



Do You Need A Better Defence Strategy?

Five Questions to Ask Before You Upgrade to a SIEM
Solution

Because DIY Security Isn't Good Enough

Information Technology (IT) security teams have to protect their organisations from cyber attackers while also addressing internal and regulatory compliance requirements, such as International Organisation for Standardisation (ISO) 27001, The Payment Card Industry Data Security Standard (PCI DSS) or General Data Protection Regulations (GDPR). This is no small task. If you're relying on a basic log manager or rudimentary spreadsheets to store and search through logs, chances are you're missing critical incidents. As attackers become more dangerous and the regulatory environment continuously evolves, basic tools just can't keep up. The time is now to upgrade to Security Information and Event Management (SIEM).

We'll explore five key questions you should ask to help you determine the best solution for your organisation.

Modern SIEM solutions go beyond the automatic collection, parsing and normalising of logs. They apply advanced correlation and analytics to automatically detect threats, assess their severity and filter through the noise to alert you to critical events. They leverage built-in automation and intelligence to keep you protected while simultaneously freeing up time to focus on remediation and recovery.



The average enterprise security team sees **200,000 security events per day.**

What is a Modern SIEM?

Advanced Analytics for Incident Identification

Extensive data collection, storage and analytics for cloud and on-premises

Real-time correlation against vulnerability data and threat intelligence

Automatic detection and prioritization of critical threats

Behavioral analytics and anomaly detection

Automatic asset, service and user discovery and profiling



Prioritized Incidents and Highest Risk Users

1

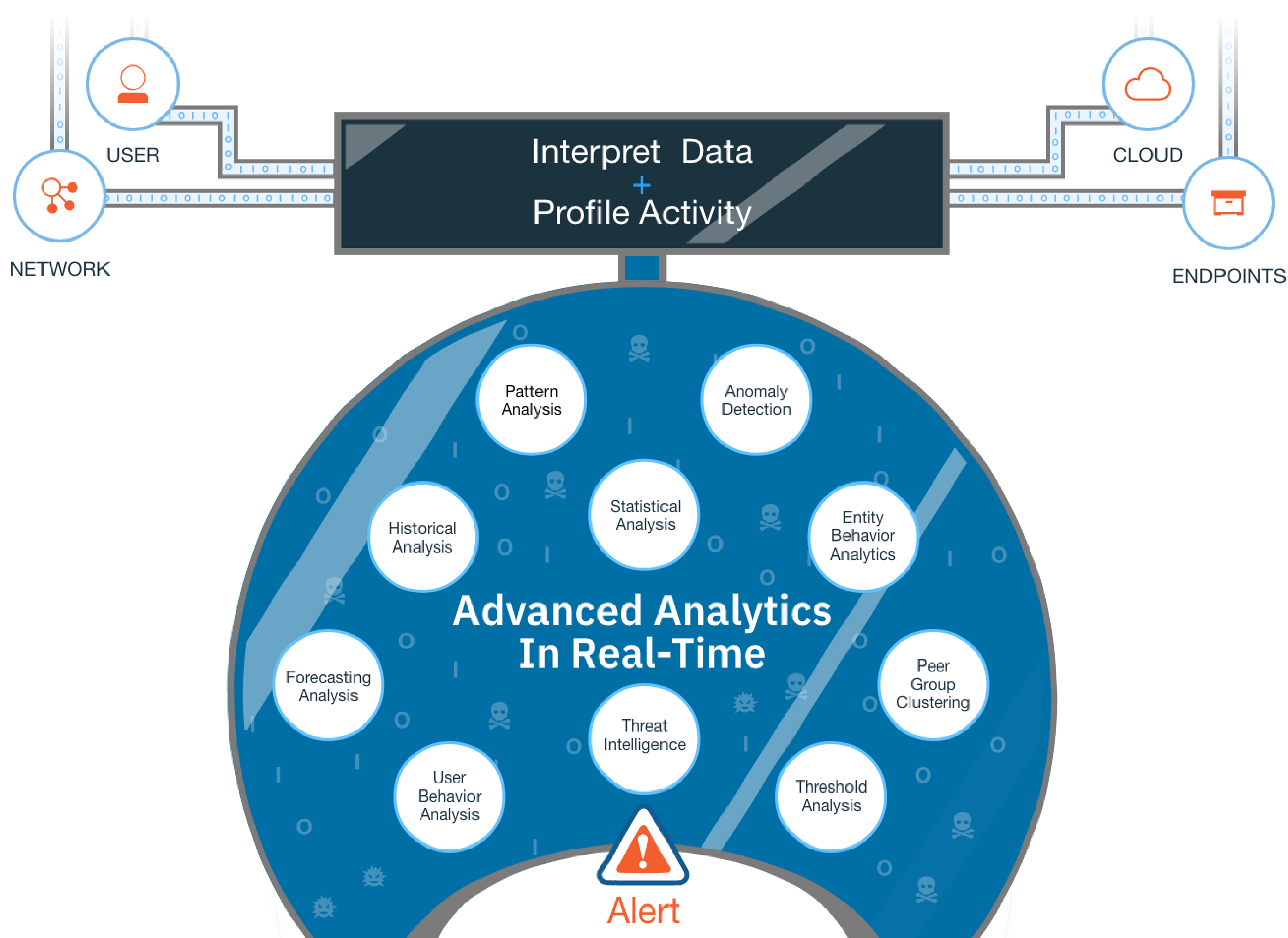
Can You Keep Up With All Your Security Data – In Real Time?

