WHITE PAPER

IDS Evaluation Guide

Learn about the critical capabilities to look for in an Intrusion Detection System (IDS)

Summary

Intrusion Detection Systems (IDS) have been a mainstay in the security practitioner's arsenal for many years. They are designed to gather and analyze information from your environments to identify possible security breaches. The following guide provides a useful reference for you when you're evaluating IDS tools.

Additionally, you'll learn how AlienVault® Unified Security Management (USM)™ delivers critical IDS functionality for your on-premises and cloud critical infrastructure as one of five built-in essential security capabilities. Managed from a single console, AlienVault USM integrates IDS with asset discovery, vulnerability assessment, behavioral monitoring, security information and event management (SIEM), and continuous threat intelligence from the AlienVault Labs Security Research Team, to add critical context to alarms and give you the ability to quickly detect and respond to threats.

Introduction

An Intrusion Detection System (IDS) is an essential tool in every security practitioner's arsenal. Intrusion Detection Systems are designed to gather and analyze information from networks, cloud services, and hosts to detect malicious activity both before and after a security breach.

In this guide, we will examine the critical components of network, cloud, and host IDS, and explain how to evaluate IDS solutions.

The core functionalities of network IDS (NIDS) include:

- Monitoring and analyzing network and system activities
- Recognizing typical attack patterns
- Analyzing abnormal network activity patterns

The core functionalities of cloud IDS include:

- Interfacing directly with cloud APIs
- Analyzing log data to spot intrusions
- Identifying which users and services have accessed the cloud environment

The core functionalities of host IDS (HIDS) include:

- Analyzing system configurations and vulnerabilities
- Assessing system, registry, and file integrity
- Analyzing abnormal user activity patterns
- Tracking user policy violations

Traditional IDS has been around for many years and forms the backbone of any good security practice. But in recent years, it has become apparent that traditional capabilities of IDS are not sufficient to deliver a complete security solution. IDS as a standalone tool provides too narrow a view of the threat vectors facing your organization. Intrusion detection needs to be augmented with other security capabilities and designed to safeguard the entirety of your critical infrastructure to achieve effective threat detection and response.

Additionally, the growing adoption of public cloud computing calls for new intrusion detection approaches and technologies, as traditional IDS solutions were not designed for or optimized for public cloud architecture.

Security teams are typically overstressed and under-resourced trying to stay ahead of the evolving threat landscape, and often do not have the time to wade through mountains of alerts. Organizations need an IDS solution that can prioritize alerts and provide a level of context to each alert. Receiving an alert in the context of your entire infrastructure allows you to focus your time on addressing the real threats.

Threat intelligence is another crucial component to augment the effectiveness of your IDS solution. Threat intelligence is information about malicious actors and their tools, infrastructure, and methods. Effective threat intelligence is essential for making sense of mountains of internal and external threat data to enable efficient threat detection and prioritized response. If you can find a solution that includes these key capabilities, you are well on your way to an effective security program.

Consider the following key questions when evaluating an IDS solution:

› Does it include network, cloud, and host intrusion detection?

› Does the IDS use a signature-based approach?

› What is the throughput of the IDS?

› Does the IDS perform protocol analysis?

› Does the IDS do aggregation (i.e. combining alerts)?

› Does the IDS have integration capabilities (e.g. with other platforms)?

› Does the IDS have contextual enhancement? Does it feed into SIEM?

› Does the cloud IDS use direct hooks into cloud APIs?

› Does the cloud IDS provide direct access to your cloud service provider's management plane?

› How quickly is the IDS able to detect the latest threats via new updates?

Network, Cloud, or Host IDS

The first thing you need to determine is if you need host intrusion detection (HIDS), cloud intrusion detection, or network intrusion detection (NIDS). Intrusion detection traditionally includes both NIDS and HIDS components, and both are essential for a complete security solution for your on-premises environments. Many traditional solutions do not include cloud IDS, which is an important consideration if your organization uses public cloud environments or plans to in the future.

Network IDS

Network IDS performs an analysis of all traffic passing through the network and matches the traffic to the library of known attacks. An alert is sent to the administrator when a match to a known attack occurs or if abnormal behavior is identified.

The advantage of network IDS solutions is that they can monitor an entire network with only a few well-situated nodes or devices, and they impose little overhead on a network. One disadvantage of network IDS solutions is that the devices have trouble monitoring high-volume traffic. When the traffic volume exceeds the IDS' capabilities, the solution will start dropping packets[1],causing it to miss attacks launched during peak traffic periods.

Cloud IDS

Public cloud environments pose a unique challenge to security professionals because traditional IDS methods don't readily adapt. Restrictions implemented by cloud service providers make it difficult to access packet-level information using port mirroring, taps, or traditional network-based methods. (The upside to these limitations is that cloud service providers take responsibility for the security of the networking infrastructure.) Regardless, IT teams are still responsible for monitoring and securing assets and data stored in public cloud environments, which requires a new cloud-native IDS toolset.

