# Enterprise Security Made Easy

## Exposing the secrets of the world's most secure networks


IAN WHITING
CEO | Titania

NICOLA WHITING
COO | Titania

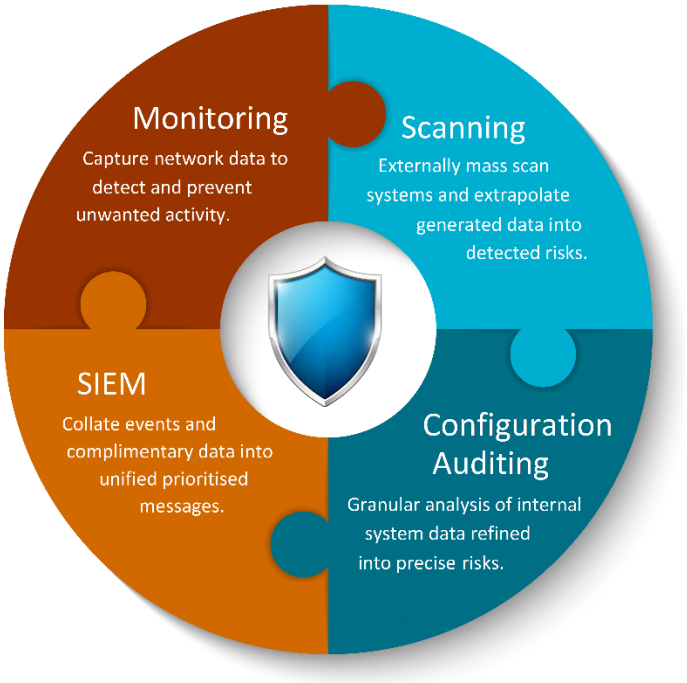
# Table of Contents

Executive Overview ..... 3
Disclaimers ..... 4
Not Covered ..... 4
Monitoring ..... 5
Summary ..... 5
Capabilities ..... 5
Technical Insights ..... 6
Performance ..... 7
Tools ..... 7
Scanning ..... 8
Summary ..... 8
Capabilities ..... 8
Technical Insights ..... 9
Performance ..... 11
Tools ..... 11
Configuration Auditing ..... 12
Summary ..... 12
Capabilities ..... 12
Technical Insights ..... 13
Performance ..... 15
Tools ..... 16
SIEM Systems ..... 17
Summary ..... 17
Capabilities ..... 18
Tools ..... 18
Conclusions ..... 19
Questions Answered ..... 19
Why is it best to avoid agent-based systems? ..... 20
How does scanning and configuration auditing differ? ..... 21
My scanner has configuration auditing, why do I need a separate tool? ..... 21
Why should I audit continually? ..... 20
Acronyms ..... 22
Product Overviews ..... 23
Author Biographies ..... 24

# Executive Overview

The world's most secure networks leverage the combined strengths of multiple technologies. Their goal is to use a multi-layered approach, to create a combined solution which is stronger and more resilient than its individual components.

This document discusses each of the four key technologies, providing both summary information and the detail behind each capability, its limitations and contributing strengths.




There are four key technologies; monitoring, scanning, configuration auditing and SIEM.

Each technology is architecturally designed for *one* specific expertise area. The complementary technologies each have a strength that none of the others can adequately provide.

- **Monitoring** – Live Activity Detection
- **Scanning** – Network Discovery
- **Configuration Auditing** – Granular Accuracy
- **SIEM Systems** – Collating the Big Picture

**Monitoring:** Provides a "Live View" of current activity on your security systems. For simplicity, monitoring includes any technology that sits on your network and monitors systems or network activity. This includes email gateways, web filtering, IPS and firewalls. Monitoring systems shine at detecting active attacks or malicious activity.

**Scanners**: Provide a "Helicopter View" of security systems. They lead with discovering what is on your network and normally provide *externally based* security insights via *generative security data*. (They interrogate, attack or exploit systems to generate security data, which they then analyse and extrapolate into meaningful results).

**Configuration Auditing:** Provides a "Granular View" of security systems. They analyze *internal* system information *already present* on your network devices, *refining* mass configuration and operating system data into precise risks and remediation actions. Granular "line by line" analysis (delivered at scale) and virtual modelling technology builds human understanding into how device settings interact with each other, giving a more accurate picture of security and compliance risks.

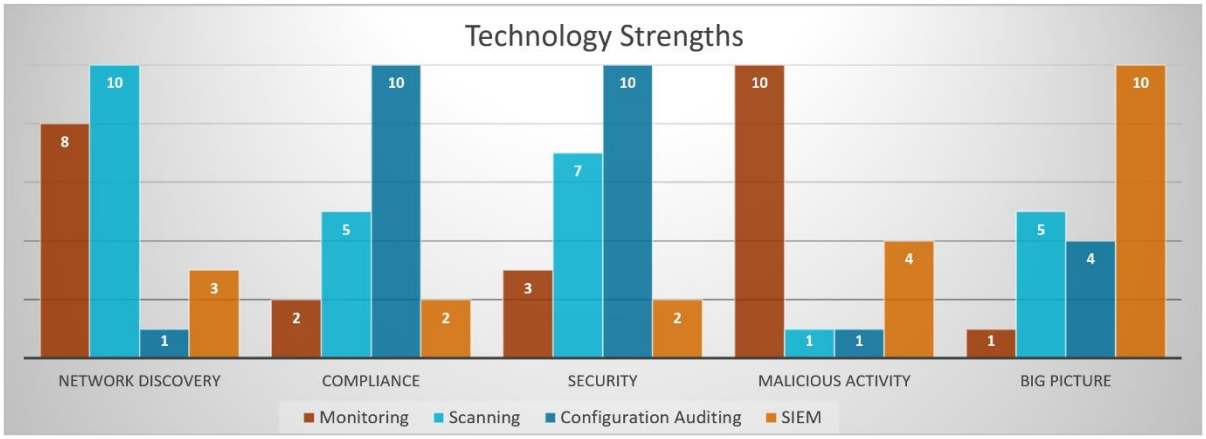
**SIEM solutions**: Provide the "Executive Summary" of your current security risks by refining key information from different technologies & data sources together into a unified "big picture".

They are particularly beneficial for large enterprises as they provide a way of viewing security, risk and compliance issues from levels of data that could otherwise be overwhelming.

Future SIEM solutions may provide the interface for autonomous mitigation solutions - the next generation of network defence systems, predicted to be "self-healing".

## Technology Strengths

Multi-layered defences leverage technology strengths to create a combined solution, stronger and more resilient than its individual components. To be effective this solution requires two complementary security perspectives – the "helicopter view" produced by scanning technology, balanced by the "granular view" of monitoring and configuration auditing.




Each technology is explained in more detail later in this document.

