Gold Microsoft Partner Microsoft

Exelegent

Azure Sentinel: 3-Week Workshop

by Exelegent & Microsoft

Exelegent

http://www.exelegent.com/ · in · 36 W Main Street, Suite 300, Freehold, NJ, US 07728

CONTACT › Search for other providers

This provider has demonstrated competency in the following areas

Gold	Communications
Gold	DevOps
Gold	Data Analytics
Gold	Data Platform
Gold	Cloud Productivity
Gold	Security
Gold	Cloud Platform
Gold	Windows and Devices
Gold	Collaboration and Content
Gold	Messaging
Silver	Small and Midmarket Cloud Solutions
Silver	Enterprise Mobility Management
Silver	Application Development
Silver	Project and Portfolio Management
Silver	Datacenter

10 -Time Gold Microsoft Partner

About us

Exelegent is a cyber security and professional services company where efficiency is standard, and our customers are our partners. Headquartered in Freehold, NJ with supporting offices in Newark, NJ and L'viv Ukraine, Exelegent leverages years of experience to bring about a world-class experience for our clients.

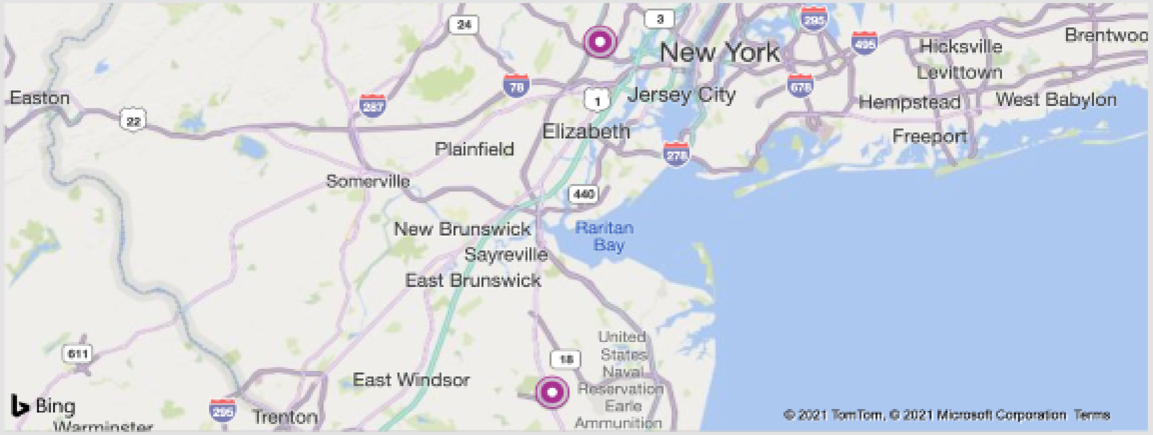
Our specialties include:

More

Skills and Capabilities

- Advanced Analytics
- Agriculture, Forestry, & Fishing
- Application Integration
- Artificial Intelligence
- Azure
- Azure Security & Operation Management

Top locations



36 W Main Street, Suite 300, Freehold, NJ, US 07728

495 N 13th street, Newark, NJ, US 07107

What our clients say:

- "Exelegent helped our company migrate from G-Suite to Microsoft Office 365 with zero downtime and zero data loss. During the process, over 3,500 users continued to collaborate and run critical business functions seamlessly.”

  Robert Florescu, CISO, CityMD

- "Switching to Exelegent has been a major contributing factor to the growth of our group. As a company looking to expand, we really value our employees' time and productivity. Exelegent's IT Support has enabled our business to run as efficiently as possible."

  Bruce Lucarelli, CTO, DermOne

- "Exelegent has been with our hospital since we've opened our doors. Their experience in a wide range of projects and solutions, and management of vendors has made a tremendous impact on our efficiency”

  Alexey Gololobov, CFO, Columbus Hospital LTACH

- “Exelegent has become our trusted business partner and completed migration on time, alleviated hosting responsibilities, and gave us capabilities to enable team productivity and data security.«

  Kevin Hannigan, President, ACC Inc.