Luckily, there is a way to gain security visibility into public cloud environments and implement cloud IDS. The cloud management plane is essentially the cloud API you can use to configure, monitor, and control your cloud environments. Access to the management plane gives you visibility into every operation in your cloud environments, including which users and systems are accessing them. For a cloud IDS solution to be effective, it must be built natively for the cloud and have direct hooks into cloud APIs.

Host IDS

A host-based IDS monitors individual hosts on your network for malicious activity.

The host IDS takes a snapshot of your existing system key files and applications and matches it to the previous snapshot. If the critical system files were modified or deleted, an alert is sent to the administrator to investigate. This functionality is also known as file integrity monitoring.

The advantage of HIDS is that these systems in general tend to be more accurate than Network-based IDS because they analyze the server's log files, not just network traffic patterns. Host-based IDS can analyze activities on the host in a very detailed manner. It can often determine which processes and/or users are involved in malicious activities, and can tell you when an attack has potentially succeeded. The issue with host-based systems is that they tend to be expensive and resource-intensive because they require installing an agent on each host you wish to monitor, with licensing generally charged on a per-seat basis.

Solution Recommendations

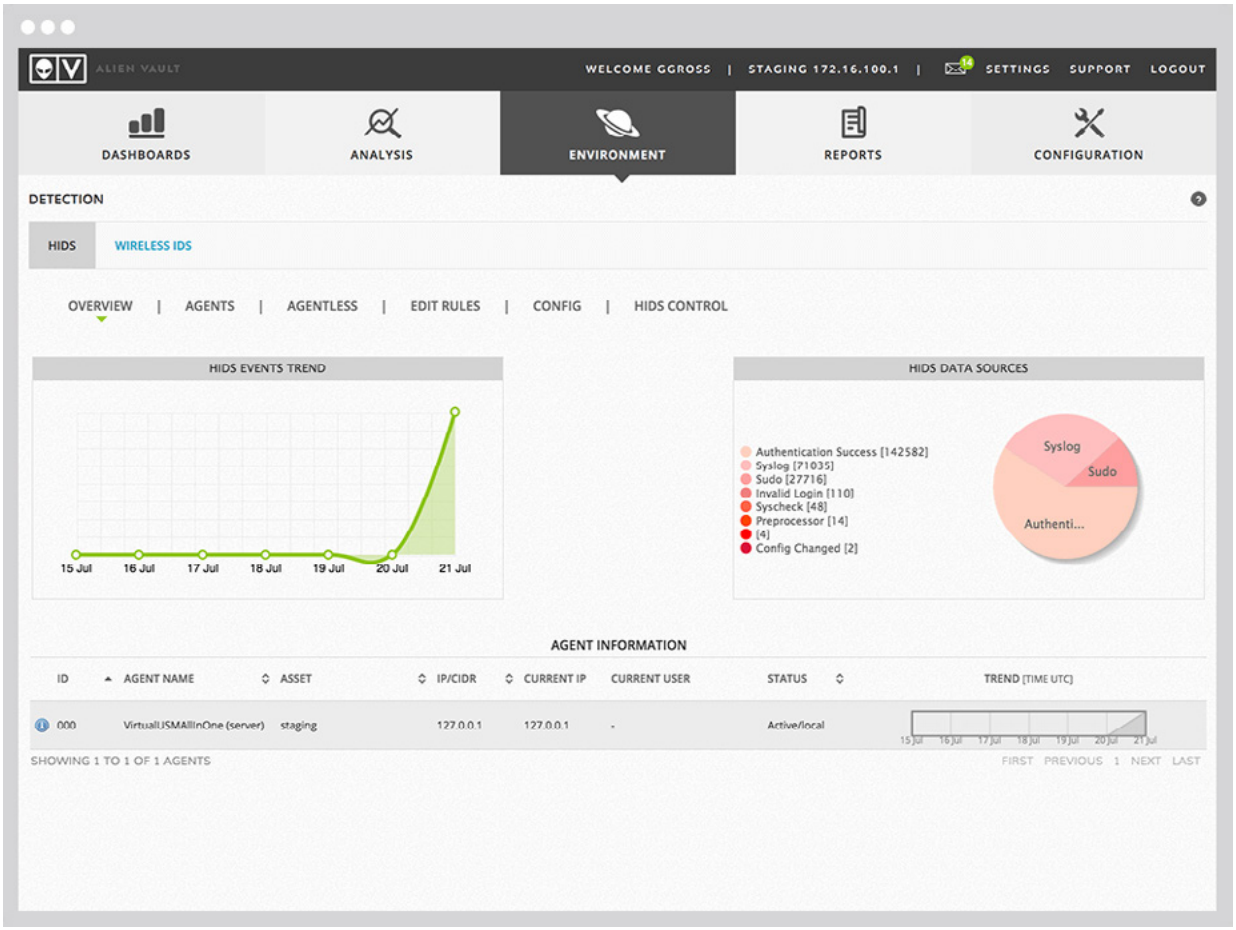
For a truly effective security control strategy for your on-premises environments, you need both NIDS and HIDS for your intrusion detection solution. NIDS and HIDS complement each other, and each provide functionality that enhances the effectiveness of the other by providing visibility into all traffic on the network as well as traffic targeting each monitored host. Organizations using public cloud environments such as Microsoft Azure or Amazon Web Services (AWS) must include cloud IDS in their security plans. If you need to secure both on-premises and cloud environments, look for options that deliver NIDS, HIDS, and cloud IDS together in one solution, rather than integrating single-point products, which can leave gaps in your security coverage. Be sure that your cloud IDS solution is natively built and can access your cloud service provider's management plane.