If you're relying on spreadsheets to search and manage logs, you're likely missing real-time changes, not to mention spending significant time and effort in an attempt just to get by. A centralised modern SIEM automates log collection, normalisation and analysis, but it doesn't just do those things. It also provides deeper network-level insights, in addition to logs.



Network flow information helps you track attackers where they can't hide

In addition to system logs, a modern SIEM also looks at network flows, endpoint data, cloud usage and user behaviour. By combining these various aspects of activity, you can get a complete picture of what's happening within your environment, understand what's normal and use that baseline of normal to automatically identify deviations that can signal a threat.



2

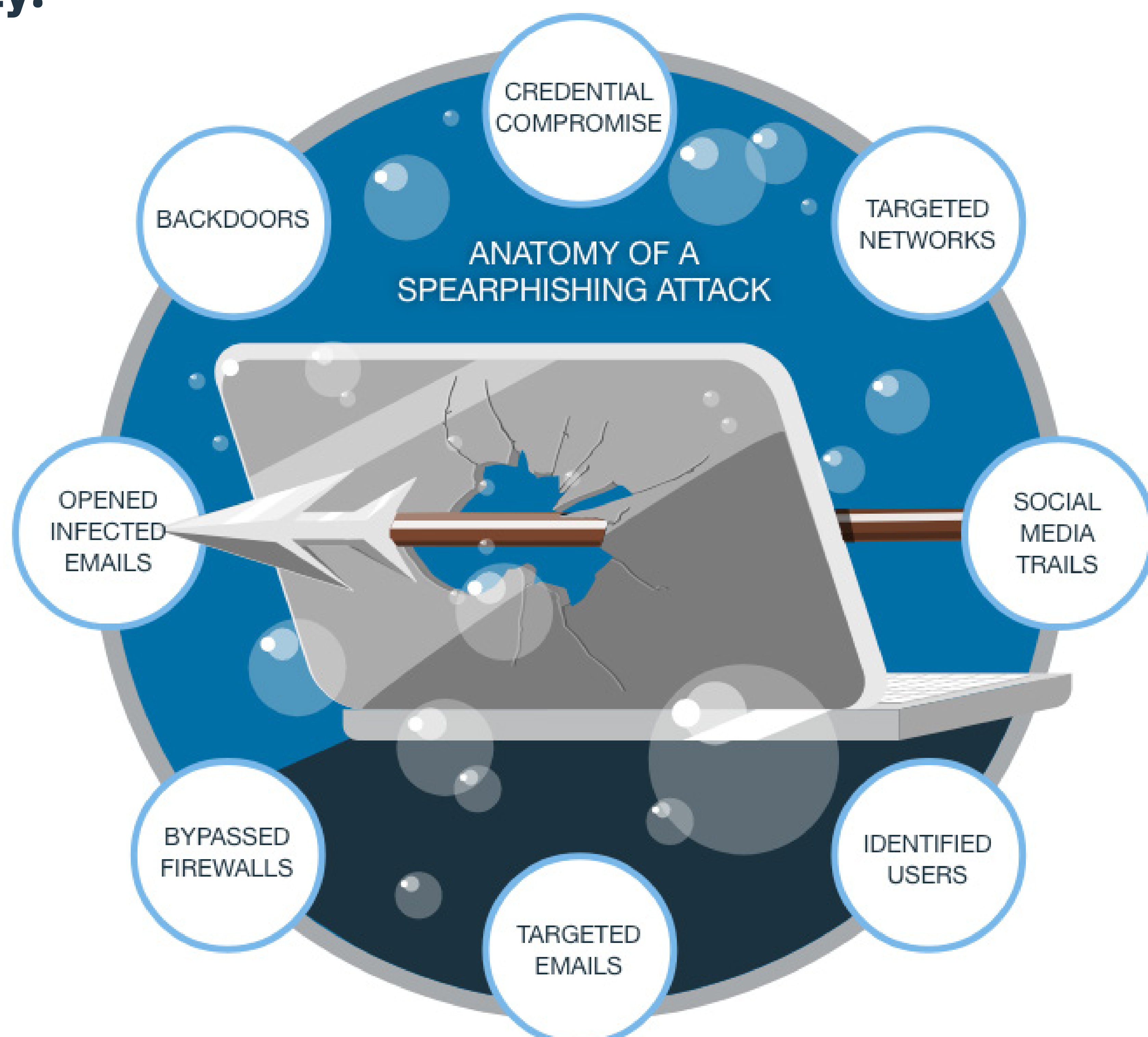
Does Your Security Program Account for The Human Element of Threats?

Sometimes a user gets tricked into clicking a malicious link. Other times, an employee simply turns against you. Do you have a solution that helps you understand the human element?



Of all attacks were carried out by insiders either inadvertently or maliciously.

Compromised or malicious users will exhibit different behaviours than others. Spotting these outliers early can help you prevent damage. To do this, you need to understand what's normal for users in your organisation and use that baseline to identify anomalies that may signal a threat. User behaviour analytics that leverage machine learning can be helpful in scaling anomaly detection enterprise-wide. When part of a SIEM, you can uncover anomalous user activities and prioritise the highest risk users capable of causing the most harm.