Exelegent

Clients

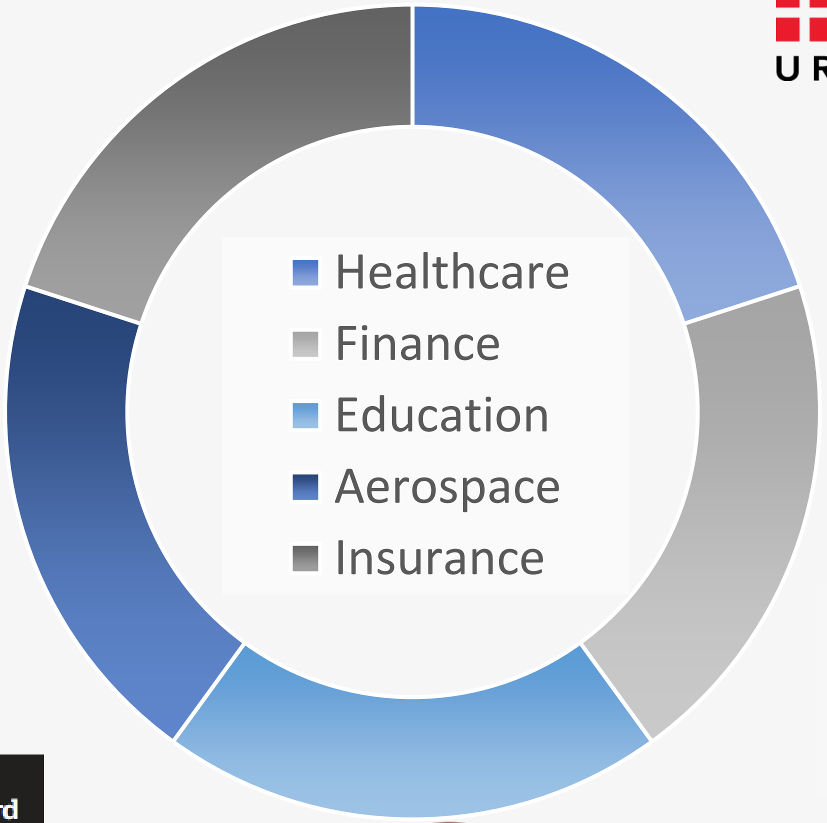
Industries we serve

WORLD INSURANCE

CITYMD URGENT CARE

SaintPeter's UNIVERSITY

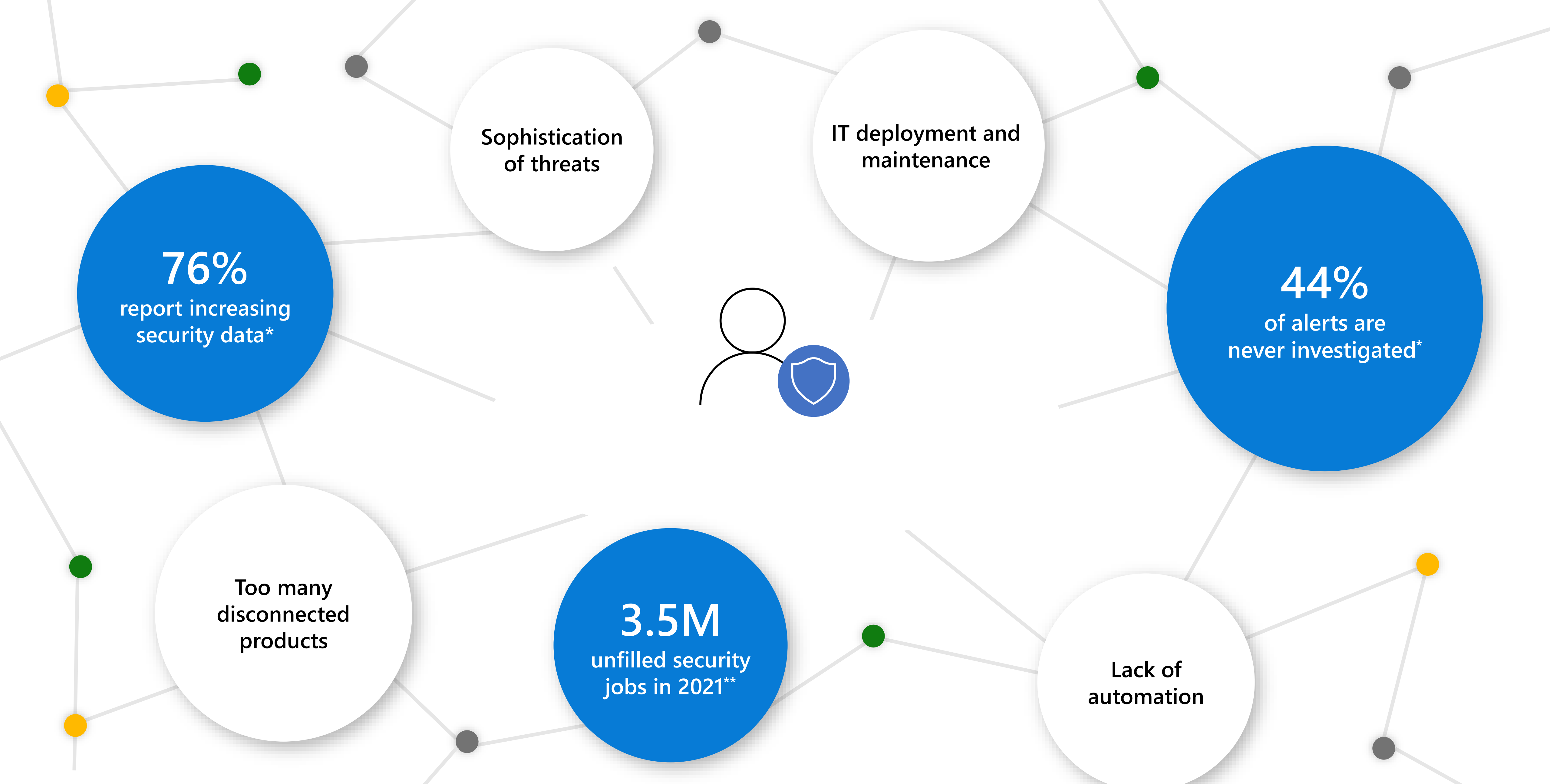
In-Phase Technologies, Inc.



OCEANFIRST BANK

CollegeBoard

ETS®



Sophistication of threats

IT deployment and maintenance

76%
report increasing security data*

44%
of alerts are never investigated*

Too many disconnected products

3.5M
unfilled security jobs in 2021**

Lack of automation

*ESG: Security Analytics and Operations: Industry Trends in the Era of Cloud Computing 2019
**CSO Magazine

Exelegent

What is Microsoft Sentinel?

Microsoft Sentinel is a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution.

Insights into threats

Get a birds-eye view across all data ingested and detect threats using Microsoft's analytics and threat intelligence. Investigate threats with artificial intelligence and hunt for suspicious activities.

In scope for this engagement.

Ability to automatically respond to detected threats

Out of scope for this engagement.

Requirements

Available to organizations with an Azure tenant.