[1] Refer also to the discussion of throughput in the 'Throughput' section below.

AlienVault USM Capabilities

AlienVault Unified Security Management (USM) provides two deployment options, USM Appliance™ and USM Anywhere™, that provide both network IDS and host IDS functionality. The host IDS is simple to set up and comes integrated out-of-the box with network IDS and a score of additional built-in security tools, all managed from a single console, to enable you to quickly correlate events, detect threats, and prioritize response.

USM Anywhere additionally offers native cloud IDS capabilities that interface directly with the management plane to give you the highest possible level of oversight of your AWS and Azure environments. By layering all three IDS functionalities in one solution, USM Anywhere gives you seamless intrusion detection and complete visibility across your entire critical infrastructure, even as you migrate infrastructure from your data center to the cloud.



Signature-based vs Anomaly-based IDS Systems

Overview

You need to determine if you want an on-premises IDS solution that is signature-based or anomaly-based. There are advantages and disadvantages of both.

Signature-based detection

Signature detection, also known as pattern matching, involves searching network traffic for packet sequences (such as file hashes) that are known to be malicious. Once a match to a signature is found, the system generates an alert.

A key advantage of signature-based IDS is that signatures are easy to develop and understand. In addition, pattern matching can be performed very quickly.

But there are certain limitations of this method. Because the signature can only detect known attacks, some approaches to signature-based detection require the creation of a signature for every attack, and thus previously unseen attacks cannot be detected. In addition, signature engines are prone to false positives because some normal network activity can be misinterpreted as malicious. However, there are ways to mitigate these disadvantages, such as using a strong correlation engine. Correlation engines detect relationships between different types of events to identify malicious activity. In doing so, correlation engines turn disparate data into actionable information.

Anomaly-based detection

Anomaly-based detection incorporates the concept of a baseline for normal network behavior. Events in an anomaly detection engine are identified by any behaviors that fall outside of the predefined or accepted model of behavior.

One advantage of anomaly-based detection is that a new attack for which a signature does not exist can be detected if the behavior falls out of the normal traffic patterns. A disadvantage of anomaly-based detection engines is the difficulty of defining rules, as the rules need to be tested extensively for accuracy, and without entering good baseline knowledge of your network, they can generate many false positives. In addition, anomaly detection engines have difficulty translating easily across differing security vendor platforms.