3

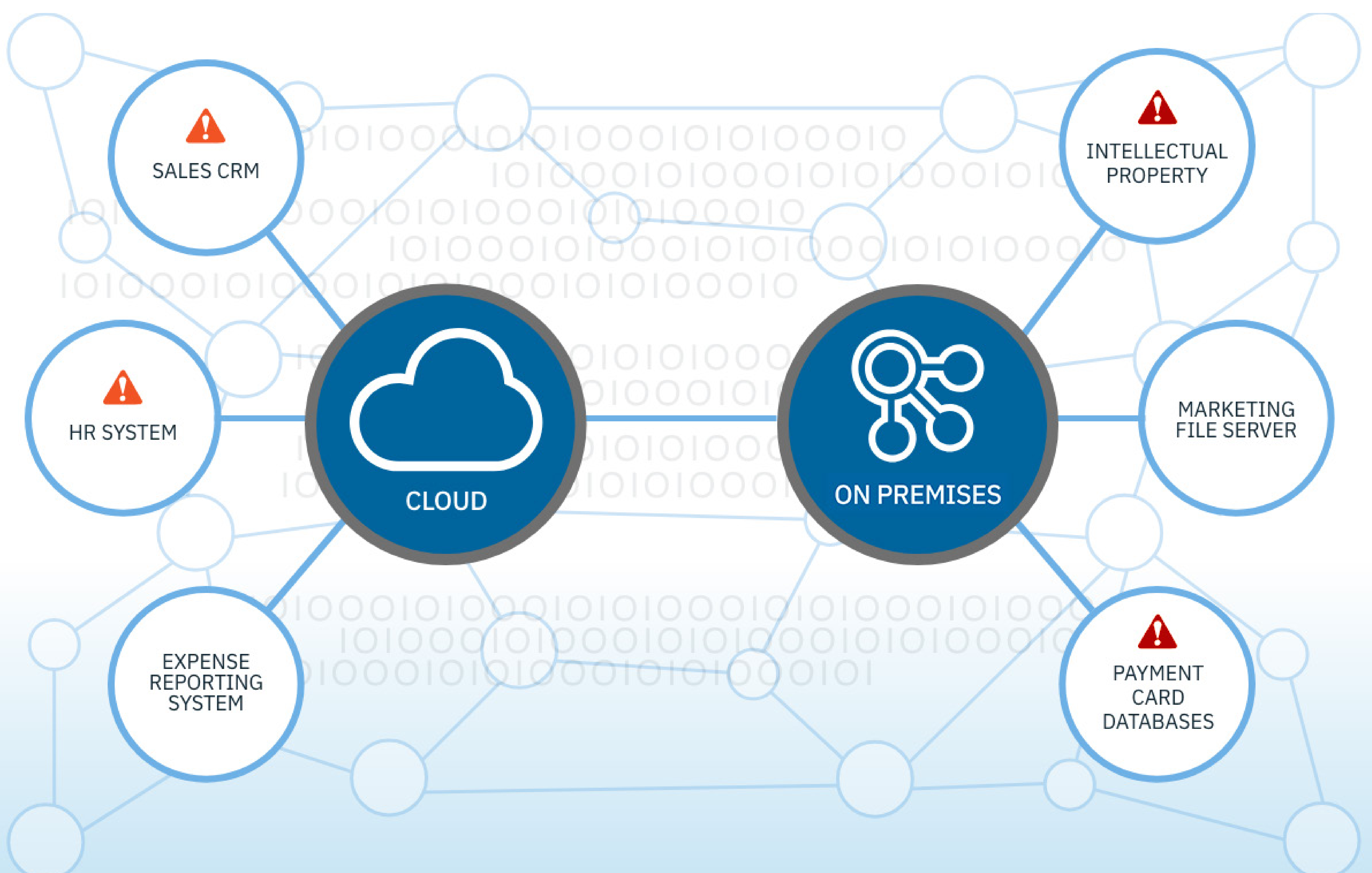
Can It Help You Prioritise Threats Against Your Most Critical Data and Assets?

A file server used by marketing and a database in your Payment Card Industry (PCI) environment carry very different levels of risks if compromised. You need a solution that understands the value of your assets, automatically prioritises threats based on business risk and alerts you when you need it.

A good security solution should offer network awareness. It should enable you to define your most sensitive assets, network segments and cloud services and leverage robust analytics that customise alerts based on risk within your unique environment.



It takes an average of **191 days to detect a breach. Another **66** to contain it.**



4

Does Your System Automate Processes to Help Make You More Productive?

With a limited talent pool in high demand, most security teams are understaffed and overextended. A good SIEM solution offers Artificial Intelligence (AI) and automation that help eliminate manual processes. Modern SIEMs can increase productivity without requiring additional headcount.

