SECURE:DATA

INTRUSION PREVENTION SYSTEMS:

FIVE BENEFITS OF SECUREDATA'S MANAGED SERVICE APPROACH

INTRODUCTION:

WHO'S IN YOUR NETWORK?

The days when cyber security could focus on protecting your organisation's perimeter are long gone. Today, the biggest threats are not just from what's lurking outside your borders, but from what suppliers, partners and employees may bring in under the radar.

Thriving technology trends like cloud, bring-your-own-device and remote access mean cyber criminals likely have a foothold inside your network already. In fact, **100% of businesses** recently surveyed by Cisco showed traffic associated with malware.

In this environment of internal threats, Intrusion Prevention Systems (IPS) are essential to safeguard your valuable assets. Based on traffic anomalies and the latest threat signatures, a standalone IPS will report or block malicious activity anywhere in your network, even if it's encrypted.

SecureData's managed service takes the enormous security benefits of **Sourcefire's IPS** a step further by ensuring it's always correctly configured, managed and monitored. Read on as this guide walks you through the five major advantages of our approach.

ARE YOU LOOKING FOR THREATS INSIDE YOUR NETWORK?

- 71% of companies are very concerned by external threats, but only 46% worry about internal ones.
- Of 2014's worst security breaches, 10% were due to portable media bypassing defences, 7% came from mobile devices and 5% from cloud services.
- 70% of attacks from inside networks come from systems compromised by malware.

STEP ONE

WE CREATE A FOUNDATION OF VISIBILITY

The security benefits of an IPS are determined long before you install one and switch it on. Understanding the threat vectors and vulnerabilities inside your network is the foundation for using an IPS to keep your assets protected and available.

Deploying an IPS is never a tick-box exercise and accepting default settings will achieve little - it must be tailored to your environment. Our Vulnerability Scanning service identifies risks and weaknesses inside your network, as well as what information could be compromised by hackers. Armed with this detailed information, we ensure your IPS is configured to block the right threats and protect the right areas, creating more sharply defined security policies based on the actual hardware and software you're using.

After the IPS is installed and placed in detect mode, we use network behaviour analysis techniques to baseline "normal" traffic. This ensures device policies are correctly configured for your environment so that the IPS can readily spot anomalies.

Additionally, a firm foundation of visibility brings more benefits than just tighter security. By eliminating unnecessary signatures during the configuration of your IPS (such as ignoring Linux threats because you have an all Windows environment) analysis of traffic will be faster and will have less of an impact on overall network performance.

EVASIVE ENCRYPTION:

SSL now accounts for an average of 25-30% of an enterprise's network traffic - and cyber criminals are exploiting it.

Encryption is a popular way of hiding malware from signature-based detection systems.

IPS uses anomaly-based detection to catch these threats, because the basic attack pattern is usually unchanged.

STEP TWO

WE PUT THE RIGHT PROCESSES IN PLACE

An IPS demands on-going supervision. Constant management, updates and reviews are essential to ensure your IPS keeps pace with the ever-changing threat landscape and the dynamic environment inside your own business.

With **315,000 new threats emerging every day**, IPS security can quickly fall behind if left untended. Meanwhile, every change in your IT infrastructure, applications or services can create new issues or vulnerabilities - and with so many different IT teams in today's organisations, security staff are not always informed when changes are made in other parts of the business.

Failing to stay up-to-date with threat signatures and policy changes will rapidly reduce the protection an IPS affords and is a huge waste - akin to investing in a state-of-the-art burglar alarm and then not even switching it on. A poorly managed IPS may even interfere with legitimate traffic or break business critical functions due to "false positive alerts". For instance, a mobile developer might find that its IPS suddenly blocks essential app services after users upgrade to the newest version of their device OS.

Having the right processes in place is essential to keep your IPS up-to-date and prevent a sudden spike in false positives, or worse, threats slipping through unnoticed. If you don't currently have processes in place to update and review your IPS, it may be time to ask if that lack of alerts is really such good news after all...

SecureData will update your IPS with the latest threat signatures on an agreed schedule – usually every week. Initially, these new signatures are placed in detect mode only; 48 hours later we will review them with you to identify any false positives and confirm if any signatures should be placed in prevention mode. This ensures your IPS yields maximum protection without interfering with legitimate business operations.

Q: WHAT'S A FALSE POSITIVE?

A: NORMAL NETWORK BEHAVIOUR THAT'S MISIDENTIFIED AS ANOMALOUS OR MALICIOUS.

A single rule causing false positives can easily create thousands of alerts in a short period of time, potentially drowning out genuine and urgent IPS alerts.

STEP THREE

WE REACT IN REAL-TIME WITH THE RIGHT EXPERTISE

IPS alerts can appear at any time of the day or night and you need the ability to respond instantly. Yet, this is not simply a question of having staff available - they also need the knowledge and expertise to assess alerts, sort those that matter from those that don't, and update the IPS swiftly to safeguard your business.

