Security use case library

Improve the value of your SIEM with the security use case library

Highlights

- Helps close gaps in your security monitoring policy and detect threats more quickly with security use cases, rules and guidance
- Helps improve ROI by reducing time to develop and implement use cases
- Provides continuous updates to help keep up with evolving threats and regulatory compliance requirements

Once you have a security information and event management (SIEM) solution in place, you're ready to start developing and implementing security use cases and rules that can be used to help improve your overall security operations. The more high-value use cases and rules you put into your SIEM solution, the better return on investment (ROI) in terms of risk reduction and threat response times. But it can be challenging and time-consuming to continuously identify, design, develop, test and implement new security use cases.

The security use case library from IBM provides subscription-based access to a large repository of use cases, rules and related implementation guidance. The contents of the library can be browsed with open-text searches and are also searchable by categories—such as threat type, regulatory compliance categories, and log source types. We developed the security use case library based on experience from hundreds of SIEM implementations, consulting engagements and managed SIEM best practices. And we'll continue to update the library as the security threat and regulatory compliance landscape continues to evolve.

Helping improve your security monitoring and threat detection capabilities

IBM's security use case library can help your organization better identify and close gaps in your current security use case coverage and improve threat detection. As part of the service, we'll provide you with an overview of our Security Use Case Development Framework. After the initial workshop meeting, we can work with you to implement use cases. Our security experts conduct weekly meetings with your IT security staff to review progress and provide any additional guidance, including guidance for developing a runbook and communications and incident response plans for your security operations center (SOC).

Helping improve ROI by reducing time to implement security use cases

The average time for developing and implementing a new security use case can takes weeks—or even months. Many custom use cases have limited value or lack appropriate threat response procedures. Our solution helps reduce upfront and ongoing operational costs associated with SIEM technology by up to 80 percent.[1] And we can reduce the required time to develop and operationalize security use cases and rules by up to 50 percent.[2]

Helping improve your ability to keep up with threats and compliance needs

As the threat landscape, technology and regulatory compliance requirements continue to evolve and change—so does our security use case library. To keep up-to-date and help reduce overall risk, we provide continuous updates to the security use case library. The content in the library is structured based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework and is also mapped to a variety of common security policies, standards and controls.

Why IBM?

IBM has over 10 years of experience in security consulting projects and continuously works with and supports over 100 clients that are subscribed to IBM's Managed SIEM services. We draw on expertise, techniques and methods from these engagements, and apply them to the content within our use case library. In addition, our library is constantly being updated based on the latest IBM® XForce® threat intelligence reports and lessons learned from our global network of SOCs.

For more information

To learn more about the security use case and rule library, please contact your IBM representative or visit the following website: **ibm.com**/services/security

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit: **ibm.com**/financing

Global Services
Route 100
Somers, NY 10589

Produced in the United States of America
February 2016

[1] Based on IBM internal data analysis. Individual results may vary.

[2] Ibid.

SED03167-USEN-00