An ideal SIEM solution helps automate threat detection, prioritisation and investigation processes. It should offer validated, out-of-box integrations with incident response and case management systems that further accelerate the containment, remediation and recovery processes.

70 percent of cybersecurity professionals report skill shortages have impacted their organisations.

By 2020, there will be **1.5 million** unfilled cybersecurity jobs, up from **1 million** just 2 years ago.

5

How Easy Is It to Get Started and Integrate into Your Environment?


Find out what deployment methods are supported. Whether you prefer hardware, software or Software as a Solution (SaaS) solutions, a good SIEM should be flexible enough to meet your needs. Next, before you can get value from your SIEM, you need to get data into it. Ask if it will work with all your systems, including on-premises assets, SaaS applications and public cloud environments.

Consider the ease of integration not just with log sources but also with complementary solutions, such as threat intelligence feeds, vulnerability scanners, incident response orchestration tools and case management systems, among other things. An open ecosystem for apps and integrations can help you stay up to date and quickly respond to changing risks and threats. The more out-of-the-box integrations, the fewer person hours are needed to extract value.



An average enterprise uses 75 security products to secure their network, they need to work together.





Criminals Are Getting Smarter. Which Leads to One More Question: Are You Prepared?

Modern SIEM solutions go far beyond basic log managers and manual processes. With 200,000 security threats a day, you need lightning-fast protection. A good SIEM should be able to detect an array of threats and threat indicators such as phishing attacks, malware, credential theft, lateral movement and data exfiltration, among many others and alert you before the damage starts. But remember: Not all SIEM solutions are created equally.

Look for a Solution That:



Offers advanced security analytics to detect a variety of threats



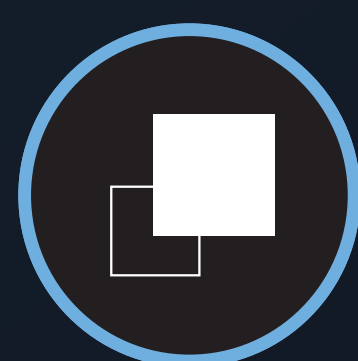
Automatically prioritises threats and alerts so you can see what matters most



Provides out-of-the-box integrations with your existing systems



Consolidates security data and insights in a single platform and interface



Has the ability to deploy at scale, from small to very large



Is flexible enough to support your preferred deployment method, be it on-premise, as SaaS or in a public cloud.



About IBM QRadar

The IBM® QRadar Security Intelligence Platform is a comprehensive security analytics solution that brings together log management, advanced analytics, network analysis, vulnerability management, user behaviour analytics, threat intelligence and AI-powered threat investigations into a single platform managed from a single interface.

Components of the solution are fully integrated, enabling customers to start as small or large as they choose and easily scale up or down as their needs change. With over 500 validated out-of-the-box integrations and pre-configured rules, customers can get up and running quickly and easily add on new capabilities through the IBM Security App Exchange.

Learn more at www.ibm.com/qradar.



References

[Investigating Threats with Watson for Cyber Security](#), **IBM**

[The IBM X-Force 2016 Cyber Security Intelligence Index](#), **IBM**

[Ponemon Institute's 2017 Cost of Data Breach Study: Global Overview](#), **IBM**

[Cybersecurity skills shortage creating recruitment chaos](#), **CSO**

[Cybersecurity labor crunch to hit 1.5 million unfilled jobs by 2021](#), **ISC**

[Defense in depth: Stop spending, start consolidating](#), **CSO**



IBM United Kingdom Limited
PO Box 41, North Harbour
Portsmouth, Hampshire PO6 3AU
United Kingdom

IBM Ireland Limited
Oldbrook House
24-32 Pembroke Road
Dublin 4

IBM Ireland registered in Ireland under company number 16226.

IBM, the IBM logo, ibm.com and QRadar are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions. It is the user's responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs. THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

© Copyright IBM Corporation 2018



Please Recycle