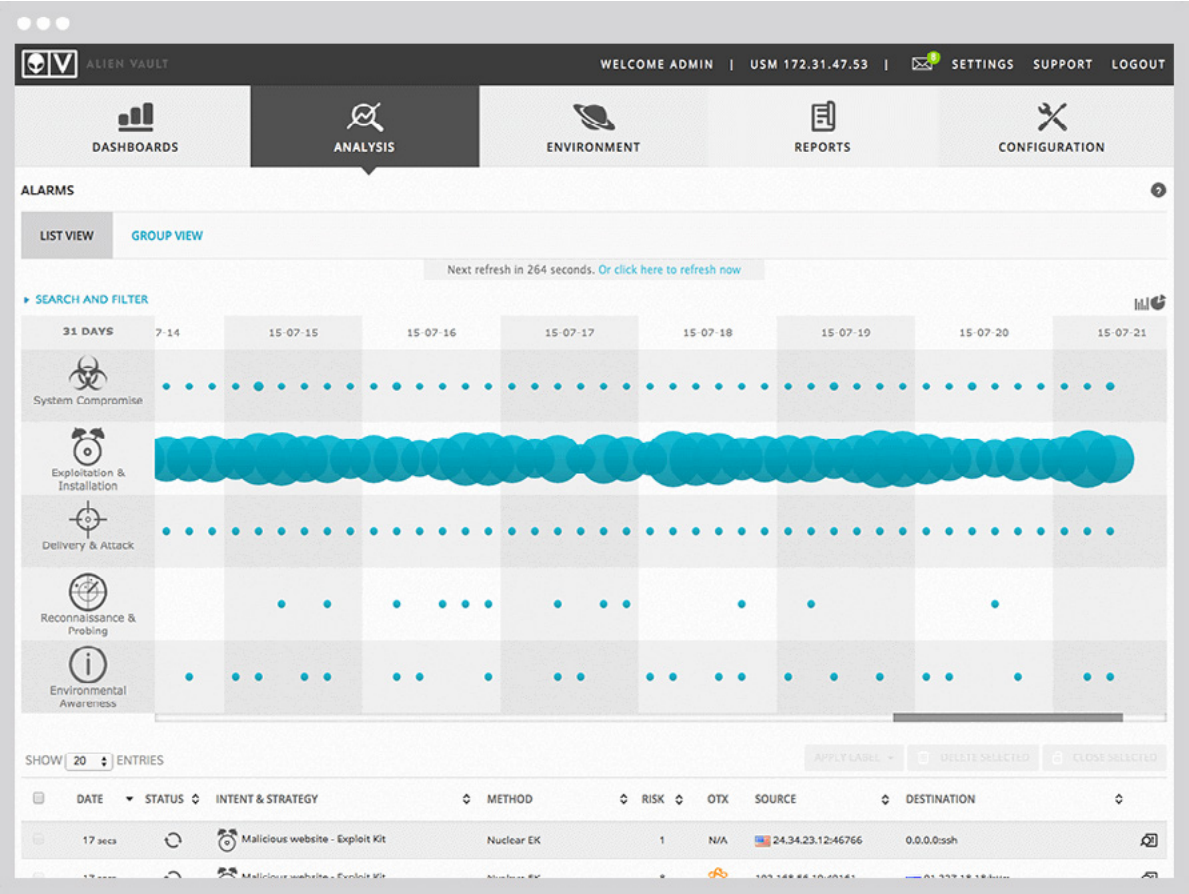
Solution Recommendations

Signature-based IDS solutions are the most practical given the resource limitations of most organizations, and one of the most effective solutions for short-term threat detection. For signature-based solutions, you need to look for a solution that rapidly updates signatures when new vulnerabilities and exploits are discovered. The signatures should be updated frequently to ensure they can detect the latest threats as well as reduce false positive alerts. The solution also needs to have the ability to import signatures from commercial and open-source signature feed providers.

AlienVault USM Capabilities

AlienVault USM delivers IDS using the signature-based detection method, and the signatures are updated continuously by the AlienVault Labs Security Research Team (see a history of update summaries in the **AlienVault forums**). AlienVault USM overcomes the traditional shortcomings of the signature-based method with its strong correlation engine. Leveraging the numerous security controls built into the USM platform, the AlienVault correlation engine uses built-in correlation rules to detect relationships between different types of events occurring in one or more monitored assets to identify threats. The use of multiple data sources greatly enhances USM's ability to identify malicious activity. AlienVault Labs Security Research Team continuously updates USM with correlation rules and signatures based on extensive global research, so you gain the assurance of having the latest threat intelligence to detect intrusions in your environments without having to conduct your own research or write your own correlation rules. In addition to their

own proprietary research, the Security Research Team integrates threat data from the Open Threat Exchange (OTX) community into the threat intelligence updates they deliver to USM, providing additional context to the IDS engine.



Throughput

Overview

The next thing to understand about your IDS solution is throughput. Throughput is the maximum amount of traffic that can be successfully processed in one second by the network IDS. Your NIDS must be able to keep up with your network traffic. This will largely depend upon your network requirements. Every organization has different bandwidth needs. Typically, the range of 100 Mbps to 1 Gbps is sufficient for most networks. (It is important to remember that networks are full duplex, meaning a 100 Mbps link can generate 200 Mbps of traffic.)

Note that performance is a significant concern for IDS deployments. Many NIDS implementations tend to drop packets due to the high throughput of today's high bandwidth network devices. Therefore, you must determine where you will put the network IDS, and how much bandwidth you'll need.

Solution Recommendations

Determine your network requirements (i.e. understand what applications you are running, how much bandwidth each application is using, how many users your network is supporting, etc.) and select a NIDS solution that can keep up with your network traffic.

AlienVault USM Capabilities

AlienVault USM provides enough throughput for most typical organizations. Organizations with high throughput environments can easily install multiple sensors to limit traffic and maintain steady performance.

Protocol analysis

Overview

The next thing to evaluate in your IDS solution is the level of protocol analysis that it performs. In protocol analysis, the network IDS examines Transmission Control Protocol (TCP) and User Diagram Protocol (UDP) payloads, which contain other protocols such as DNS, FTP, HTTP, and SMTP (i.e. the Layer 7 applications). As an example, threats can be transmitted through legitimate DNS traffic, which isn't normally inspected or blocked. The IDS understands how these protocols are supposed to work, and can fully decode and interpret the protocols to detect threats using signatures.

This process allows a much larger range of signatures to be created than would be possible through more basic signature techniques.

Solution Recommendations

Make sure your IDS solution does robust protocol analysis, including application layer decoding of HTTP, FTP, SMTP, SSL, SSH, and DNS protocols.

AlienVault USM Capabilities

AlienVault USM performs protocol analysis to deliver an extensive range of signatures.

Aggregation

Overview

IDS systems generate an enormous amount of data, including scores of alerts and events based upon the signatures in the system. Often there are duplicative events from various systems, and other alerts that could be characterized as noise. This is a major pain point for all organizations – you get flooded with alerts. This can also lead to inadvisable workarounds, including restricting or turning off the signatures altogether. These workarounds are not advisable for multiple reasons. First, an attack may in fact be happening, and you need to be able to properly identify it. In addition, you will lose capabilities that are needed for reporting purposes.