Optimize security operations with cloud-native SIEM powered by AI and automation

Harness the scale of the cloud

Detect evolving threats

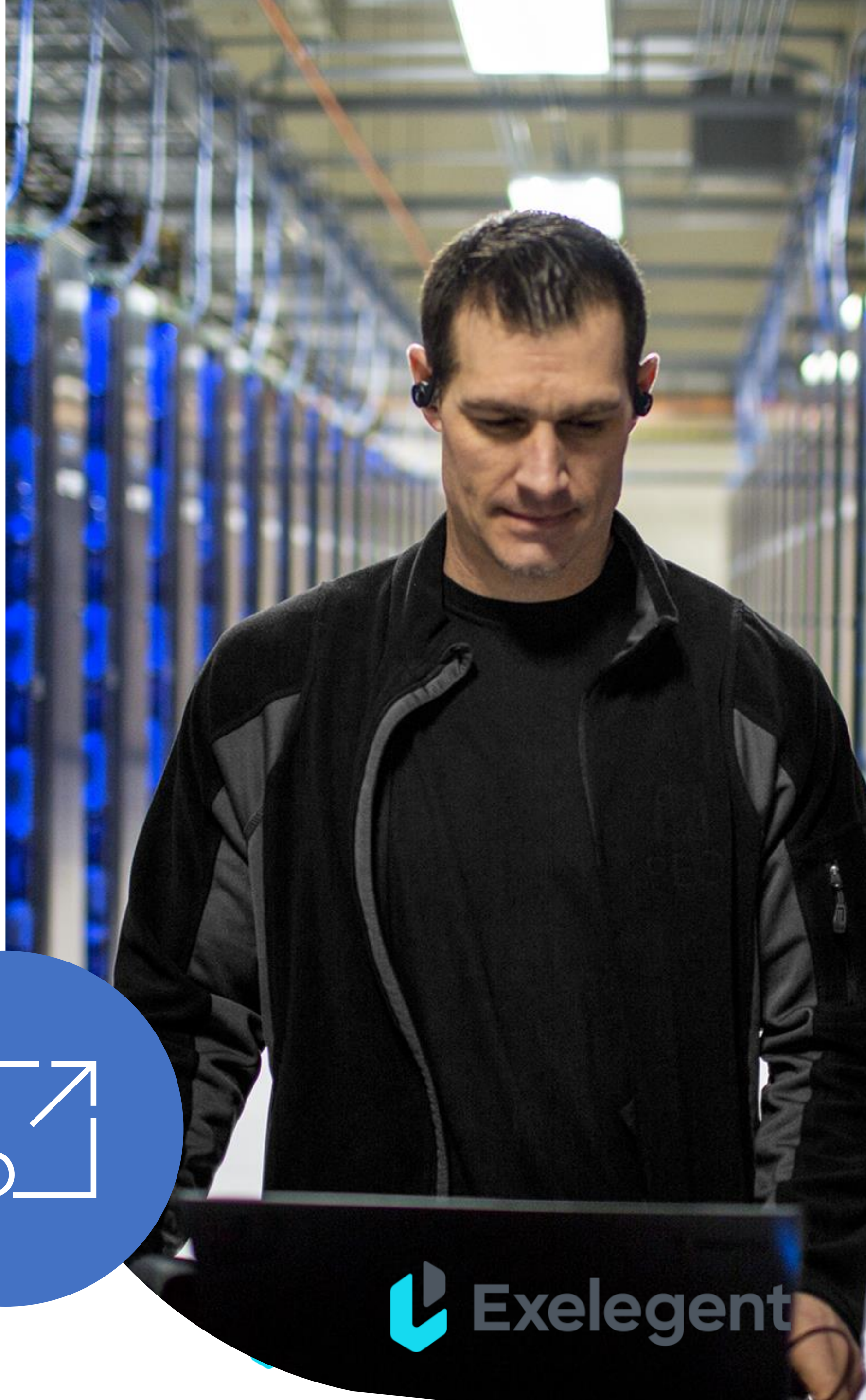
Expedite incident response

Get ahead of attackers

Exelegent

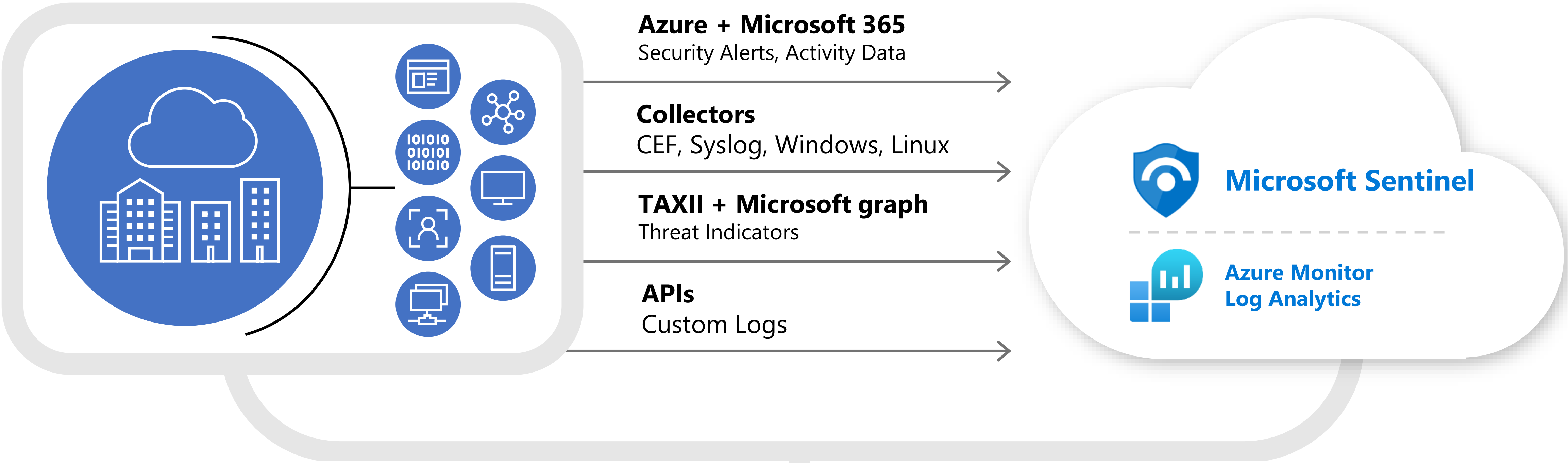
Harness the scale of cloud-native SIEM

- Eliminate infrastructure setup or maintenance
- Put no limits to compute or storage resources and scale at will
- Collect and analyze data across your entire organization at cloud scale
- Pay only for what you use—resulting in a SIEM 48% less expensive than traditional SIEMs*



*Forrester Consulting, Total Economic Impact™ of Microsoft Azure Sentinel, 2020

Collect security data at cloud scale from any source



Azure + Microsoft 365
Security Alerts, Activity Data

Collectors
CEF, Syslog, Windows, Linux

TAXII + Microsoft graph
Threat Indicators

APIs
Custom Logs

Microsoft Sentinel

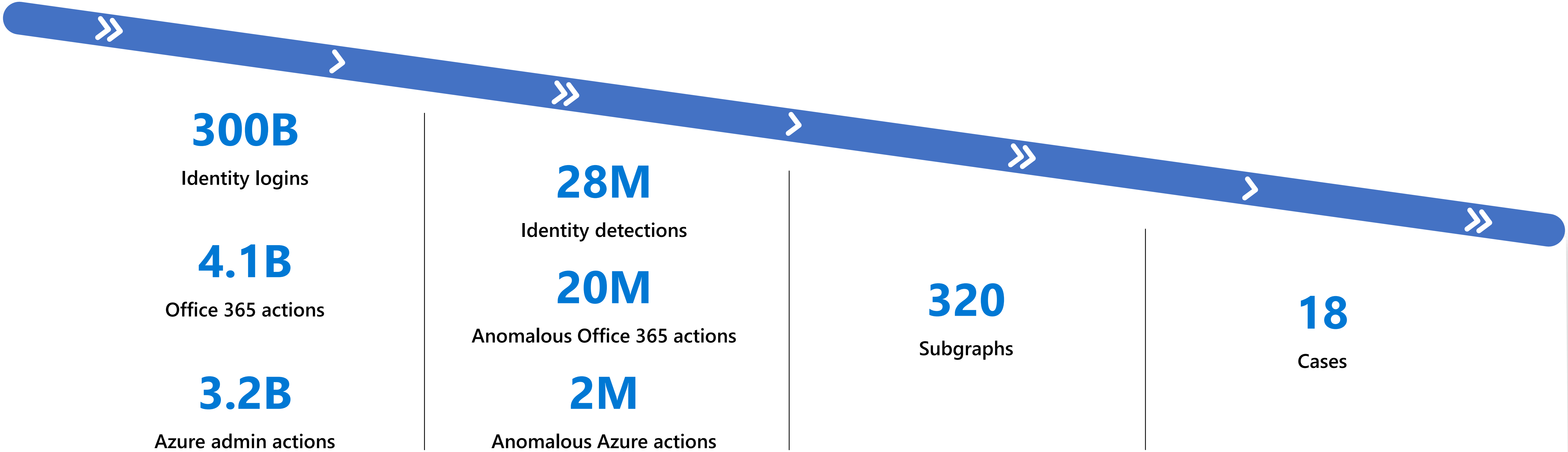
Azure Monitor
Log Analytics

Proven log platform with more than 10 petabytes of daily ingestion

Exelegent

Reducing alert fatigue

Analyzing activities across multiple cloud services into high-fidelity security cases