## Disclaimers

As we are discussing the "most secure" networks in the world we will talk about the most applicable technologies in each area. This document will include *advanced* monitoring & scanning tools, *intelligent* configuration auditing systems and *market leading* SIEM solutions.

For reference there are two types of configuration auditing technologies:

- "find and match" text string analysis (grep) tools and
- solutions with built-in AI / virtual modelling intelligence.

As "grep" configuration auditing is prone to false positives and negatives this document focuses on configuration auditing solutions with enhanced process automation, built-in intelligence engines and natural language processing capabilities.

## Not Covered

Although building a secure intelligent architecture is essential, technology alone will not create a secure network – there are other vital components. Industry best practices, user training, behavioural analytics, polices, procedures and compliance standards are not covered in this document, but should be additionally incorporated into your security ecosystem and practices.

# Monitoring

## Summary

Monitoring in its simplest form is to listen to all communications to and from networked devices. By passively listening to the network traffic you can determine a lot of information about the network and systems, including some security issues. Monitoring is like sitting on a bench opposite a building and noting all its security controls such as: visitor access, security checks, CCTV cameras and the working patterns of personnel.

Just like the analogy above, there is a limit to the information that you can gather by monitoring alone. However, you may be able to detect and prevent an attack in progress, or in the case of a gateway, filter the content allowed through.

The strength of monitoring and gateways is to provide visibility of live events on your network, allowing you to filter content and prevent unwanted access.

- NON-DISRUPTIVE
  With the exception of gateway devices, monitoring does not send network traffic to other systems.
- ACCURATE
  Information gathered is derived from network packets sent from the devices, so little guess work is involved.
- LIVE PROTECTION
  Identify and protect against attacks as they happen.
- LIMITED COVERAGE
  Monitoring can only audit what it has visibility of, therefore the extent of what it can audit is restrictive.

## Capabilities

For ease of classification, both detection and gateway types of device are grouped together in this section. These are available as a single combined multifunctional device.

- Gateways (firewall, email or web) provide key security functionality by monitoring and filtering network traffic between different network classifications. This could be between the Internet and your organization's internal network, or between internal network boundaries.
- Monitoring systems (network, IPS or AV) provide detection of potentially harmful activity, such as malicious hackers, ransomware or other malware.

In addition to providing a barrier between networks, gateways often contain sophisticated policy rules. For example, an email gateway can provide content analysis to help prevent data leaking from one classification of network to another. Web gateways can provide access restrictions preventing users from browsing to sites known to contain malware, or non-business-related content.

The capabilities of network monitoring systems range from simple network activity detections through to sophisticated behaviour analysis. The accuracy of the detections from these systems tends to be high since they are analysing real data and behaviour detection tends to be good.

Although monitoring systems can detect potential security issues based on the network traffic that they are able to see and dissect, their network visibility limits their auditing capabilities.

*TIP*
Monitoring systems can detect network scans as an attack. You may be able to avoid this by configuring your monitoring system to ignore scans originating from your scanner. If you don't, you may be inundated with alerts and your audit scans could be blocked.

*TIP*
Monitoring systems will often have a malicious behaviour analysis feature. Vulnerability scans test for issues by exploiting services, so they are likely to trigger this feature. It is not always possible to exclude specific systems as it is often an "off" or "on" setting. It is not a good idea to switch it off permanently, but you may need to switch it off to enable vulnerability scanners to work effectively. (If you get lots of alerts from your monitoring systems, you can plan to filter them).

## Technical Insights

A lot of information can be gathered just by connecting to a network and listening to the traffic that is sent between systems:

- Detection of potential attacks in progress, by examining network activity and behaviour that is typical for hackers or ransomware.
- Information broadcasts (e.g. LLDP and CDP) including system names, domain information, software versions, model information, addresses, device capabilities and more.
  All useful intelligence for a security auditor - or an attacker.
- Routing updates (such as RIP and BGP) can include information about the structure of your network. Gateway addresses, subnets and other details can be used by an attacker for putting together a picture of how everything is connected.
- Time synchronization updates are also useful for an attacker, as a number of network services are dependent on time being consistent, for all devices on that network.
- Switching protocols (such as VTP, DTP, STP and RSTP) provide information on the configuration of the network and VLANs.
- Other protocols (such as NBNS, DHCP and Gratuitous ARP) will also provide additional information.

Gateway functionality can be found integrated into modern multi-function firewall devices as well as in standalone and virtual appliances. Choosing between them will in most part be dictated by the requirements of your environment and the throughput required for processing the data.

*TIP*
To capture more network traffic, switches can often be configured to set individual ports to "monitor" or "mirror" mode. This mode causes the network switch to send all, or some, additional network traffic to the port for diagnostic, monitoring and detection purposes. Be aware that this mode normally causes the configured port to become read-only.

## Performance

Network traffic is a passive activity; you will only see network packets when the sender transmits them. Some protocols send regular updates, such as LLDP, DTP and STP, whilst others only send data when there is something to send. The performance of the monitoring system will greatly depend on the quantity of data and complexity of analysis.

The volume of data, policy rules, specification of the physical device and the amount of capabilities enabled will all have an impact on a gateway's performance. When scaling gateway systems and planning for the future, it may be easier to assess them as separate capabilities being provided by different appliances.

## Tools

There are a huge range of appliances available to choose from. To create the most secure environment you should, as a minimum, plan to have firewall, email gateway, web gateway and Intrusion Prevention System (IPS) capabilities. Best practice suggests having multiple devices from different vendors, just to ensure that nothing is missed.

Network monitoring, detection and prevention features can typically be found on the following types of network appliances.


Some appliances may have the capability to provide Data Loss Prevention (DLP), where the appliance provides an analysis of the network traffic in order to prevent sensitive data from being transferred. For example, if sensitive documents were marked in a particular way, you could configure DLP to detect that marking and either prevent documents from passing through or require authorization.

> *TIP*
> Wireshark is a very popular Open Source standalone network monitoring tool. It is really useful for diagnostic purposes and breaks down any captured network traffic to its component parts. It will give you a good idea of the type of traffic travelling over your network and has capabilities to re-construct data streams and save data for later analysis.

# Scanning

## Summary

Scanning is the process of actively generating and sending large quantities of network traffic (to one or more systems) then extrapolating information from the returned responses. Scanning can be broken down into two different scan types:

- network scanning is used to identify active hosts and services. This is performed by sending specially crafted network packets to different network addresses and ports. The response, or lack of, is then used to determine what hosts and services may be available on the network;
- vulnerability scanning is used to help identify potentially vulnerable services and hosts. This is performed by sending specially crafted network packets to services. The network packets are designed to exploit, or trigger a behaviour in the service. If the service then responds in a way that indicates the exploitation was successful, it is reported as a vulnerable service. Sometimes the exploited service is further used to gain additional information from the vulnerable system.