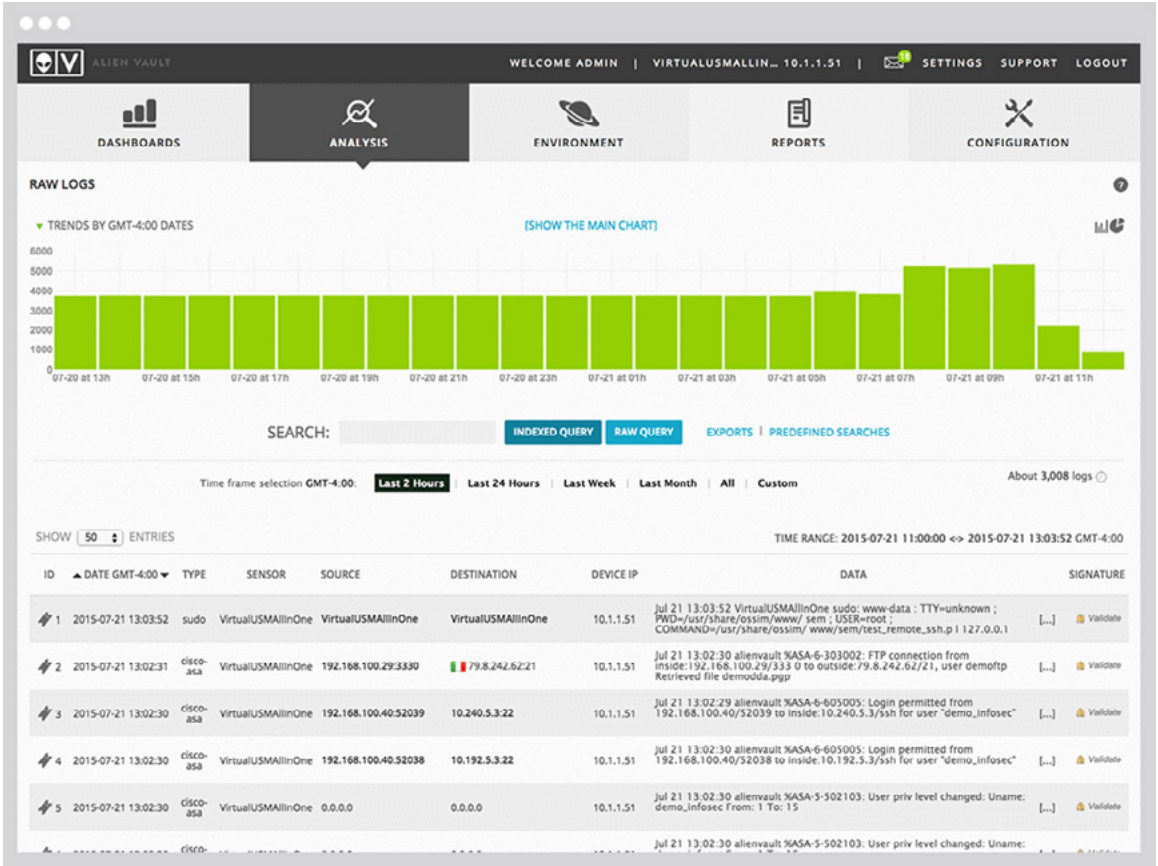
The optimal way to deal with this pain point is to use an IDS solution that has aggregation capabilities. Aggregation, the ability to combine events into one alert, is critical to help you focus your efforts on detecting actual threats. You need to be able to correlate the output of several systems and give your security operators a condensed view of the reported security issues.

Solution Recommendations

Select an IDS solution that has aggregation capabilities.

AlienVault USM Capabilities:

AlienVault USM delivers cutting edge aggregation functionality. It accomplishes this with its strong correlation engine, which links together disparate events from IDS and other built-in security controls to consolidate event data and turn the data into useful information. In addition, the correlation directives that are delivered by the AlienVault Labs Security Research Team ensure that every alert generated is meaningful and actionable.



