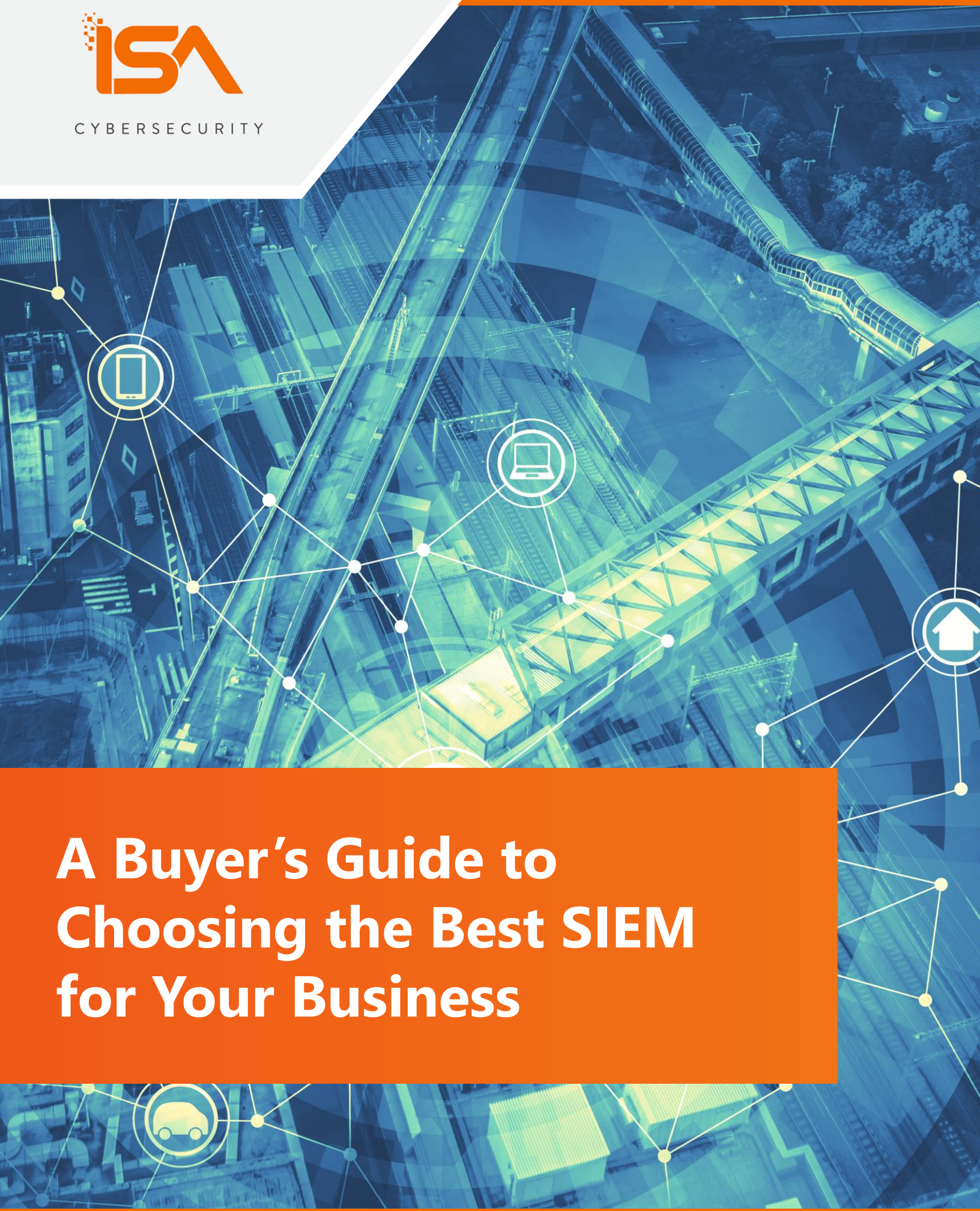
ISA CYBERSECURITY



A Buyer's Guide to Choosing the Best SIEM for Your Business

Understanding SIEM

History of SIEM

Security Incident and Event Management (SIEM) technologies have been around for decades. They were originally designed to bring order to the chaos of security and event alerts generated by the ever-increasing number of IT systems in production environments. Technical staff find it complex enough monitoring alarms on a single file server – with a panoply of specialty systems, networked devices, wireless equipment, and emerging cloud systems, it was impossible for humans to assess, correlate, and react to the volume of operating data created every minute.

SIEMs changed all that by ingesting, aggregating, and analyzing log and system data. Informational alarms were ignored, "expected" or tolerable alerts were de-prioritized, with focus drawn squarely on unexplained anomalous behaviours. SIEMs also provided a high-level view of what was happening on a network, across devices, in real time. A warning message that might be of mild concern if it appeared on a single server became much more interesting when it flashed across several systems at the same time. A SIEM's ability to normalize and cross-reference log data brought insight out of the noise, bringing real-time threat detection and incident prioritization.