Scanners should be used for network discovery purposes - identifying systems, services and the networks that they are connected to. Vulnerability scanning should only be used if system availability is not critical and even then, only run with safe mode enabled.

**DISCOVERY**
Network scanning is a great way of identifying active systems, services and networks.

**NO SYSTEM UNDERSTANDING NECESSARY**
As long as networked systems offer standard services and communicate over standard protocols, they can all be scanned.

**DISRUPTIVE**
Scanning is a very active form of auditing. Sending out lots of network packets, queries and exploiting vulnerabilities can cause significant network disruption.

**TIME INTENSIVE**
Scanning a network can be time intensive, especially when network filtering is configured. The time can also be extended by intelligent systems actively disrupting what they will see as an attack.

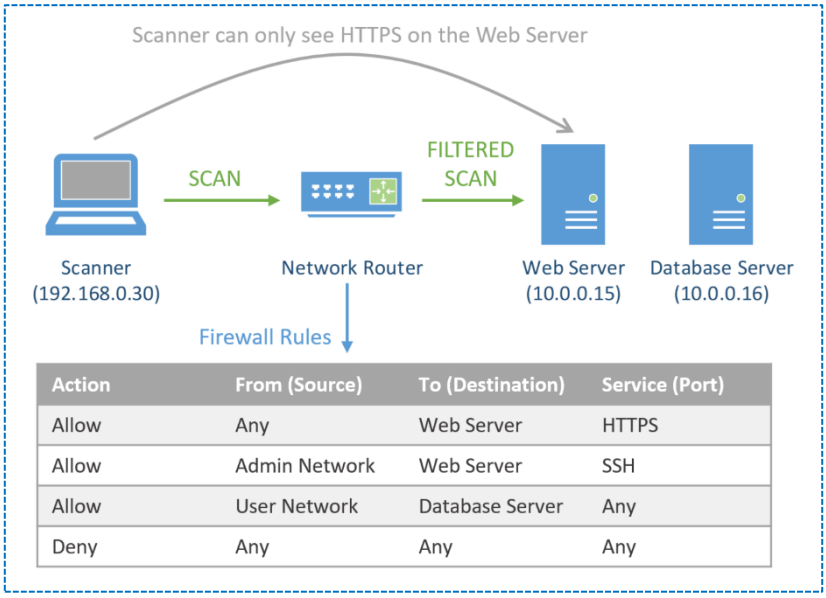
## Capabilities

Network scanning is a great way of detecting the presence of active systems, devices and networks. When combined with a vulnerability scan, it provides good visibility of what services are available on the network and the potential vulnerabilities in those systems. Scanners don't need to be able to understand the platform that they are scanning, as long as the services respond in a standard way.

> *TIP*
> It is worth noting that scanners report on things that respond to them. A lack of response will make the scanner assume that nothing is there. In the real world, network filtering and detection systems on modern network switches, routers, firewalls and packet shapers may block your scans. So you need to be aware that your scans may not reach all of your network devices.

Scanners are great at highlighting if you have network segmentation issues. The world's most secure networks segment them into subnets containing similar systems. Network filtering is then used to restrict access between those segments. Segmentation helps with network security and can also improve network performance.

Scanners are not practical for auditing network filtering, so would be supplemented by intelligent configuration analysis solutions, such as Nipper Studio. A scanner is only able to audit filter rules from its own address. In the example shown below, the scanner would not be able to determine that the database server existed (or that it is completely open to the user network).




| Action | From (Source) | To (Destination) | Service (Port) |
|---|---|---|---|
| Allow | Any | Web Server | HTTPS |
| Allow | Admin Network | Web Server | SSH |
| Allow | User Network | Database Server | Any |
| Deny | Any | Any | Any |

It is also difficult for a scanner to determine whether firewall rules have been applied directly on a scanned system, or an intermediary device. If a scan is being dropped, then there is no response for the scanner to analyse. Intelligent configuration auditing tools, would again provide the data required.

> *TIP*
> Vulnerability scanners typically determine if vulnerabilities exist in a network services by sending exploit codes to those services. Vulnerabilities are not part of a network services designed behaviour and can therefore disrupt or create issues with that service. It is not uncommon for vulnerable services to become unstable, temporarily unavailable or permanently unavailable. If you are auditing a live network, you should enable your scanner for “safe checks only”.

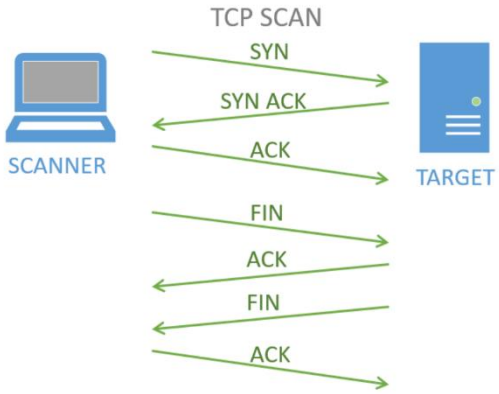
## Technical Insights

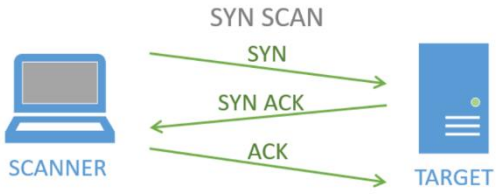
There are different methods for scanning Internet Protocol (IP) services running over Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). TCP is connection based protocol, requiring two communicating hosts to perform a conversation to establish a connection between them. The IEEE IP standard describes precisely what network packets are expected between two hosts connecting via TCP and what the responses should be.

UDP, being a connectionless protocol, only defines the structures required to communicate. A UDP service does not necessarily require a prior establishment of communications.

Both TCP and UDP provide 65535 ports each, from which services can be offered by a networked host. There are also other IP protocols, such as Internet Control Message Protocol (ICMP), that scanners can also probe.

There are two main scan types used by scanners when performing TCP scans. A TCP (connect) scan is the safest method as it follows the IEEE standard method of creating a connection. However, a SYN (half open) scan is the most popular default. It generates less network traffic and does not create an open a connection. The downside of a SYN scan is that because it doesn't follow through to open up a connection it can cause issues on some systems. SYN scanning will typically require administrative permissions to construct custom IP packets.




| | TCP Scan | SYN Scan |
|---|---|---|
| Open Ports | 7 Packets | 3 Packets |
| Closed Ports | 2 Packets | 2 Packets |
| Filtered Ports | 1 Packet | 1 Packet |

There are two main techniques that scanners will use to gain more information about the hosts and services. If the scanner detected the service using a SYN scan method, then it will have to reconnect to it using a standard TCP open. The first technique is to examine the information returned to the scanner when connecting to the service. A lot of services return information in the connection banner, e.g. SSH services return some version information. The second technique is to send triggers to the service in order to query it for more information, e.g. determining HTTP options for a web service.