Integration

Overview

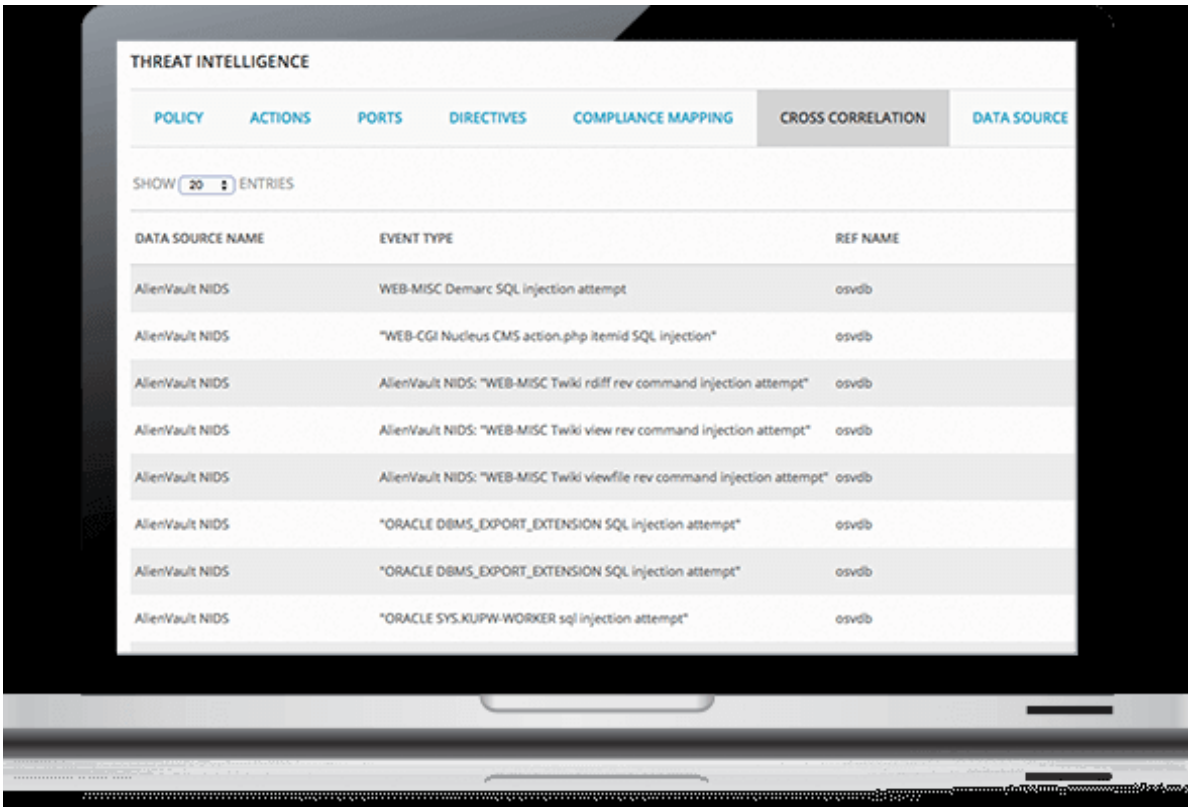
As critical as IDS is to your security program, one security tool is not sufficient. Most companies have multiple security tools to achieve effective threat detection and response. To get the most out of your IDS, it needs to be integrated with other security tools. This means that it needs to have the capability to send and receive alert data to and from other data sources so that you achieve better context and correlation of threat data and better prioritization of alerts.

Solution Recommendations

Choose an IDS solution that has strong integration capabilities.

AlienVault USM Capabilities

AlienVault USM was built to integrate data with other platforms and deliver exceptional correlation capabilities. It is an intuitive, comprehensive security platform that integrates seamlessly with external security tools, in addition to the built-in integration of IDS with asset discovery, vulnerability assessment, behavioral monitoring, and SIEM capabilities. With AlienVault USM, you'll have the ability to incorporate data from third-party technologies and devices to better correlate activity within your environments and identify malicious activity. This data feeds into AlienVault USM's correlation engine to greatly enhance threat detection and response capabilities.