Future of SIEM

But technology hasn't stopped evolving in last 20 years, and SIEMs have followed suit. SIEMs are just as important as ever, but have become just the hub of a more sophisticated threat detection approach. So, how do you choose the best SIEM for your business?

What to look for when implementing or upgrading your SIEM

1 Flexible Pricing

Most SIEMs are based on metrics like EPS (events per second) or GBPD (gigabytes per day), while some price models offer unlimited logging at a flat rate. These consumption values are important to understand as factors that will drive cost. Another key pricing lever is storage – SIEMs can have massive databases that securely house event data for reporting, comparison, and compliance purposes. Check your requirements (many regulatory regimes require six or even 12 months of data to be retained); it's essential to know the implications of long-term storage from a cost and performance perspective.

2 User and Entity Behavior Analytics (UEBA)

Today's SIEMs don't just alert you to warnings and errors, but have the (artificial) intelligence to evaluate whether routine activities on a system are within the acceptable or predictable bounds of operation. That behavioural analysis can flag potential incidents that might seem innocuous in isolation, but should raise concern when placed in context.

3 SOAR and XDR

Even with efficiencies that a SIEM can create, there are still too many logs, alerts, and alarms for humans to manage. This is where Security Orchestration, Automation, and Response (SOAR) is the key to making a SIEM truly effective. Alarms prioritized by SIEM can be super-charged by a SOAR solution to automate and coordinate responses automatically, increasing efficiency, and reduce response time to potential attacks. Extended Detection and Response (XDR) is the next generation of SIEM solution. XDR solutions go beyond merely identifying potential threats but actually responding, defending, or even neutralizing threats as they arise.

4 Ease of Connection

Not all SIEMs are created equal. Look for a SIEM that has a great number of pre-defined integrations with current operating systems, devices, and applications. That enables you to get running faster, with more confidence that your connections are tried and tested. Of course, not every system will have pre-built connectors to every source: custom applications or niche, specialized systems will require manual work to develop integration points – be sure to get a sense of how complex it is to build and maintain these connections, and work developers who have expertise in the field.

5 Ease of Integration

Just as SIEMs must connect to data sources to collect information, they should be able to integrate with other applications in your environment. Can your SIEM speak to your reporting systems? Can it mesh with your ticketing system for prioritization and data augmentation to assist with responses? Will it integrate seamlessly with your authentication system? A SIEM should also work harmoniously with your vulnerability management system by leveraging threat intelligence to stay current with emerging risks. A modern SIEM should have all of these bases covered. Understanding these dynamics in advance can create all the difference between a smooth implementation to a complex, costly, or incomplete deployment. Remember your SIEM is supposed to create efficiencies – not headaches.

As SIEM has become the centre of a sophisticated threat detection approach, it requires a significant commitment of computing and personnel resources – both up front and on an ongoing basis to fully leverage its power.

6 Ease of Reporting

For day-to-day management to executive reporting, your SIEM should have easy-to-use, centralized management and executive dashboards to give you, your authorized staff, and your leadership group actionable information about the health of your systems. Security and compliance reporting is an integral part of demonstrating the value of your solution.

7 Development Roadmap

Sure, there are lots of SIEM solutions out there: open source, freeware, pre-packaged solutions, and so on. Be sure that your SIEM of choice has the flexibility and stability you need not just today, but tomorrow as well. Choose a well-established SIEM that is constantly being improved, and has a growth path laid out for years to come; watch for vendors who may be playing out the string with fading technology that isn't keeping pace with today's systems.

Make sure your solution has the legs for the long haul, so you're not looking to replace a solution even before you've finished installing it.

ISA Cybersecurity is here to help

Modern technologies have improved the efficiency and effectiveness of SIEMs, but make no mistake: fully leveraging the power of a SIEM requires a significant commitment of computing and personnel resources – both up front and on an ongoing basis. This is why most organizations look to the cloud for SIEM SaaS solutions, and establish partnerships with third parties to host or manage their solutions. With the 24x7 demands of SIEM monitoring, the extraordinary challenges of recruiting and retaining qualified cyber personnel, and the daunting cost and complexity of a DIY solution, many organizations large and small have realized the benefits of partnering. Working with a trusted managed security service provider allows companies to enjoy the security of a leading, modern SIEM technology without the headaches of licensing, staffing and maintenance costs.

With auditors, compliance officers, cybersecurity insurers, and your executive all asking about SIEM, take these factors into account. Need more information? ISA Cybersecurity can help. We can get you up and running quickly on a hosted SIEM solution, or we can even manage your in-house SIEM if you prefer to host it yourself.

About ISA Cybersecurity

ISA Cybersecurity is Canada's leading cybersecurity-focused company. We have over three decades of experience in helping our customers overcome their cyber challenges.

Expert implementation, maintenance, and monitoring of leading SIEM technologies make ISA Cybersecurity your preferred partner.

Contact us today to learn more, or discover our Hosted and Managed Services.

GET IN TOUCH

1-877-591-6711

info@isacybersecurity.com

isacybersecurity.com

Toronto | Calgary | Ottawa