Typically, service specific triggers are sent by scanners to the standard service ports in order to determine what type of service may be listening on a given port. This involves sending more triggers / queries to the service.

There are several different methods that vulnerability scanners use to identify potential vulnerabilities in services:

- sending the same types of exploit code or triggers to a service, that an attacker would use, in order to determine if the service is vulnerable. If the service is exploited, it is reported as vulnerable;
- examination of service banner messages, version numbers and other returned data to attempt to determine if the service is likely to be vulnerable or contain a security issue;
- performing an analysis of the information returned and extrapolating if a security issue is likely to exist.

## Performance

A system with 8 open services and no network filtering, a full TCP port scan would generate 131,110 network packets. For a full SYN scan there would be slightly less network packets, at 131,078. To expand that example to a relatively small network. Assuming that there are only 100 active systems on a class C network, also with 8 open services and no network filtering. There would now be 23,203,544 packets for the TCP scan and 23,200,344 packets for the SYN scan.

If a vulnerability scan were to be performed, then there would be significantly more network packets transmitted over the network. If other protocols, such as UDP, were also to be tested, then there would be more network packets again.

If there is no network filtering configured then scan results can be quick with vulnerability scans taking a little longer. Typically scans of multiple systems happen in parallel, helping to reduce the time taken to audit entire networks at the expense of the immediate network bandwidth. If network filtering were to be configured then, although there would be far less network packets transmitted, the scans would take much longer as the scanner would be waiting for a response from the target system.

> *TIP*
> Most scanners do not perform full TCP or UDP port scans by default. If you want to perform full TCP or UDP audits you will need to modify the scanners default options.

## Tools

The most popular Open Source tool used to perform network scanning is NMAP. It has an extensive range of options and scan types. It also has simple host and service type detection, based both on responses and triggers sent to the services. The standard tool does not include scheduling or integration with SIEM systems, but given the flexibility of the tool you could add those manually.

Nessus is one of the most popular commercial vulnerability scanners. It is feature rich with many scan options, including scheduling and integration. It also has safe mode and re-scan features. (Re-scanning systems at the end of an audit is useful to establish what services and systems have become unresponsive). Nessus has an added element of configuration auditing but it uses entry level, “find and match” text string analysis (grep) technology - prone to false positives and negatives

> *TIP*
> Always investigate what services and systems may have become unresponsive after scanning. Even if the loss of a service is not immediately noticed, its loss may cause other unforeseen issues.

> *TIP*
> Unless you have a reason not to, always use safe mode in your vulnerability scanner. It will cause them to audit a smaller number of issues but will greatly increase the chance that systems and services will remain stable.

# Configuration Auditing

## Summary

Configuration auditing is sometimes referred to as a *build review* by penetration testers. It involves a "line by line" granular assessment of the *internal system instructions* (configuration or O/S) of a physical or virtual device. As these instruction sets determine a system's *actual* security response it is regarded as the least intrusive, most accurate and detailed way of determining the systems security and compliance status.

For reference there are two types of configuration auditing technologies:

- "find and match" text string analysis (grep) tools and
- solutions with built in AI / virtual modelling intelligence.

As "grep" configuration auditing is prone to false positives and negatives we focus on solutions with enhanced process automation, built-in intelligence engines and advanced language processing. They provide the appropriate accuracy for current SIEM solutions and the future capabilities needed for fully autonomous vulnerability discovery and mitigation.

The strength of configuration auditing is in its flexibility, accuracy and depth of detail. Internal systems data (e.g. configuration options, installed software, services etc) provides factual information that you rely on. Autonomous audits can be performed by connecting over the network to the systems (online) or reading in configuration backups (offline) – you can support air-gapped, remote or supply chain systems with the same solutions.

**ACCURATE**
Auditing actual settings, software and options creates precise findings.

**COVERAGE**
Direct access to a system enables the most complete audit coverage.

**NON-DISRUPTIVE**
Audits using standard administrative interfaces limits disruption. Offline auditing produces no network traffic.

**FAST**
Auditing is quick in all scenarios.

**PLATFORM SUPPORT**
Configuration auditing tools have to be programmed to support the platforms being audited. Although all mainstream platforms are supported, support for fringe systems may not be defined.

## Capabilities

Configuration auditing provides granular detail and a wide depth of knowledge. It supports a diverse range of both physical and virtual network devices. These include: servers, routers, firewalls, network switches, workstations and printers. Advanced tools may also audit enterprise applications, databases and bespoke systems.

The configuration auditing process used to be performed manually by auditors either logging in to each individual system, or using a backup configuration, and going through system options "line by line". These processes generated accurate information, but were slow and required specialist skills.

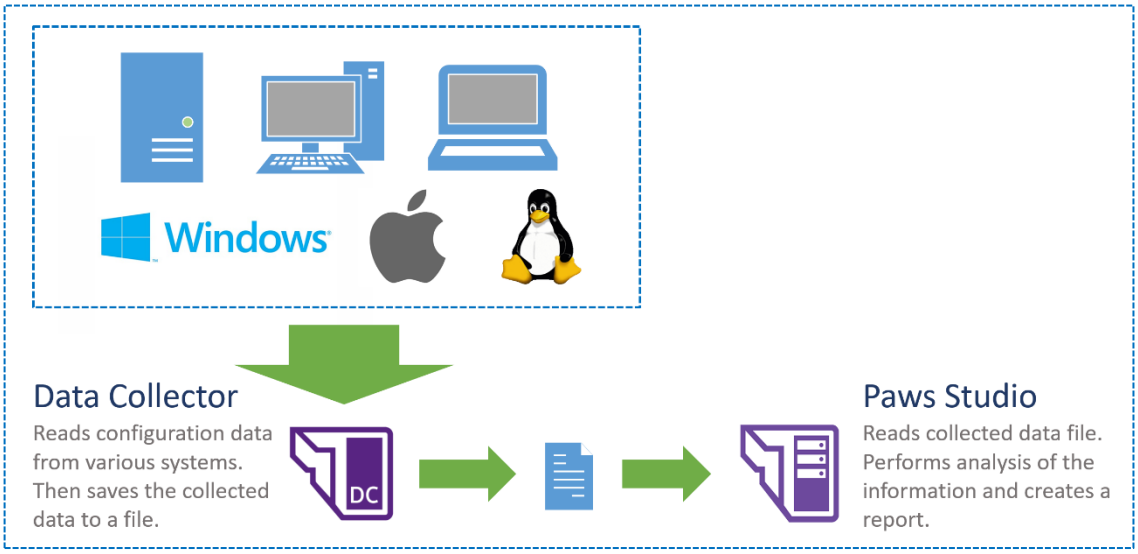
Configuration auditing tools, such as Nipper Studio, automate these manual processes but maintain the auditors expertise. Nipper builds a virtual model of each device, then uses an intelligence engine to understand the interactions between different configuration options, the effect of default settings and their impact on security & compliance. It helps eliminate human inconsistencies and errors.