Contextual Enhancement

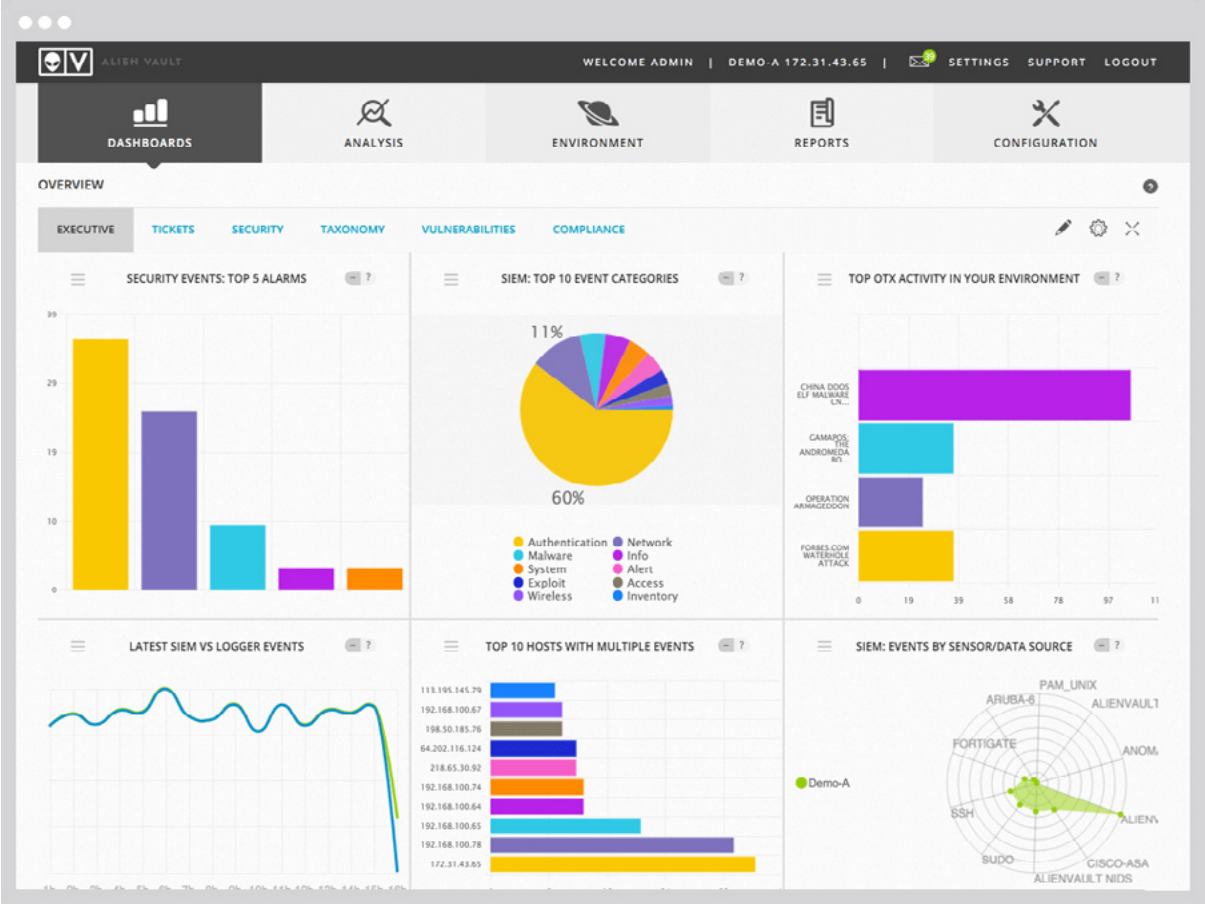
Overview

An IDS on its own can only do so much; IDS data needs to be supplemented with additional data about the network, cloud services, applications, devices, and users to be truly meaningful. The way to do this is with context. Putting threats in context is essential for a truly effective IDS solution. This requires correlating information from a range of sources, including information from internal sources such as network IDS, host IDS, cloud IDS, system logs, and firewall logs, as well as from external sources. This correlation capability is a must-have for a successful security program.

An effective IDS system also needs to feed into a security information and event management (SIEM) solution. SIEM software is designed to import information from various security-related logs, including those from IDS, vulnerability assessment, and asset management tools, and correlate events among them. Integration with SIEM provides additional needed context for your alerts.

Solution Recommendations

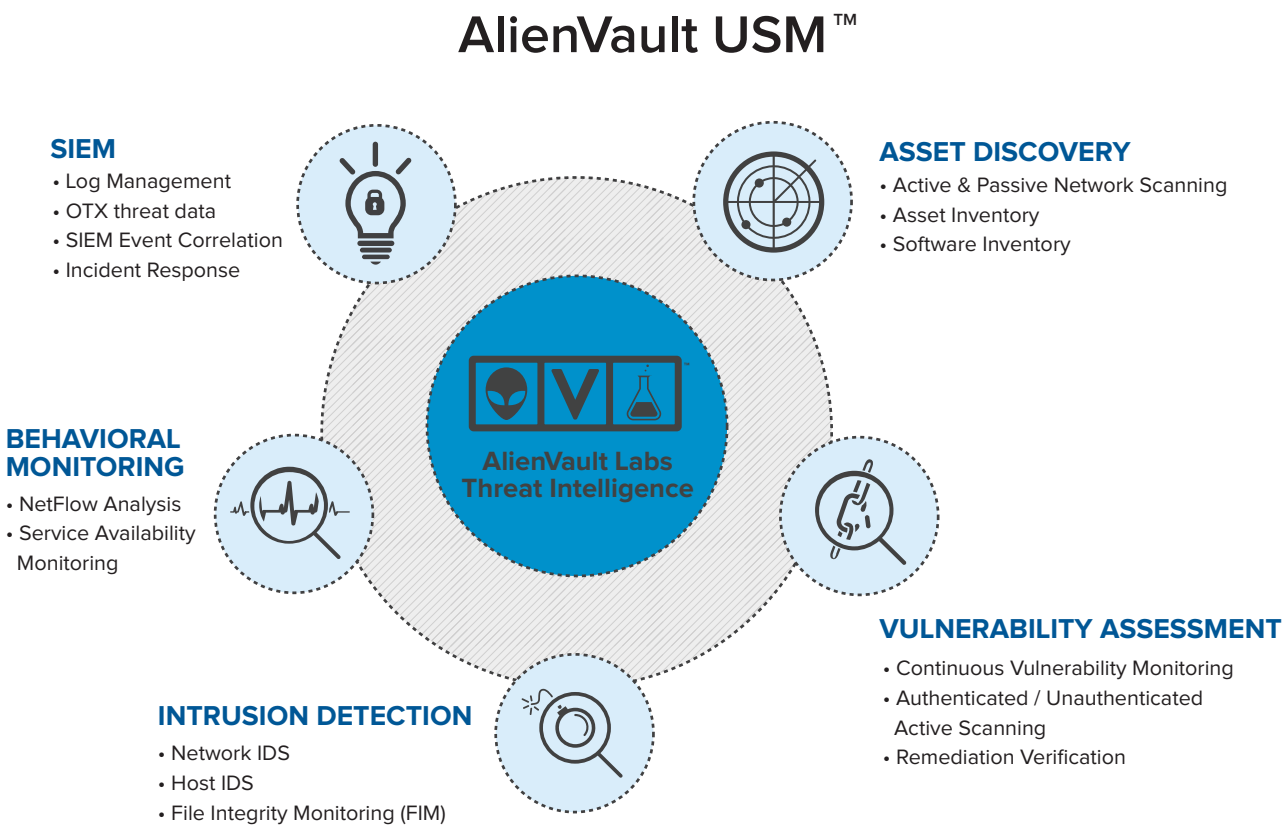
You need to select an IDS solution with the ability to deliver supplemental data to provide additional context to the alerts. This will improve the efficiency and effectiveness of your threat detection capabilities.



