Microsoft Azure Sentinel Deployment Planning Services

March 2020

nccgroup

What we’ll do during the Engagement

An engagement allowing you to experience Azure Sentinel & find threats in your environment

Analyze your requirements and priorities for a Security Information and Event Management (SIEM) deployment

Define scope & deploy Azure Sentinel in your production environment integrating with Microsoft and 3rd party solutions

Remote monitoring* NCC Group pro-active threat hunting to discover Indicators of Attack during the alert & log collection phase

*Optional component to be discussed

Discover threats to your on-premises and cloud environments across email, identity, and data and demonstrate how to automate responses

Recommend, HLD & next steps to a production implementation of Azure Sentinel

nccgroup

Scenario A – Remote Monitoring

Experience NCC Group Remote Monitoring Service

NCC Group Visibility & Control Over Blind Spots

Identity security perimeter to protect cloud, mobile and IoT assets using Azure Sentinel

Automated policy monitoring and enforcement for modern estate

Designed for organizations that can't justify building and staffing their own SOC or when you need to offload certain monitoring tasks so that your SecOps team can focus on key risk areas.

We will manage your Azure Sentinel deployment remotely during the alert and log collection phase allowing us to also provide:

- **Incident monitoring** - Our security analysts will provide remote monitoring of Azure Sentinel for incidents during the engagement.
- **Proactive threat hunting** - Our security analysts will use Azure Sentinel's powerful hunting search and query tools to hunt for security threats across your organization's data sources.

Out of scope

- **Incident response** – Not included in the default scope

Requirements

- Access to deployed Azure Sentinel instance in your tenant using delegated access through either Azure B2B or Azure Lighthouse (recommended)

Azure Sentinel Agile & Efficient Threat Protection

Automated and integrated toolsets for response efficiency and effectiveness

Integrated telemetry to reduce noise and increase accuracy

Scenario B – Joint Threat Exploration

Collaborative Exploration

Visibility & Control Over Blind Spots

Identity security perimeter to protect cloud, mobile and IoT assets using Azure Sentinel

Automated policy monitoring and enforcement for modern estate

No remote monitoring. Instead we will complete the threat exploration step together, allowing your security analysts and engineers additional hands-on experience with Azure Sentinel to enable you to manage Azure Sentinel as part of your existing SOC. As part of the joint Threat Exploration you will:

- **Experience Azure Sentinel** - Get hands-on experience and learn how to discover and analyze threats using Azure Sentinel. Learn how to automate your Security Operations to make it more effective.
- **Analyze threats** - Analyze and gain visibility into threats to your Microsoft 365 cloud and on-premises environments across email, identity and data in order to better understand, prioritize and mitigate potential cyberattack vectors

