.

Alert metadata combined with enriched data from Stamus Stamus Security Platform opens the door to countless possibilities. You can, for example, suppress the alert in the server network if the upgrade source top domain is debian.org and keep it if it is not.

Know Your Enemy

The ability to filter IDS events by any metadata criteria is certainly empowering but do we really want to have to look at Ubuntu upgrade alerts in our server network? Now imagine the ability to tag them as informational so they don't pollute the alert dashboard. Any combination of filters (using metadata) can be used to tag an event as informational or relevant. This enables the ability to tag the Linux distribution upgrade as informational and tag as relevant a Kali Linux distribution upgrade, something that's not likely to conform with your organization policies.

Stamus Stamus Security Platform automatically identifies informational and relevant events and allows an analyst to create their own tags with an easy-to-use web interface with an unparalleled ability to dynamically explore and hunt within your network data. Metadata fields are presented to the user in logic groups and selected with a click to add that criteria to any given filter set applied to the data. This capability allows the user to discover data associated with any hypothesis they may have regarding a potential compromise. In other words, practitioners can add filters to discover something unique and save it as a part of a routine.

Once a filter set is limiting the data to a semantically homogeneous set of alerts, the analysts can decide to transform that filter set into an action. The transformation and suppression tagging will then be applied to all the upcoming events.

Converting the exploration and proactive hunting of a skilled analyst to automated actions is a key advantage of Stamus Stamus Security Platform , allowing analysts to streamline their daily routines as well as the security team as a whole.

Summertime, and the Livin' is Easy

Instead of checking the same alert list every day, analysts simply start their day by being immediately introduced to relevant events and trigger an incident response if needed. From there, an analyst can explore and hunt through untagged events and further bolster their teams' overall security posture in the process. After a few days of using the solution, the only events on the network that are unclassified are those that have never been seen before. They can then be easily analyzed, classified, and will not clutter the dashboard in the future unless, of course, you want them to.

GEORGE GERSHWIN'S
Porgy and Bess
RCA RED SEAL 3 RECORD SET COMPLETE RECORDING
IRA GERSHWIN DuBOSE HEYWARD
As produced on stage by
SHERWIN M. GOLDMAN and HOUSTON GRAND OPERA

This creates a virtuous circle where the analysts are not overwhelmed with the data and can focus on what really matters: defending their network.

* All references to copyrighted works are made with great respect and admiration for the respective artists: MARRS, Led Zeppelin, Depeche Mode, Rage Against the Machine and George Gershwin

ABOUT STAMUS NETWORKS

Stamus Networks believes in a world where defenders are heroes, and a future where those they protect remain safe. As defenders face an onslaught of threats from well-funded adversaries, we relentlessly pursue solutions that make the defender's job easier and more impactful. A global provider of high-performance network-based threat detection and response systems, Stamus Networks helps enterprise security teams accelerate their response to critical threats with solutions that uncover serious and imminent risk from network activity. Our advanced network detection and response (NDR) solutions expose threats to critical assets and empower rapid response.

STAMVS NETWORKS

5 Avenue Ingres
75016 Paris
France

450 E 96th St. Suite 500
Indianapolis, IN 46240
United States

contact@stamus-networks.com
www.stamus-networks.com