AlienVault USM Capabilities

AlienVault USM delivers essential security capabilities on top of its IDS in a single platform. The IDS functionality is integrated with asset discovery, vulnerability assessment, and behavioral monitoring in a native SIEM solution to provide critical context. The AlienVault Labs Security Research Team provides additional context to your alerts by delivering continuous threat intelligence updates to your USM deployment. The Security Research team uses OTX threat data to inform their own research, meaning that insights drawn from the latest in-the-wild attacks contributed by 53,000 participants around the world are built directly into your security plan.

These continuous updates from the Security Research Team are delivered in the form of eight coordinated rulesets, such as new correlation rules, IDS signatures, and remediation templates, which enable AlienVault USM to analyze the mountain of event data from all your data sources. Pre-built correlation directives link events to identify threats targeting your environments, eliminating the need for you to spend hours creating your own. The USM platform delivers a prioritized assessment of the threats targeting your environments, telling you the most important threats to focus on right now, and provides guidance on how to respond to those threats



Summary

Intrusion Detection Systems are one of the most effective security controls available today, particularly when IDS data can be correlated with asset information, vulnerability data, and threat intelligence to provide valuable context and prioritization of alarms. Using the information in the guide above, you'll be able to effectively assess the capabilities of the many IDS tools available and find the solution that best fits your needs.

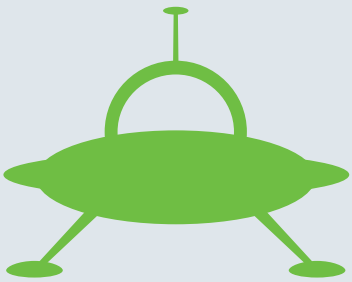
AlienVault Unified Security Management Overview

AlienVault's Unified Security Management (USM) platform provides a fast and cost-effective way for organizations with limited security staff and budget to address compliance and threat management needs. With all the essential security controls built-in, AlienVault USM puts complete security visibility within fast and easy reach of smaller security teams who need to do more with less.

AlienVault USM provides five essential security capabilities that provide the technology you need.

USM integrates threat intelligence from the AlienVault Labs Security Research Team and the Open Threat Exchange (OTX), which eliminates the need for IT teams to spend precious time conducting their own research on emerging threats. The Security Research Team spends countless hours mapping out the different types of attacks, the latest threats, suspicious behavior, vulnerabilities and exploits uncovered across the entire threat landscape. The team produces actionable threat intelligence, which is information about malicious actors, their tools, infrastructure and methods, which is continuously built into the USM platform through threat intelligence updates.

The Security Research Team informs their own research with threat data from AlienVault OTX, the world's first truly open threat intelligence community that enables collaborative defense with actionable, community-powered threat data. With 53,000 participants from 140 countries around the world sharing 10 million threat indicators every day, OTX provides global insight into attack trends and bad actors. Because OTX threat data represents the latest in-the-wild attacks from a wide variety of industries, countries, and organization sizes, the Security Research Team is able to deliver threat intelligence updates that reflect the broadest possible view of attacker techniques, ensuring that your USM deployment is always equipped to detect emerging threats.



About AlienVault

AlienVault has simplified the way organizations detect and respond to today's ever evolving threat landscape. Our unique and **award-winning approach**, trusted by **thousands of customers**, combines the essential security controls of our all-in-one platform, AlienVault **Unified Security Management**, with the power of AlienVault's **Open Threat Exchange**, the world's largest crowd-sourced threat intelligence community, making effective and affordable threat detection attainable for resource-constrained IT teams. AlienVault is a privately held company headquartered in Silicon Valley and backed by Trident Capital, Kleiner Perkins Caufield & Byers, Institutional Venture Partners, GGV Capital, Intel Capital, Jackson Square Ventures, Adara Venture Partners, Top Tier Capital and Correlation Ventures.