300B
Identity logins

4.1B
Office 365 actions

3.2B
Azure admin actions

28M
Identity detections

20M
Anomalous Office 365 actions

2M
Anomalous Azure actions

320
Subgraphs

18
Cases

Service layer
raw events

Anomalous behaviors
and detections

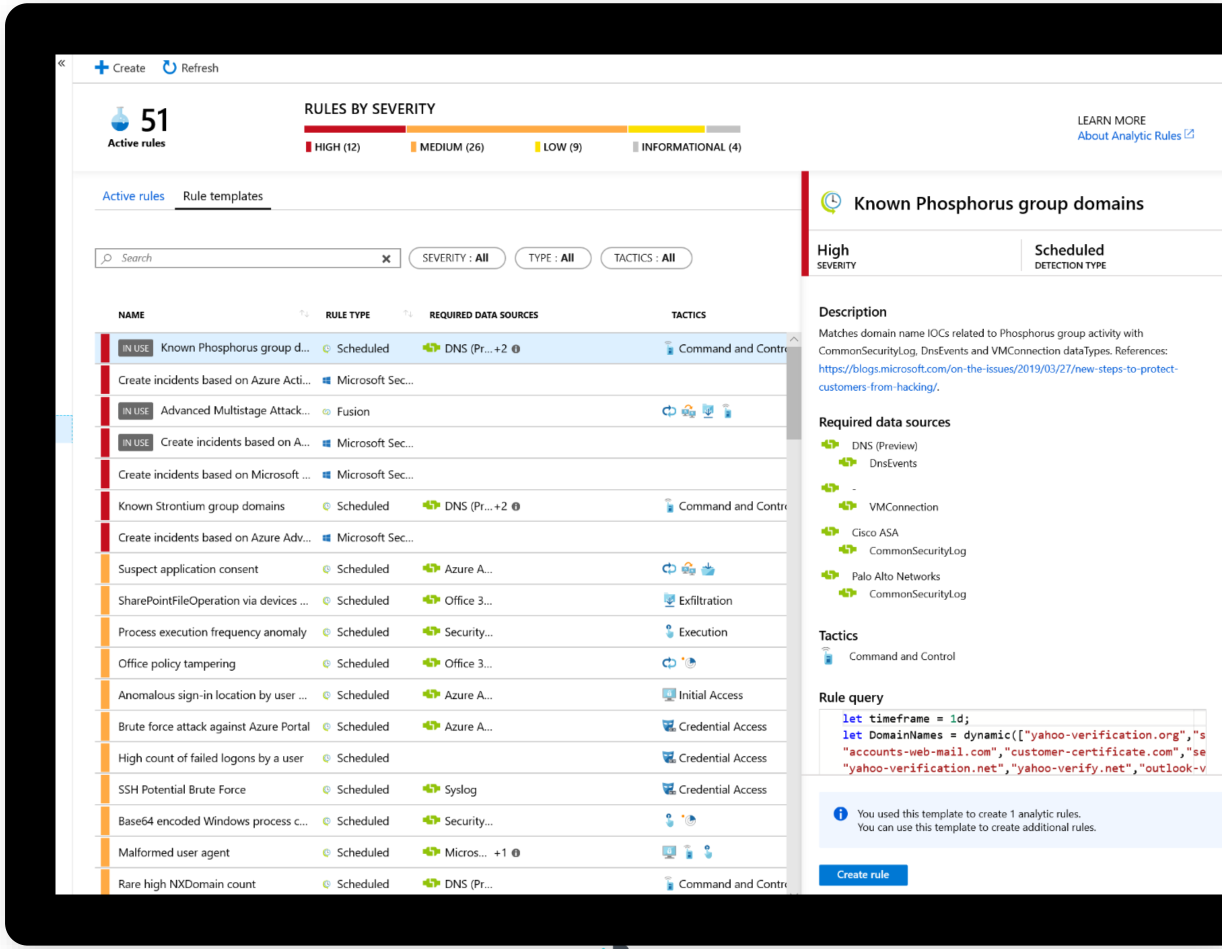
Convert
to graph

Score each subgraph
with Machine Learning

Exelegent

Leverage extensive library of detections or build your own

- → Choose from more than 100 built-in analytics rules
- → Customize and create your own rules using KQL queries
- → Correlate events with your threat intelligence and now with Microsoft URL intelligence + network data
- → Democratize machine learning with code-free, customizable ML anomaly detections



51
Active rules

RULES BY SEVERITY
HIGH (12) MEDIUM (26) LOW (9) INFORMATIONAL (4)

LEARN MORE
About Analytic Rules

NAME	RULE TYPE	REQUIRED DATA SOURCES	TACTICS
IN USE Known Phosphorus group d...	Scheduled	DNS (Pr... +2	Command and Contr
Create incidents based on Azure Acti...	Microsoft Sec...		
IN USE Advanced Multistage Attack...	Fusion		
IN USE Create incidents based on A...	Microsoft Sec...		
Create incidents based on Microsoft ...	Microsoft Sec...		
Known Strontium group domains	Scheduled	DNS (Pr... +2	Command and Contr
Create incidents based on Azure Adv...	Microsoft Sec...		
Suspect application consent	Scheduled	Azure A...	
SharePointFileOperation via devices ...	Scheduled	Office 3...	Exfiltration
Process execution frequency anomaly	Scheduled	Security...	Execution
Office policy tampering	Scheduled	Office 3...	
Anomalous sign-in location by user ...	Scheduled	Azure A...	Initial Access
Brute force attack against Azure Portal	Scheduled	Azure A...	Credential Access
High count of failed logons by a user	Scheduled		Credential Access
SSH Potential Brute Force	Scheduled	Syslog	Credential Access
Base64 encoded Windows process c...	Scheduled	Security...	
Malformed user agent	Scheduled	Micros... +1	
Rare high NXDomain count	Scheduled	DNS (Pr...	Command and Contr

Known Phosphorus group domains

High
SEVERITY

Scheduled
DETECTION TYPE

Description

Matches domain name IOCs related to Phosphorus group activity with CommonSecurityLog, DnsEvents and VMConnection dataTypes. References: https://blogs.microsoft.com/on-the-issues/2019/03/27/new-steps-to-protect-customers-from-hacking/.

