An Ode to Cybersecurity

In digital realms where secrets dwell, cyber guardians stand without fear
Vigilance unyielding and purpose clear

When breaches occur, they arise to analyze forensic and clues
Tracing digital footprints, seeking the source
Thwarting the adversary's remorseless course.

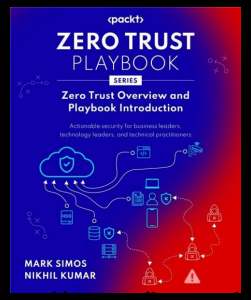
So here's to the defenders, the silent brigade
Their battle fought in the binary shade
They stand as our shield, night and day.

- Copilot with prompting/editing by Mark Simos

The No BS SOC

Mark Simos

Lead Cybersecurity Architect, Microsoft
Zero Trust Architecture Co-Chair, The Open Group
Author, ZeroTrustPlaybook.com

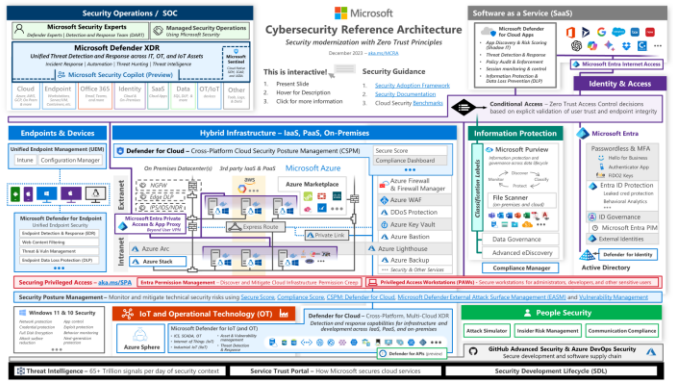


aka.ms/MarksList

Agenda – the No BS SOC

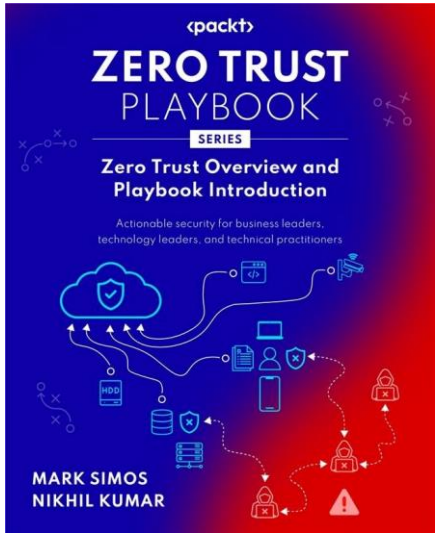
- **Who is this dude? Where does this come from?**
- **Where does the SOC BS come from?**
- **SecOps Antipatterns –** *Common mistakes across SOCs*
- **What does good look like?** *Mission, Success Factors, & Metrics*
- **Challenges –** Continuously Changing Threats & Risk of Burnout
- **How is AI changing SecOps?**
- **Story of a SOC -** *How SecOps Teams, Careers, and Skills Grow*
- **Call To Action:** *Stay Focused on What Matters!*