Could your organisation rapidly triage a genuine cyber attack at 4am on Sunday? The skills of well-trained security analysts are essential to understand an attack, determine its trajectory and root cause, as well as what your organisation's response should be.

While a next-generation IPS can pinpoint the source of a threat and identify network repercussions, expert analysts are essential to help your organisation deal with the problem, make the right decisions and, ultimately, take action to avoid re-infection by hardening your defences. With expert management, a next-generation IPS can even construct rules to detect any possible variant of an exploit, allowing you to protect the entire vulnerability not just defend yourself against individual threats. This approach offers the greatest protection against zero-day threats.

By opting for a managed service approach, you can guarantee IPS alerts are handled in real-time, without concerns over resource shortfalls due to sickness or holidays. Our team includes Certified Security Experts and we deliver not just the knowledge of one person, but 130 security professionals across the organisation - putting a huge range of skills and experience at your disposal, all leveraged through a single 24x7x365 contact point in our UK-based Security Operations Centre.

MAJOR IPS SERVICE FEATURES:

- 24x7x365 proactive, expert monitoring of device(s).
- Dedicated incident, problem and change teams.
- Assigned technical guardian.
- Weekly policy and hardware backup.
- Remote system re-builds.
- Unlimited and unmetered:
  - Policy changes
  - Support
- Risk assessment of changes.
- On-going technology upgrades and updates.
- Weekly signature updates and reviews of false positives.
- Weekly calls, monthly service reports and regular reviews.
- Basic Vulnerability Scanning service (remote).

STEP FOUR

WE ELIMINATE THE DRAIN ON YOUR RESOURCES

To ensure you drive maximum value from your IPS and better secure your organisation, continuous management is essential. Yet, the need for on-going monitoring can be a major drain on both your time and budget. On average, an IPS demands of 100 hours of staff time per month. And, of course, cyber criminals do not keep office hours; at least three security staff will be required to ensure 24x7 monitoring.

Locating the in-house expertise to manage and monitor your IPS can also be an expensive proposition. A new hire with the necessary skills can be costly, as can investing in re-training and redeploying existing staff. Taking personnel away from their current roles can have knock-on implications as well. For instance, an IT Manager would spend less time on their core role of optimising IT to make your organisation more efficient and profitable.

Our service enables organisations to cost-effectively access essential IPS expertise, without making a full-time hire.
And, of course, with expertly managed IPS your organisation is less exposed to the financial risks of a compromise – be that the cost of repairing damage, loss of business, or regulatory penalties.

YOUR IPS WILL BE DEMANDING:

- 100 hours of management time per month.
- A minimum of four full-time staff to deliver 24x7 supervision.

STEP FIVE

WE HELP YOU TRANSITION TO INTELLIGENCE

By matching the advanced capabilities of a next-generation IPS with SecureData's managed services, your organisation can set itself on a path to harnessing threat intelligence that will underpin more effective, offensive security.

As a first step, the logs from your IPS and other security devices can be fed into a Security Information and Event Management (SIEM) solution, allowing you to identify and respond to security events automatically, as well as prioritise attacks by threat-level to ensure the best use of your resources.

This can be taken even further with SecureData's Greater Intelligence service, which combines information from inside your network with data feeds from the outside world to build a comprehensive picture of your security posture.

Greater Intelligence allows you to create an active defence that responds to both external risks and internal vulnerabilities dynamically - identifying critical threats, delivering alerts and taking defensive actions in real-time.

By overseeing your IPS as part of a wider set of services, SecureData can make the most of granular detail about threats to improve your protection. For instance, correlating disparate attacks into related incidents, aligning application usernames with violations to identify attackers, or blocking threats based on geo-location information.

NEXT-GENERATION IPS CAPABILITIES:

- **Open architecture:** full visibility into the detection engine and rules.
- **IPS rule creation:** easily create custom rules.
- **Vulnerability-based protection:** detect any variant of an exploit.
- **Network behaviour analysis:** baseline "normal" network traffic to detect anomalies.
- **Virtual IPS and management console:** inspect traffic between virtual machines.

CONCLUSION:

THE TIME IS NOW

With it becoming ever more common for today's threats to be carried right through your business's front door on mobile phones or USB sticks, a standalone IPS is essential. An integrated IPS in your next-generation firewall might sound like enough, but ultimately it can only protect your perimeter.

Combining powerful IPS security with a dedicated managed service makes the most of your investment. It allows you to reap all the benefits, and none of the drawbacks. We ensure flawless IPS performance, while reducing costs, time-consuming management, and the need to hire new expertise.

To find out more about how Managed IPS can help you, visit: **www.secdata.com.**

SECURE:DATA

SecureData House,
Hermitage Court,
Hermitage Lane,
Maidstone,
Kent ME16 9NT

T: +44 (0)1622 723400
F: +44 (0)1622 728580

E: info@secdata.com
www.secdata.com
Follow us on Twitter: @secdataeu