Required data sources

DNS (Preview)
  DnsEvents
-
  VMConnection
Cisco ASA
  CommonSecurityLog
Palo Alto Networks
  CommonSecurityLog

Tactics

Command and Control

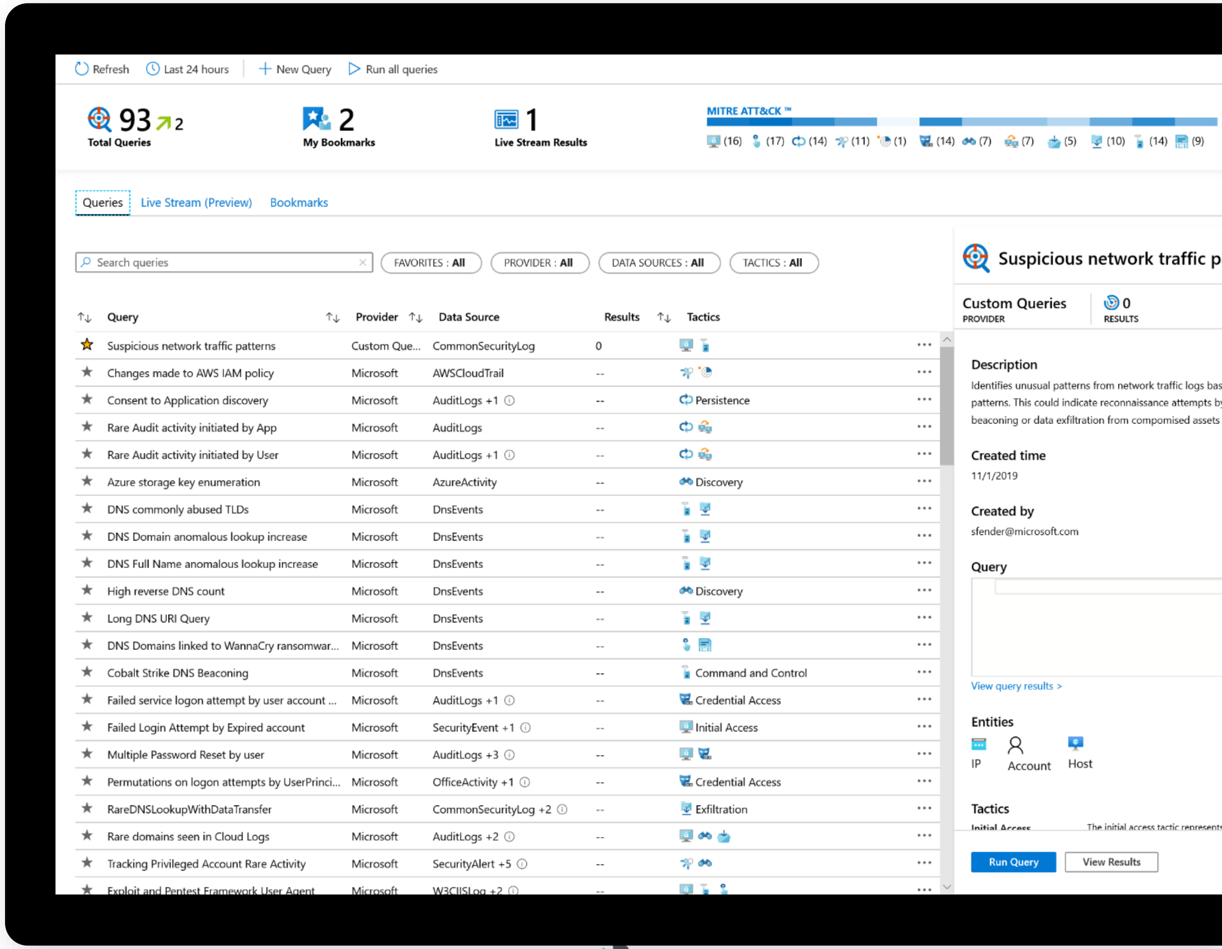
Rule query

```
let timeframe = 1d;
let DomainNames = dynamic(["yahoo-verification.org","s
"accounts-web-mail.com","customer-certificate.com","se
"yahoo-verification.net","yahoo-verify.net","outlook-v
```

You used this template to create 1 analytic rules.
You can use this template to create additional rules.

Start hunting over security data with fast, flexible queries

- → Run built-in threat hunting queries—no prior query experience required
- → Customize and create your own hunting queries using KQL
- → Integrate hunting and investigations
- → Use bookmarks and live stream to manage your hunts



Query	Provider	Data Source	Results	Tactics
Suspicious network traffic patterns	Custom Que...	CommonSecurityLog	0	
Changes made to AWS IAM policy	Microsoft	AWSCloudTrail	--	
Consent to Application discovery	Microsoft	AuditLogs +1	--	Persistence
Rare Audit activity initiated by App	Microsoft	AuditLogs	--	
Rare Audit activity initiated by User	Microsoft	AuditLogs +1	--	
Azure storage key enumeration	Microsoft	AzureActivity	--	Discovery
DNS commonly abused TLDs	Microsoft	DnsEvents	--	
DNS Domain anomalous lookup increase	Microsoft	DnsEvents	--	
DNS Full Name anomalous lookup increase	Microsoft	DnsEvents	--	
High reverse DNS count	Microsoft	DnsEvents	--	Discovery
Long DNS URI Query	Microsoft	DnsEvents	--	
DNS Domains linked to WannaCry ransomwar...	Microsoft	DnsEvents	--	
Cobalt Strike DNS Beaconing	Microsoft	DnsEvents	--	Command and Control
Failed service logon attempt by user account ...	Microsoft	AuditLogs +1	--	Credential Access
Failed Login Attempt by Expired account	Microsoft	SecurityEvent +1	--	Initial Access
Multiple Password Reset by user	Microsoft	AuditLogs +3	--	
Permutations on logon attempts by UserPrinci...	Microsoft	OfficeActivity +1	--	Credential Access
RareDNSLookupWithDataTransfer	Microsoft	CommonSecurityLog +2	--	Exfiltration
Rare domains seen in Cloud Logs	Microsoft	AuditLogs +2	--	
Tracking Privileged Account Rare Activity	Microsoft	SecurityAlert +5	--	
Exploit and Pentest Framework User Agent	Microsoft	W3CIISLog +2	--	

Suspicious network traffic p

Custom Queries
PROVIDER

0
RESULTS

Description

Identifies unusual patterns from network traffic logs bas
patterns. This could indicate reconnaissance attempts b
beaconing or data exfiltration from compomised assets