Out of scope

- **Incident response** - Not included in the default scope

Requirements

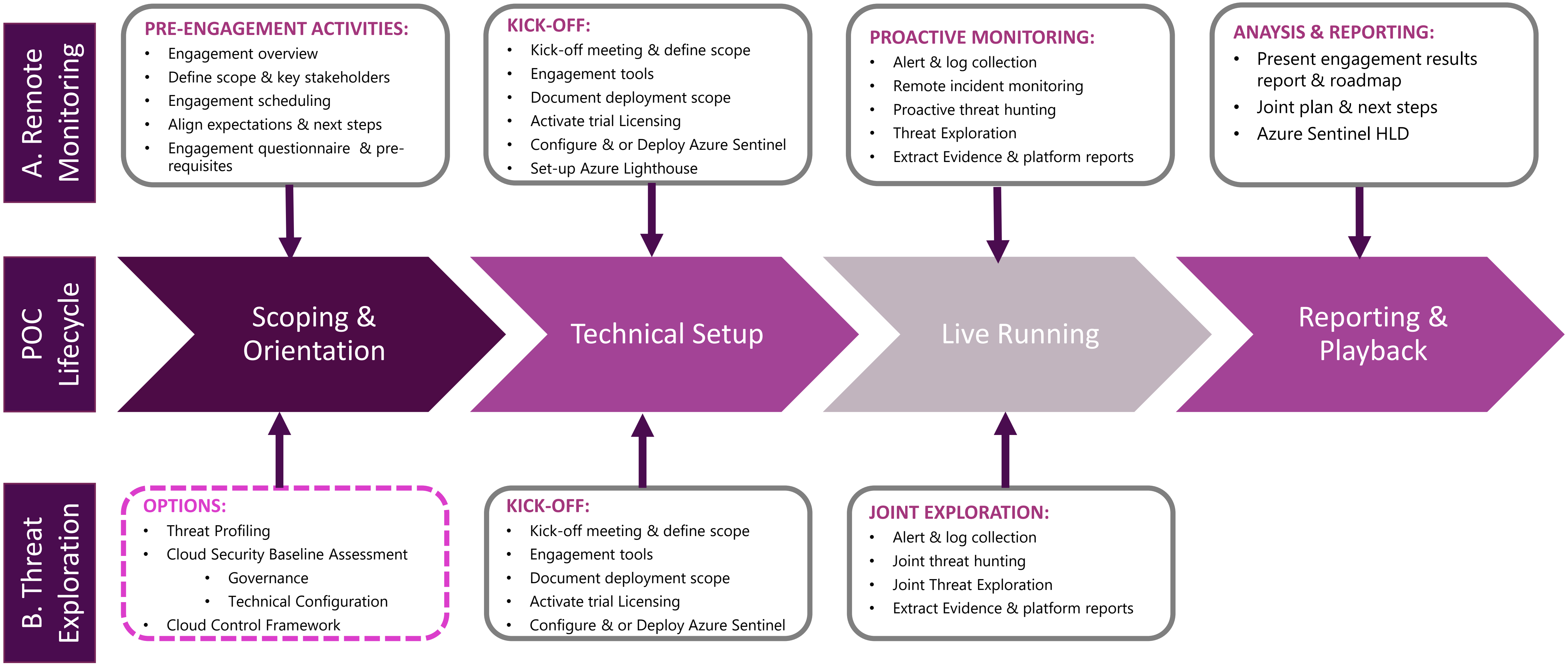
- No additional requirements necessary

Azure Sentinel Agile & Efficient Threat Protection

Automated and integrated toolsets for response efficiency and effectiveness

Integrated telemetry to reduce noise and increase accuracy

Engagement Timelines



A. Remote Monitoring

PRE-ENGAGEMENT ACTIVITIES:

- Engagement overview
- Define scope & key stakeholders
- Engagement scheduling
- Align expectations & next steps
- Engagement questionnaire & pre-requisites

KICK-OFF:

- Kick-off meeting & define scope
- Engagement tools
- Document deployment scope
- Activate trial Licensing
- Configure & or Deploy Azure Sentinel
- Set-up Azure Lighthouse

PROACTIVE MONITORING:

- Alert & log collection
- Remote incident monitoring
- Proactive threat hunting
- Threat Exploration
- Extract Evidence & platform reports

ANAYSIS & REPORTING:

- Present engagement results report & roadmap
- Joint plan & next steps
- Azure Sentinel HLD

POC Lifecycle

Scoping & Orientation

Technical Setup

Live Running

Reporting & Playback

B. Threat Exploration

OPTIONS:

- Threat Profiling
- Cloud Security Baseline Assessment
  - Governance
  - Technical Configuration
- Cloud Control Framework

KICK-OFF:

- Kick-off meeting & define scope
- Engagement tools
- Document deployment scope
- Activate trial Licensing
- Configure & or Deploy Azure Sentinel

JOINT EXPLORATION:

- Alert & log collection
- Joint threat hunting
- Joint Threat Exploration
- Extract Evidence & platform reports

nccgroup

Outcomes

Understand the benefits of a cloud native SIEM

Understanding of how Azure Sentinel, a cloud native SIEM can improve operational efficiencies for your security operations

Results Report

Lists and interprets cyberattack threats targeting currently your organization, observed in this engagement

Threat Mitigation Recommendations

Maps observed threats to Microsoft 365 security products and features in order to mitigate impact of these threats

Next Step Plan

At the end of the engagement we will provide a recommended deployment roadmap to help you build a business case for the deployment of Azure Sentinel.

People led knowledge and capability is at our core

nccgroup

www.nccgroup.trust

Twitter: @NCCGroupplc @NCCGroupInfoSec