> *TIP*
> Configuration auditing features added to other types of tools, such as scanners, are not sophisticated enough to accurately assess security and compliance issues. They perform searches to match patterns (grep) when identifying issues. Because they lack a basic understanding of how devices work, this approach often leads to false positives or false negatives.

In addition to compliance and security audits, configuration auditing software will also be able to create configuration reports and analysis. For example, Nipper can analyse firewall rules to identify unused rules and objects, rules that say the same thing or rules that contradict each other. You can also analyse access to and from specific systems, or alignment against your company's policies.

Advanced system configuration auditing tools, such as Paws, enable you to also audit bespoke or custom applications. By enabling the audit to create their own policy checks, it is quick and easy to add additional tests for systems – even those purpose built for a specific environment.

Offline auditing also provides for a great way to assess isolated systems or your supply chain without requiring direct access to them. For network devices this could be auditing device backups. For operating systems, Paws Studio offers a unique offline capability through its data collection tool.




## Technical Insights

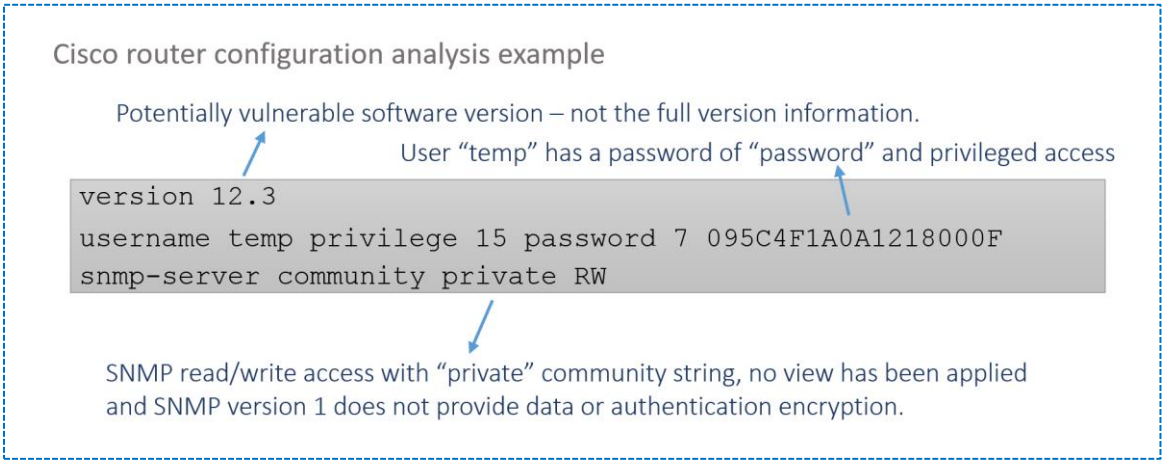
Configuration auditing used to be performed manually by auditors, sometimes with the help of scripts, sometimes with a check list. It used to be a very time intensive activity before automation came along, and it is still manual on less common platforms.

When manually assessing configurations, the auditor would need to have an understanding of the platform they were auditing. It was also not uncommon for auditors to have PDF manuals for the devices that they were assessing. This would enable them to lookup command syntax as they progress through the configurations line by line.

*TIP*

If you are going to manually audit a device, such as a Cisco router, don't forget that system defaults are not usually shown. The defaults may also change depending on the software version. So, if you are auditing the configurations line by line, be aware that you also need to audit what is not shown. Experienced auditors with intimate knowledge of the devices they are assessing will be aware of system defaults. Nipper Studio will automatically do this for you.

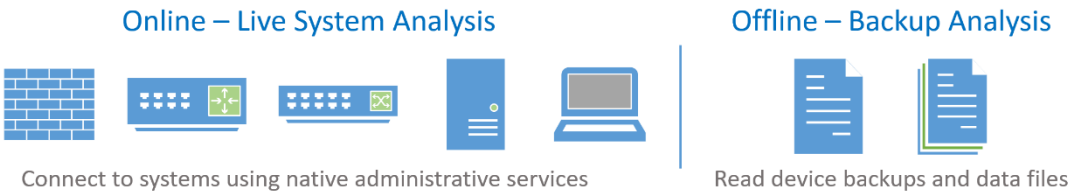
The following example shows only 3 lines from what could be a 200 line Cisco router configuration. It highlights some issues which may be found during a manual audit. Although there are only 3 lines, there are 6 security issues, including some very serious risks. Configuration auditing tools can perform these kind of detailed audits in seconds.




The information you can assess using configuration auditing includes:

- Software (what is installed, versions, is it supported, are automatic updates enabled etc);
- Services (administrative services enabled, how they are configured, are they encrypted, how strong is the encryption, what access do they give, is there any filtering etc);
- Protocols (what protocols are configured, how are they configured, are they authenticated, are they encrypted, how strong is the encryption, what versions are used etc);
- Platform basics (is time synchronization configured, is it authenticated, what authentication is used, are certificates valid, are there logon banners, what do the banners say etc);
- Networking (what interfaces are enabled, is there network filtering configured, are there any weaknesses in the filtering, what network protocols are used, is port security enabled, what authentication is configured etc);
- Permissions (what file permissions exist, who has system access, user authorization etc);
- Applications (what is installed, how they are configured, their authentication etc).

Windows system configuration information is stored across a lot of different components. Configuration auditing tools, such as Paws Studio, will perform various API calls, registry queries, WMI queries, policy examinations, user queries etc. The same is true for Apple Mac and GNU/Linux systems where configuration information is saved in multiple locations.



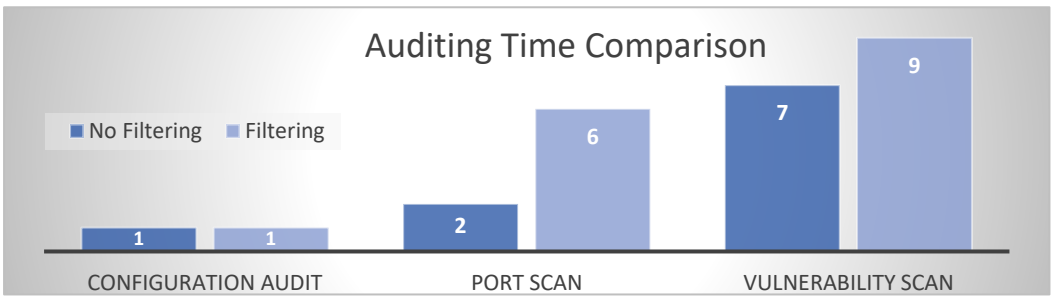

Offline (or backup) auditing has been available for some time now for network devices using tools such as Nipper Studio. This is where a saved copy of the network devices configuration (usually a text or XML file) is read instead of using a live connection to the device. The advantage is that devices can be audited with absolutely no network traffic or interaction with the audited system. This provides the ultimate in non-disruptive auditing capabilities, whilst still maintaining all detail.