Created time

11/1/2019

Created by

sfender@microsoft.com

Query

View query results >

Entities

IP Account Host

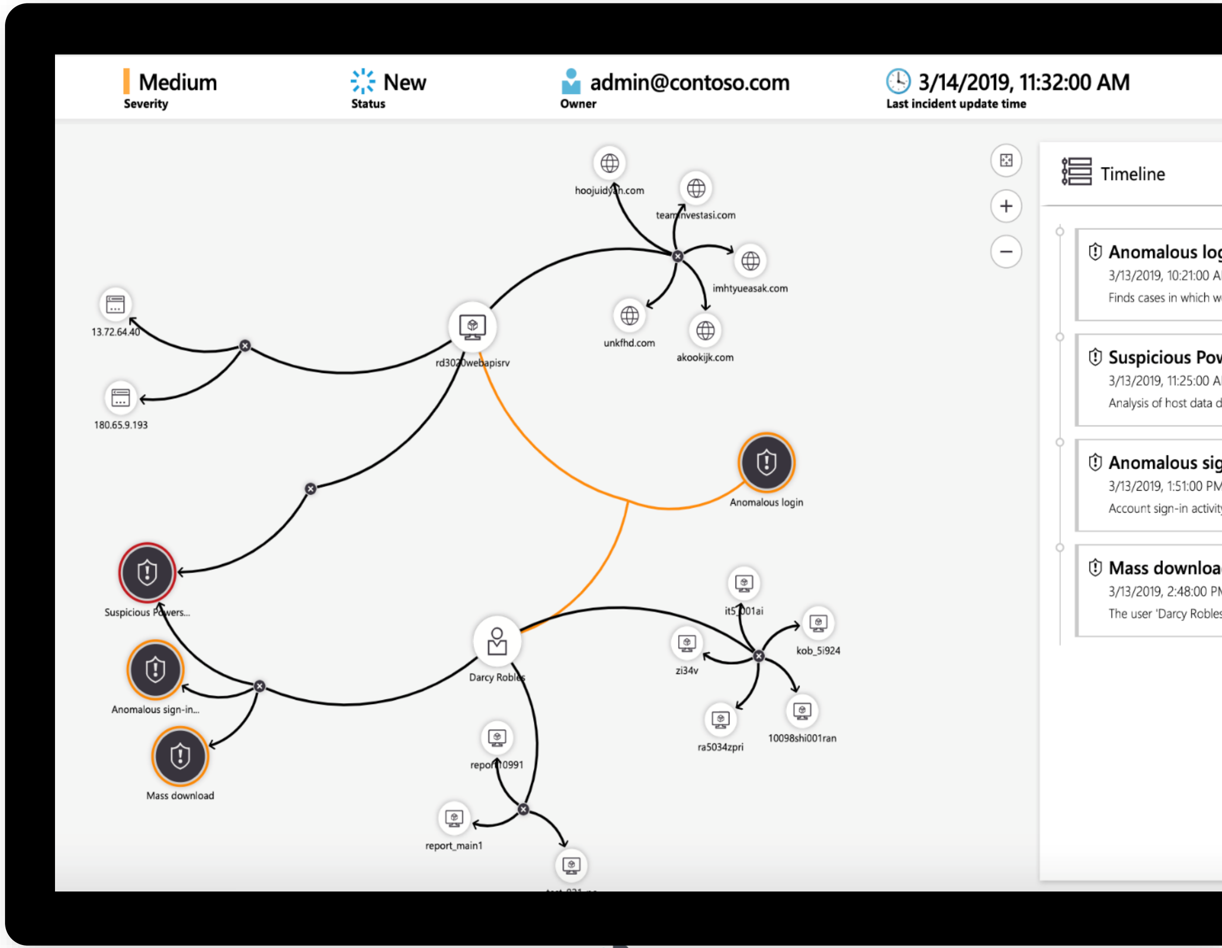
Tactics

Initial Access The initial access tactic represents

Visualize the entire attack to determine scope and impact

- → Navigate the relationships between related alerts, bookmarks, and entities
- → Expand the scope using exploration queries
- → Gain deep insights into related entities—users, domains, and more

80% reduction in investigation effort
compared to legacy SIEMs[1]



Medium
Severity

New
Status

admin@contoso.com
Owner

3/14/2019, 11:32:00 AM
Last incident update time

Timeline

Anomalous log
3/13/2019, 10:21:00 A
Finds cases in which w

Suspicious Pow
3/13/2019, 11:25:00 A
Analysis of host data d

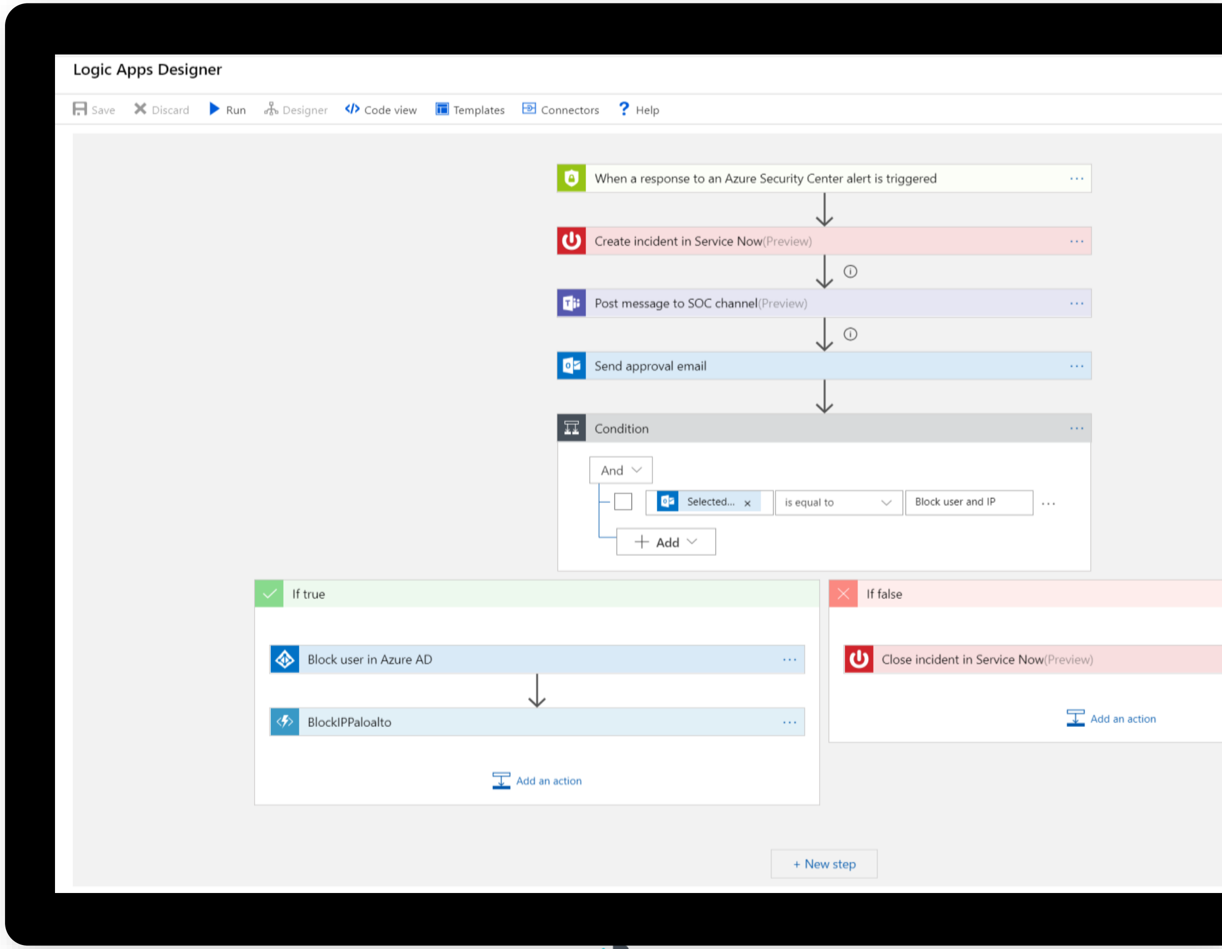
Anomalous sig
3/13/2019, 1:51:00 PM
Account sign-in activit

