Hitchhiker's Guide to Managed Security

Capabilities and Limitations

Understand the technical detection capabilities and limitations of the service being offered.

- What are the provided detection capabilities?
- Is the service based (solely) on a commercial product?
- Is it possible to implement custom detection logic?
- What kind of log sources can be ingested by the provider?

Communication

Understand which alerts and incidents are handled by the service provider.

Understand your responsibilities and those of the service provider.

- Is it clear which and how alerts and incidents are handled by the service provider?
- Are responsibilities clearly defined?
- Are means of communication clearly defined, including fallback solutions?

Transparency

Understand how the service provider documents their services and how this information is made available to you.

- Are custom use cases documented in a comprehensive way?
- Is the documentation accessible to you at any time?
- Is it possible to track decisions taken by the service provider in a comprehensive way?
- Is the provided dashboard comprehensive and usable?

Continuous Improvement

Keep challenging your detection capabilities.

- Are current detection capabilities sufficient and do they cover changes made to your IT environment?
- How can your detection capabilities be improved?
- Do your existing detection capabilities still work as expected?

Coverage

The provided coverage of the service should fit your environment.

- Does the service reflect your threat model?
- Are all key aspects of your IT infrastructure and critical assets covered by the service?
- Does the time coverage of the service match your business model and availability?

Incident Handling

Understand which information is provided by the service provider in case of an incident.

Understand which reactions the service provider can perform in case of an incident.

- What information is provided in case of an incident?
- Is the provided incident information comprehensive and useful for you?
- Should a service provider be able to take actions autonomously in case of an incident?

Implementation

Avoid common pitfalls during the implementation phase.

- Are all log sources correctly integrated?
- Are all use cases tailored for your environment? (Thresholds, localization, etc.)
- Are all use cases regularly tested and verified in your environment?
- Is a clear exception handling process defined?
- Are exceptions crafted as narrowly as possible?
- Is the implementation clearly documented?

COMPASS® SECURITY

For more information, read the blog post
https://blog.compass-security.com/?p=8468

Version 1.0, January 2025
Compass Security