Offline auditing of operating systems (such as auditing from Windows backups), may have required large impractical data dumps. However, Paws provides an intelligent solution to this problem - it separates the audit data collection from the analysis and reporting. The data collection tool is able to run separately on the system that you want to audit, without having to install anything or add requirements such as .Net or Java. It collects only the required data and saves it to an encoded file, for transfer to the analysis and reporting system. This provides fully automated and customizable auditing of disconnected and isolated systems.

Online auditing of systems is typically achieved using standard administrative protocols, such as SSH. Therefore, alerts on monitoring systems are unlikely to be triggered by an audit. Additionally, network filtering devices will not need to be reconfigured to permit audits. This means that whilst configuration auditing is the most detailed and accurate auditing technology, it is non-disruptive.

## Performance

The network traffic generated for an audit will range from nothing (for offline auditing) through to standard administrative levels of traffic (for online auditing). Speed is also a factor.




Configuration auditing doesn't have to wait for network responses, so is generally the fastest form of auditing. Simple port scans do not generate many queries, so is also relatively quick (though information returned is limited). Vulnerability scans are significantly slower due to the number of network packets sent. If network filtering is enabled, it will prevent scanning queries being returned, this introduces significant delay (as the scanner awaits a response before timing out).

Offline configuration auditing performance is seriously impressive. Just like with network scanners, audits of larger networks are completed in parallel to improve the audit time. Nipper Studio sets the benchmark for offline configuration auditing. A full best practice security audit of 200 Cisco switch configurations can completed on a 2014 Intel core i5 with 8GB of memory in just over 2.3 seconds.

## Tools

The leading configuration auditing tool for network devices is Nipper Studio, providing best practice security audits, compliance reports, scheduling, good device support and integration with SIEM systems. Paws Studio and Nessus both provide excellent operating system auditing capabilities. However, Paws offers greater flexibility by including the ability to audit systems offline, adds advanced database support and includes customizable policies.

When selecting the right tool to use for configuration auditing there are a couple of things to be aware of:

- Avoid agent-based systems where possible. They introduce both network management and security issues. (see Q&A for more information)
- Scanners with added configuration auditing capabilities may lack the architecture needed to provide an accurate audit. Independent lab tests of a market leading scanner with such features, proved it only 16.4% accurate.

The downside of configuration auditing is that the auditing tools must be programmed to understand the system or device that they are auditing. They have to be able to understand the configuration options of the audited platform and how to interact, or read the configuration file. Nipper Studio leads the way in this area, currently supporting 122 different network infrastructure devices from 35 manufacturers.

# SIEM Systems

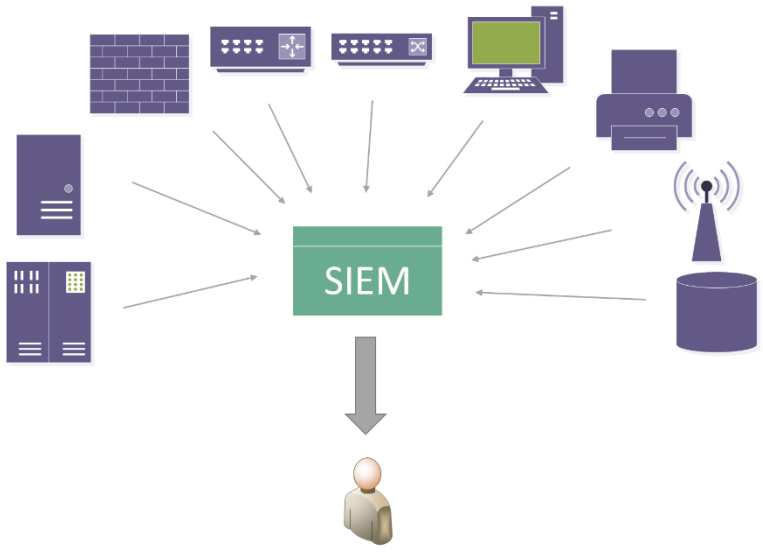
## Summary

Security Information and Event Management (SIEM) systems collate data sent from one or more sources. They then apply rules and analysis to the data in order to extract and categorize real-time events to help administrators identify maintenance, security and compliance issues. Dashboards are typically flexible and enable admins to create overviews that meet their own organizations demands. SIEM systems also provide long term recording of events for historical analysis.

When configured with rules that link together different types of events, SIEM systems can deliver the kind of intelligent analysis needed in the most secure environments. For example, you could link together events from a door access system to user logins to determine if the same person appears to be in two places at once.

A SIEM systems strength is in collating security and compliance information from your systems.

- **INFORMATION COLLATION**
  They are designed to collate information from various sources and put all your security and compliance information in one place.
- **FAST**
  They are quick at providing you with updates on what is happening right now in real-time.
- **REACTIVE**
  A lot of systems enable you to create actions to be automatically triggered when certain events are detected.
- **COMPLEX**
  SIEM systems can be complex to configure and setup. Some systems have plugins to help manage data from specific source types.




NOTE: SIEM systems are only as accurate as the data that they receive.

> *TIP*
> To get the most out of a SIEM system, you need to ensure that the information it is analysing is accurate. This is especially true if you are going to be triggering automated responses when certain events are detected. One such adjustment would be to lower the reliance on vulnerability information sourced from scans and place more emphasis on configuration analysis results.

## Capabilities

There are well established industry standard formats for event information transmission. Most network devices, operating systems, appliances and enterprise applications support those formats. This enables SIEM systems to consume vast quantities of information from a wide variety of different systems.

Some SIEM systems enable you to customize, or add plugins, to fine tune and categorize the data arriving from specific applications or appliances. This enables the system to better understand and interpret the information being sent and allows the SIEM to make more informed analysis.

It is also possible on a lot of SIEM systems for data analysis to trigger a response. One example would be if a user account is performing unusual activity – the SIEM system could trigger a response to lock the user account and alert network administrators

> *TIP*
> The quantity of information available to SIEM systems can be a problem as well as an advantage. It is worth fine tuning the source systems to only show the events that you are interested in. This will help reduce the demand on network bandwidth, improve the performance of the SIEM system analysis and reduce storage requirements.

## Tools

There are lots of commercial and Open Source SIEM systems. Some of the commercial offerings include free versions that have a reduced function set or limit data size.