Mass downloa
3/13/2019, 2:48:00 PM
The user 'Darcy Robles

[1] Commissioned study-The Total Economic Impact™ of Microsoft Azure Sentinel, conducted by Forrester Consulting, 2020

Automate and orchestrate security operations using integrated Azure Logic Apps

- → Build automated and scalable playbooks that integrate across tools
- → Choose from a library of samples
- → Create your own playbooks using 200+ built-in connectors
- → Trigger a playbook from an alert or incident investigation

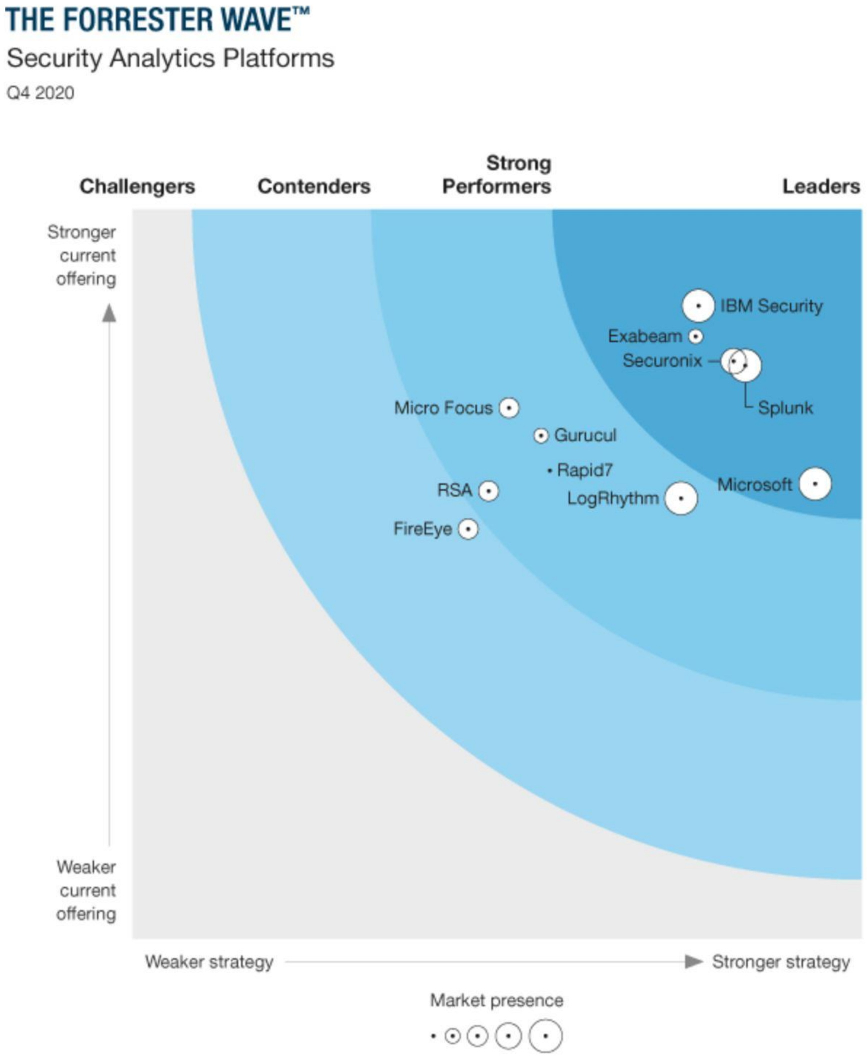


Exelegent

FORRESTER®

“**Microsoft roars into the security analytics market…**
The vendor’s entry into the security analytics space captivated security buyers. Microsoft’s bold move to allow the ingestion of Microsoft Azure and Microsoft Office 365 activity logs into Sentinel at no cost makes the solution attractive to enterprises invested in Azure and Microsoft 365.”

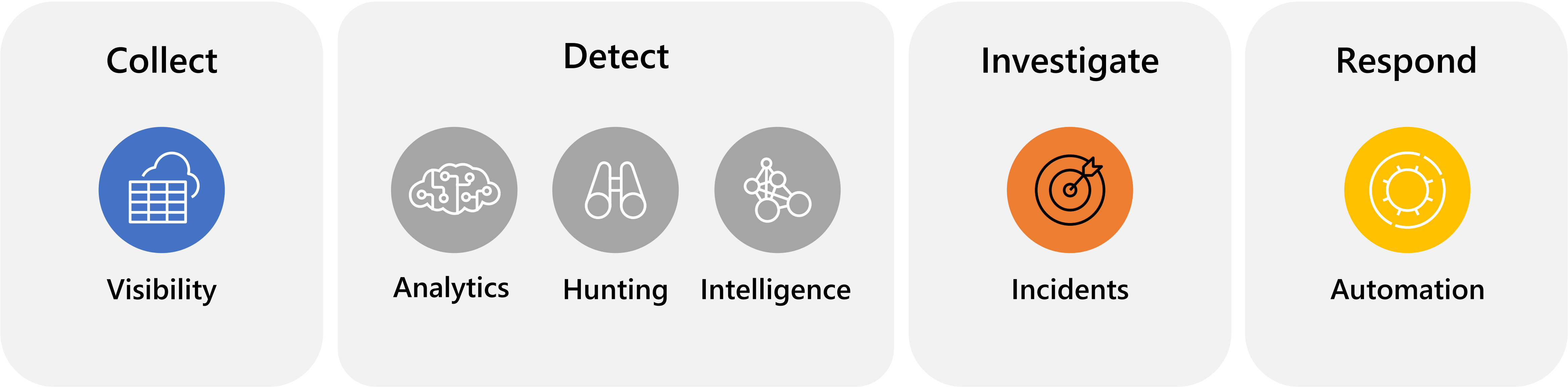
- The Forrester Wave™: Security Analytics Platforms, Q4 2020 report



