Microsoft Sentinel

Keep it simple by starting out small

August 2022

MINDCORE

Get at good start to Microsoft Sentinel

Microsoft Sentinel is a scalable, cloud-native, Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) solution. Microsoft Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for attack detection, threat visibility, proactive hunting, and threat response.

Sentinel is a strong addon to existing security measures. It takes security to the next level, by analyzing data collected across all existing security solutions, using advanced queries, to detect suspicious activity, and can function as the central security incident portal for your entire organization. This reduces time spent on figuring out what is happening, allowing the organization to instead focus on what to do.

Establish acceptance of the fact that it is continuous work to manage and maintain Sentinel. Your environment (inside and outside your organization) is constantly changing, and therefore a good setup today is not necessarily a good setup tomorrow. This means that Sentinel is constantly evolving.

Start small and build from there. Mindcore suggests starting with a Proof of Concept (PoC) with a few data connectors. This is the best way to assess the solution and to understand the insights that you can gain, and how to use this insight to improve your security.

Typical scope is 2-4 working days, split over 2-3 weeks.

Customer Cases

A few of the organizations, that Mindcore has supported with Sentinel

Our expert on Microsoft Sentinel

Michael Nielsen
Microsoft Security Consultant
Mindcore

MICROSOFT SENTINEL | PROOF OF CONCEPT

WHERE DO WE START?

Initial conversation on what the organization expects from Sentinel, and where to start, i.e.

- ✓ Entity Behavior
- ✓ Break the glass account successful/failed login
- ✓ Incidents/alerts based on license type and available data
- ✓ Architecture

INITIAL SETUP

Initial setup of Sentinel and PoC scope

- ✓ Sentinel
- ✓ Log Analytics
- ✓ Agents
- ✓ Pre-defined analytic rules
- ✓ Data connectors
- ✓ OPTIONAL: Single Logic App

POC TEST PHASE

- ✓ Data collection (1-2 weeks)
- ✓ Review collected data to verify insights

EVALUATE & OUTPUT

- ✓ Evaluate PoC output
- ✓ Discuss how the organization can adopt, manage and expand the use of Sentinel

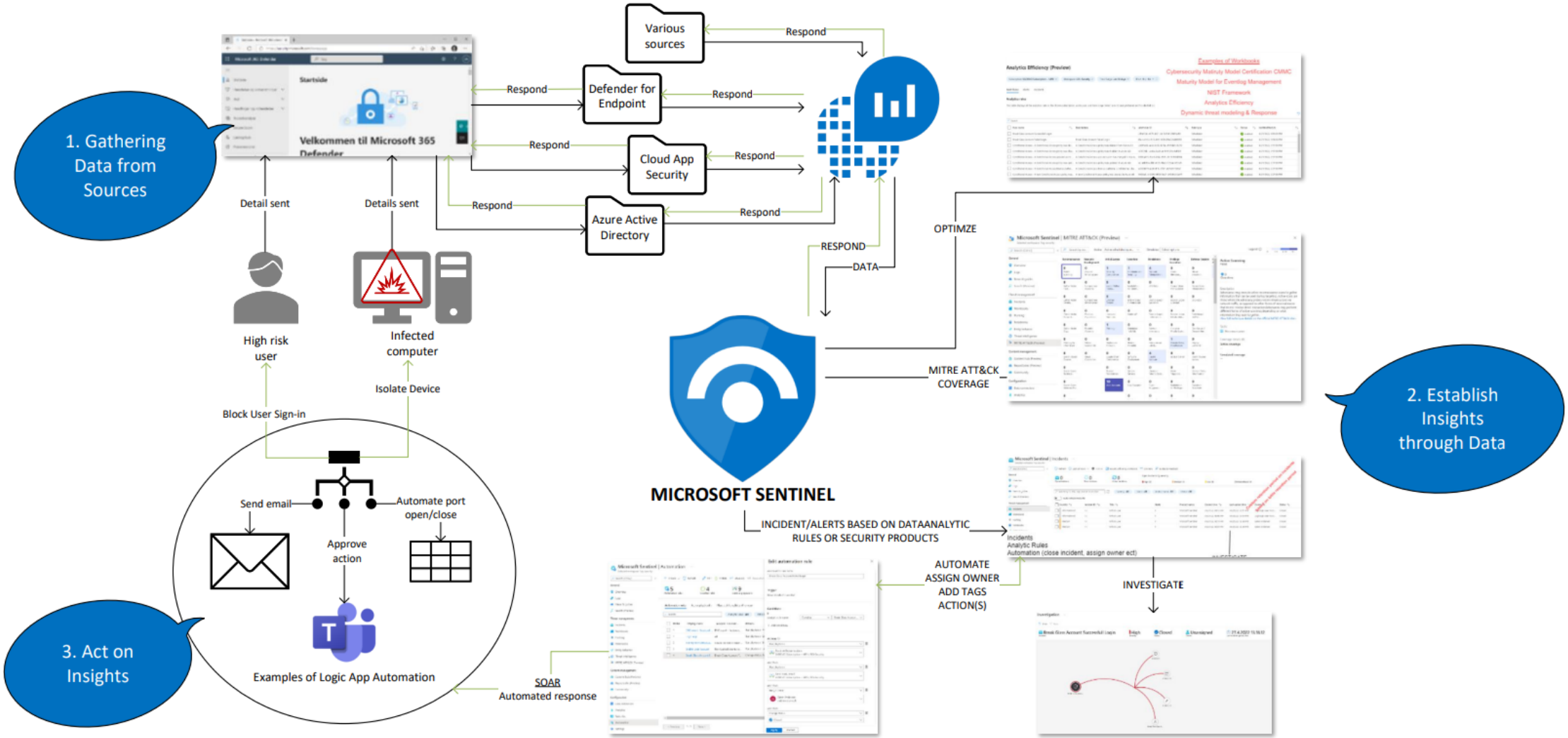
ITERATIVE DEVELOPMENT

After evaluation and output, new data can be added to expand the use of Sentinel

Important thing to remember is that to ensure that organization is ready to use and react to additional insights

For the technical reader

Below is a high-level overview of Sentinel and the eco-system surrounding it - from data sources to insights and acting on those insights.



For more information

· MINDCORE ·
Lottenborgvej 26A, 2800 Kongens Lyngby

Michael Nielsen

Security Consultant
E-mail: mn@mindcore.dk
Mobil: +45 3131 9244

Jacob Guldager-Løve

Partner
E-mail: jgl@mindcore.dk
Mobil: +45 52 15 01 14

Rasmus Kruse Steglich-Andersen

Director
E-mail: rk@mindcore.dk
Mobile: +45 5215 0173