Popular SIEM platforms include Splunk, LogRhythm, ArcSight and Alien Vault. Some SIEM systems can become very expensive once you have costed-in options and how much data it will analyse. To help you pick the right solution, specify your own requirements, what you want the system to tell you, how much data it is likely going to process and what budget you have.

SIEM systems will typically consume data in both industry standard and custom formats. These include Syslog, Windows events, JSON and plain text data streams. Since consuming data is a key component SIEM systems, the main providers will generally support a wide variety of data sources.

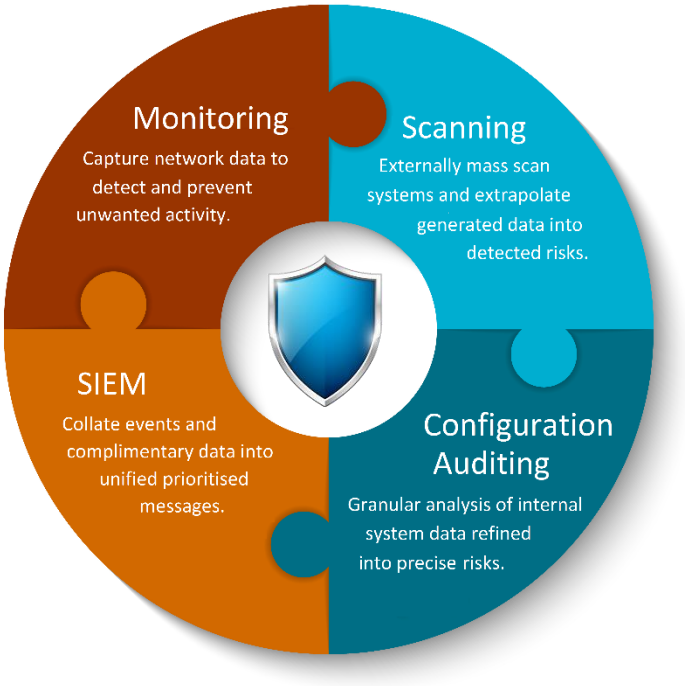
# Conclusions

Rising attacks and technology growth means the demand for skilled cyber experts is outstripping current and future supply - creating a widening skills gap. Enterprises need effective security, they also require in-house and external cyber teams to deliver architecture for commercial growth.
To allow both to be delivered, the end goal for many organizations is autonomous mitigation and flexible "self-healing" systems.

No single technology has the "silver bullet" for this, only through partnerships and collaboration can these systems become a reality. Next generation systems will combine "helicopter" executive summary views (scanning & SIEM), built on the bedrock of "granular" accuracy (monitoring & configuration auditing). Marrying these "Yin & Yang" security technologies, will become the new norm.

Each technology is architecturally designed for *one* specific expertise area. The complementary technologies each have an essential requirement that none of the others can adequately provide.

- MONITORING
  Live detection and protection
- SCANNING
  Asset Discovery, Security "Helicopter Views"
- CONFIGURATION AUDITING
  Compliance / Security "Granular Accuracy"
- SIEM SYSTEMS
  Collate the big picture "Executive Summary"




Combining these strengths into an integrated solution delivers the accurate compliance and security data and operational systems that are essential for current and future autonomous needs.
It will free up cyber experts from much of the time consuming but essential systems housekeeping and allow them to focus on delivering the architecture needed for commercial growth.

There may be challenges along the way. Not all vendors have standalone technologies that are easy to integrate into new solutions or flexible enough to white box. However, there are vendors that already meet those needs (some are highlighted in this paper). The goal of autonomous mitigation and flexible "self-healing" systems, is deliverable and achievable today.

# Questions Answered

## Why is it best to avoid agent-based systems?

Agent-based auditing software may reduce network traffic during auditing and can help when communication is difficult, but they introduce a series of security and management complications:

- ⛔ You will need to install / deploy / configure the agents.
- ⛔ Multiple technology agents can conflict with each other or impact system performance.
- ⛔ Agent software needs to be constantly maintained and updated and there are many cases of agents containing security vulnerabilities. Agents tend to have administrative level of access, so security holes create serious issues. (e.g. McAfee / Heartbleed https://kc.mcafee.com/corporate/index?page=content&id=SB10075 ).
- ⛔ Agents tend to work on non-standard high numbered network ports, so you will need to re-configure your network firewall rules in order for the agents to communicate to the management system.
- ⛔ They are typically complex to configure and manage.

Choosing from a wide variety of agentless tools will avoid many of these challenges.

## Why should I audit continually?

Whilst anti-virus software is normally run continually, scanning and configuration auditing are often scheduled events or an activity performed by penetration testers. However, new vulnerabilities can be introduced at any time, which can leave you at risk.

Desktop settings are changed, new users are added, domain policies are modified, firewall rules are adapted and you add new software or updates, on a daily basis. Network environments are constantly changing and evolving and it can stretch your security team.

Continual monitoring (combining a scanners “helicopter view” with the “granular accuracy” of intelligent configuration auditing) helps your team close compliance & security gaps faster.

## How does scanning and configuration auditing differ?

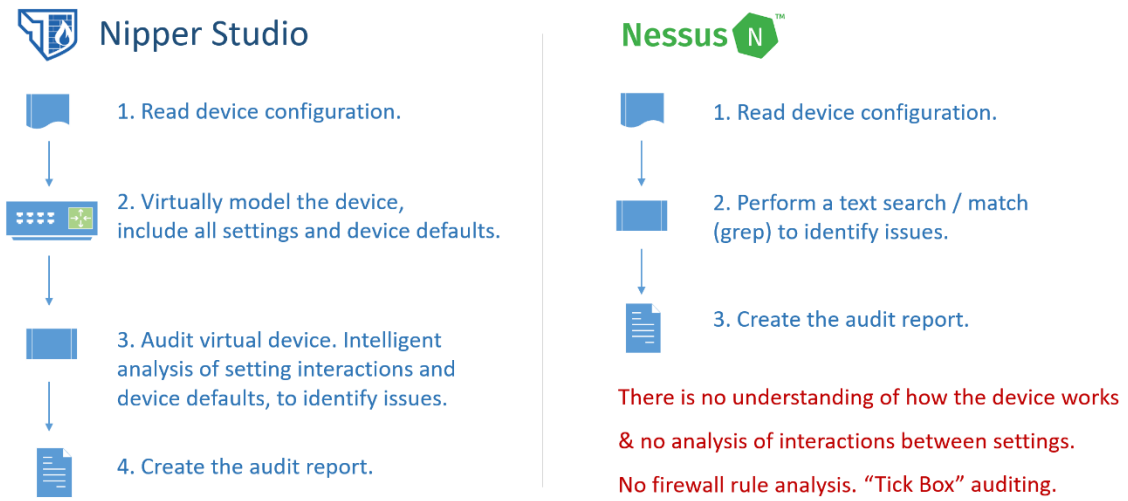
Scanners are very different in architecture and focus from configuration auditing tools.
i) **Configuration auditing tools audit *internal system information, refining mass configuration and O/S data*** (that is already present) into specific vulnerability and remediation advice.
ii) **Scanners audit *external system information*** they interrogate, attack or exploit systems to ***generate mass security data***, which they then analyse and extrapolate into meaningful results.