The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave™ are trademarks of Forrester Research, Inc. The Forrester Wave™ is a graphical representation of Forrester’s call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave™. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

An end-to-end solution for security operations

« Powered by community + backed by Microsoft's security experts »



Analyze

- Business and IT requirements
- Existing SIEM/SOC tools
- Data sources to be connected
- Security Operations automation requirements

Define scope & deploy

- Define the scope of the Microsoft Sentinel deployment
- Deploy and configure Microsoft Sentinel
- Connect Microsoft Sentinel to ingest data from:
    - Azure AD Identity Protection
    - Microsoft Defender for Cloud Apps
    - Microsoft Defender for Office 365
    - Agreed 3rd party Syslog integration
    - Limited nr. of on-premises servers

Remote Monitoring

- Remote incident monitoring during the data collection phase
- **Optional -** Threat hunting to discover Indicators of Attack in the ingested data

Discover

- Use Microsoft Sentinel to analyze and discover threats to your organization

Recommend

- Map found threats to Microsoft 365 security products
- Provide a Microsoft Sentinel deployment roadmap

Exelegent

Kick-off Meeting

Introduce the Microsoft Sentinel Workshop engagement, discuss the upcoming activities, align expectations and establish timelines.

Define Scope

Define and finalize the engagement scope and required configuration settings for the engagement tools.

Threat Check Configuration

Deploy and configure the Microsoft 365 security tools in your production tenant.

Microsoft Sentinel Configuration

Deploy and configure Microsoft Sentinel in your production tenant.

Engagement scenarios

Scenario 1 – Remote monitoring of threats

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 Microsoft 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 Microsoft Sentinel for incidents during the engagement.
- Optional - Proactive threat hunting - Our security analysts will use Microsoft 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 Microsoft Sentinel instance in your tenant using delegated access through either Azure B2B or Azure Lighthouse (recommended)

Scenario 2 – Joint threat exploration

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

- Experience Microsoft Sentinel - Get hands-on experience and learn how to discover and analyze threats using Microsoft 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

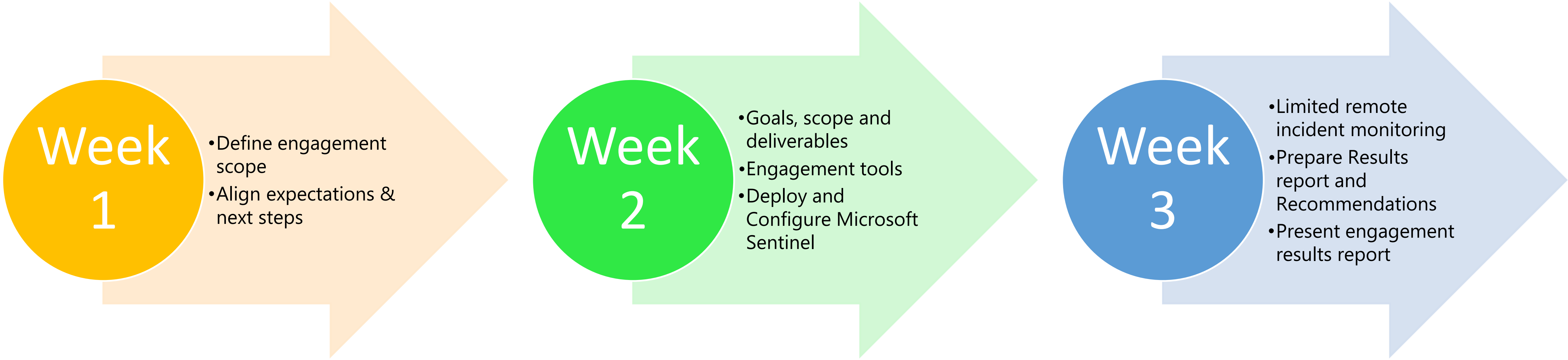
- **Incident response** - Not included in the default scope

Requirements

- No additional requirements necessary

Exelegent

Weekly Agenda



Week 1

- Define engagement scope
- Align expectations & next steps

Week 2

- Goals, scope and deliverables
- Engagement tools
- Deploy and Configure Microsoft Sentinel

Week 3

- Limited remote incident monitoring
- Prepare Results report and Recommendations
- Present engagement results report

Pre-engagement Call – 1-hour

Goals:

- Introductions
- Engagement overview
- Define engagement scope
- Identify right stakeholders
- Engagement scheduling
- Align expectations & next steps
- Provide engagement questionnaire

Kick-Off – 1-hour

Goals:

- Kick-off meeting
    - Goals, scope and deliverables
    - Engagement tools
    - Expectations and next steps

Define Scope – 1-hour

Goals:

- Define and document deployment scope

Threat Check and Microsoft Sentinel Configuration – 4 hours

Goals:

- Set-up trial license
- Deploy and Configure Microsoft Sentinel
- Setup Azure Lighthouse

Remote Monitoring – 2h/week

Goals:

- Limited remote incident monitoring
- Proactive threat hunting

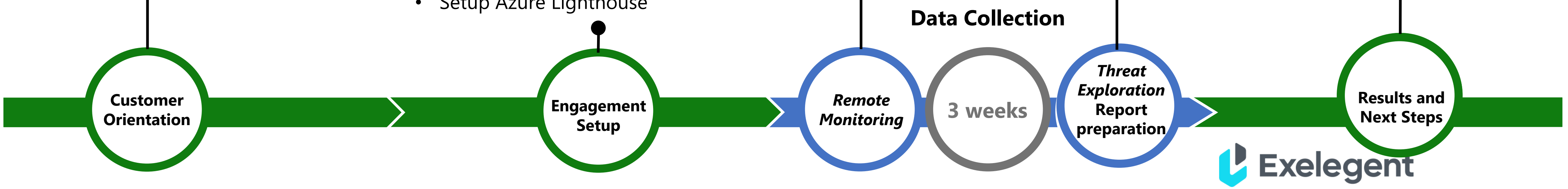
Threat Exploration and Report Generation – 5 hours

Goals:

- Threat Exploration
- Prepare Results report and Recommendations

Results Presentation – 2 hours

- Present engagement results report
- Joint plan and next steps



Customer Orientation

Engagement Setup

Data Collection

Remote Monitoring

3 weeks

***Threat Exploration* Report preparation**

Results and Next Steps