## My scanner has configuration auditing, why do I need a separate tool?

Multi-layered security is dependent on having *most applicable* technologies in each area.
Accuracy and reliability are the key benefits of Configuration Auditing.

There are two types of configuration auditing technologies:
i) "find and match" text string analysis (grep) tools and
ii) solutions with built in AI / virtual modelling intelligence.

Some market leading scanners, such as Nessus, have added a basic configuration auditing (grep).
As "grep" configuration auditing is prone to false positives and negatives, it is not suitable to provide the accurate baseline information required by current and future SIEM systems.



# Acronyms

| Acronym | Description |
|---|---|
| **API** | **Application Program Interface**<br>An API enables computer programs to access the functionality of another. |
| **ARP** | **Address Resolution Protocol**<br>Is an IP protocol that enables computers to marry hardware addresses with IP addresses. |
| **AV** | **Anti-Virus**<br>Software that enables the detection, quarantine and removal of malicious software. |
| **BGP** | **Boarder Gateway Protocol**<br>BGP is a dynamic routing protocol that helps routers make decisions about where to forward traffic. |
| **CDP** | **Cisco Discovery Protocol**<br>Is a protocol used by Cisco, and some HP, devices to advertise information about themselves. |
| **DHCP** | **Dynamic Host Configuration Protocol**<br>DHCP is used to allocate IP addresses, and other network settings, to networked systems. |
| **DLP** | **Data Loss Prevention**<br>DLP software monitors data transfers and attempts to prevent unauthorised data transfers. |
| **DTP** | **Dynamic Trunking Protocol**<br>A Cisco protocol designed to enable switches to negotiate VLAN trunks (where VLANS pass between them). |
| **GB** | **Gigabyte**<br>GB is a measurement of computer storage capacity. It is 1 billion bits (1's or 0's). |
| **ICMP** | **Internet Control Message Protocol**<br>Is a standard IP protocol that is mostly used for sending error messages between systems. |
| **IEEE** | **Institute of Electrical and Electronics Engineers**<br>IEEE is the professional association that defines and manages standards such as IP. |
| **IPS** | **Intrusion Prevention System**<br>IPS are systems that monitor activity. They then detect and prevent unwanted types of activity. |
| **LLDP** | **Link Layer Discovery Protocol**<br>LLDP is used by networked devices to advertise their capabilities to other networked devices. |

| Acronym | Description |
|---|---|
| **NBNS** | **NetBIOS Name Service**<br>NBNS is used to manage system name registration and resolution in NetBIOS networks. |
| **RIP** | **Routing Information Protocol**<br>RIP is a dynamic routing protocol that helps routers make decisions about where to forward traffic. |
| **RSTP** | **Rapid Spanning Tree Protocol**<br>RSTP is a network protocol designed to detect and prevent network loops between switches. |
| **SIEM** | **Security Information and Event Management**<br>SIEM systems provide real-time storage and analysis of system, application and network events. |
| **SNMP** | **Simple Network Management Protocol**<br>SNMP is a standard IP protocol used for querying and managing networked devices. |
| **SSH** | **Secure Shell**<br>SSH is most commonly used to provide encrypted administrative access to servers and devices. |
| **STP** | **Spanning Tree Protocol**<br>STP is a network protocol designed to detect and prevent network loops between switches. |
| **TCP** | **Transmission Control Protocol**<br>TCP is a key IP protocol that defines how computers establish, transmit and close network communications. |
| **UDP** | **User Datagram Protocol**<br>UDP is a key IP protocol that defines how computers can transmit network communications without connecting. |
| **VLAN** | **Virtual Local Area Network (LAN)**<br>VLANs enable the creation of isolated virtual networks within and between connected network switches. |
| **VTP** | **VLAN Trunking Protocol**<br>VTP is a Cisco protocol that shares VLAN definitions between different network switches. |
| **WMI** | **Windows Management Instrumentation**<br>WMI provides an interface for software components to access Windows system information. |
| **XML** | **Extensible Markup Language**<br>XML is a method of storing and sharing structured data. |

# Award Winning Technology from Titania Limited

## Why use Nipper Studio?

Our advanced security and compliance software is award winning and trusted globally. We offer configuration auditing with granular accuracy, tested and verified by U.S. DoD, FBI, UK Government and Dept. of Energy.

Nipper Studio will analyze internal system information on your firewalls, switches and routers, refine mass configuration and operating system data into precise risks and remediation actions. And produce granular "line by line" analysis (delivered at scale) giving a more accurate picture of vulnerabilities, security and compliance risks.

Add Nipper Studio to your multi-layered defence strategy and gain a more accurate picture of your security risks.

Download and install the latest version of Nipper Studio and get started in minutes.

## Why use Paws Studio?

Paws Studio combines advanced configuration, security and compliance auditing, with completely customizable policies, including regulatory baselines. And produces granular reporting to help strengthen your systems defences.

This technology is award winning and trusted globally by U.S. DoD, FBI, UK Government and Dept. of Energy.

Analyze your laptops, workstations and servers. Unify data output and automate compliance and security policy audits in minutes. Use and customize policies from some of the most trusted institutions such as: DISA, STIG, NERC, SANS, OVAL, NSA & DCPP

Download and install the latest version of Paws Studio and get started in minutes.

# Author Biographies

## Ian Whiting

Ian is the founder and CEO of Titania, a leading innovator and award-winning cyber company with offices in the UK and USA. Before founding Titania and creating the companies' flagship Nippersoftware, Ian was an ethical hacker and CHECK Team Leader.

Ian helped support the British Prime Minister on a UK cyber trade visit to Washington, helping to create closer ties between Britain and theUS.

## Nicola Whiting

Nicola is COO of Titania. She has advised government on engaging SME's in Cyber Strategy and in September 2017 she was named by SC Magazine as one of the top 20 most influential women working in cyber security.

One of her proudest moments was meeting the Queen at Buckingham Palace, to celebrate Titania's award for enterprise innovation.

Today Titania's Pro configuration auditing software serves many industries in over 90 countries, defending both the UK and its allies' cyber borders.

Clients include the NHS, the UK and USGovernments, defense, law enforcement agencies such as the FBI and numerous banks, charities and other organizations.

Titania continues to win awards for security innovation and their core mission is to "make security simple".