About the Chef
Mark Simos



Lead Cybersecurity Architect
Microsoft

Zero Trust Architecture Co-Chair
The Open Group

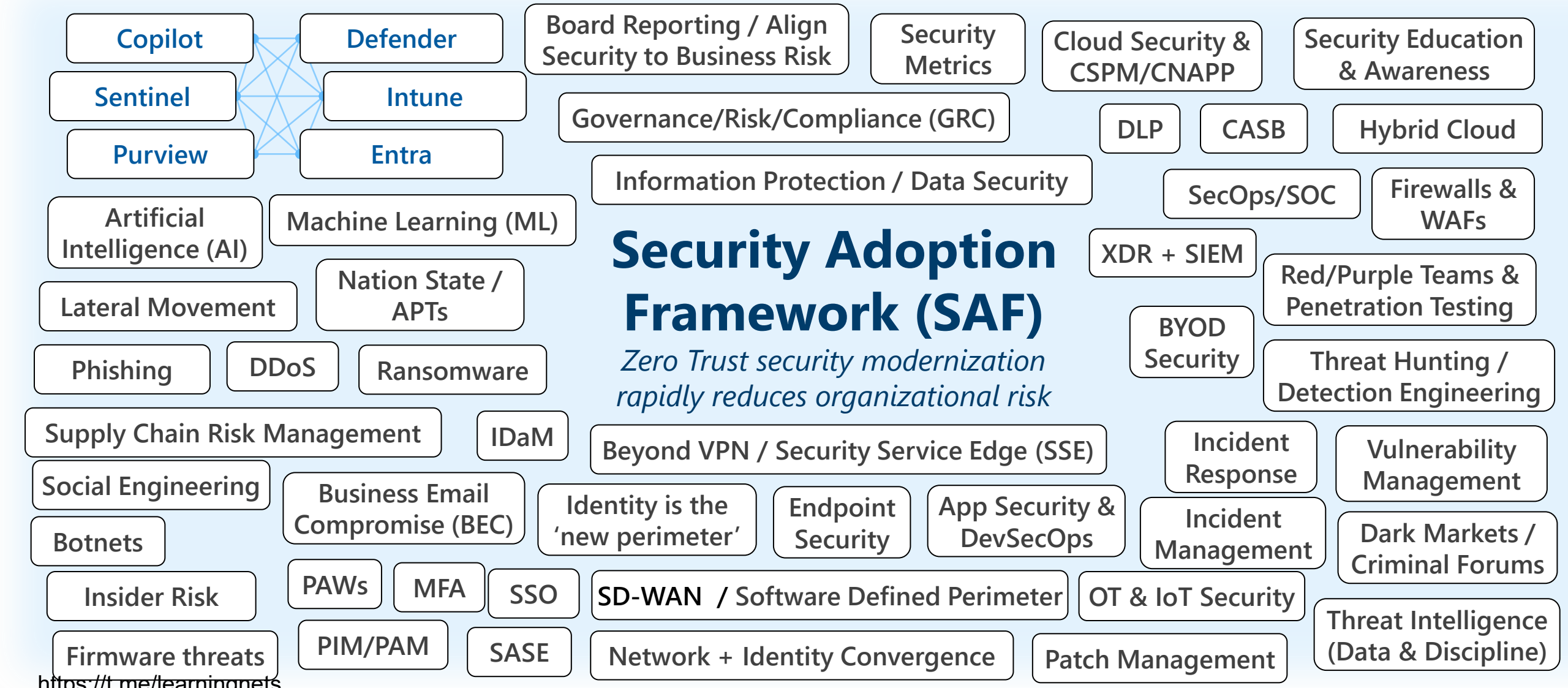


Author, Zero Trust Playbook
ZeroTrustPlaybook.com

aka.ms/MarksList

SAF Brings Clarity to Security

Enables security execution by connecting and organizing security problems, solutions, and models



Security Adoption Framework (SAF)

Zero Trust security modernization rapidly reduces organizational risk

Microsoft

CEO

Business Leadership

CIO CISO

Technical Leadership

Architects & Technical Managers

Implementation

Securing Digital Transformation

Business and Security Integration

Security Strategy, Programs, and Epics

Architecture and Policy

Technical Planning

Implementation and Operation

Engaging Business Leaders on Security

Security Strategy and Program

CISO Workshop

End to End Zero Trust Architecture

Microsoft Cybersecurity Reference Architectures (MCRA)

Secure Identities and Access

Modern Security Operations (SecOps/SOC)

Infrastructure & Development Security

Data Security & Governance

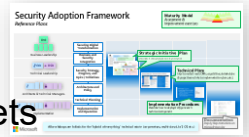
IoT and OT Security

Technical Capabilities Implementation

Security Capability Adoption Planning (SCAP)

Technology Implementation & Optimization

Includes Reference Plans



Workshops available in Microsoft Unified

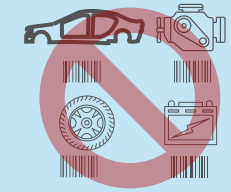
Coordinated & integrated *end-to-end security across the '**hybrid of everything**' (on-prem, multi-cloud, IoT, OT, etc.)*

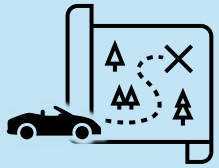
Where does the SOC BS come from?

‘Silver Bullet’ Mindset

Believing a single solution could magically 100% solve a complex problem

- *Making/believing an absolute claim*
- *Waiting for a perfect solution*
- *Lack of lifecycle thinking*





Technology-Centric Thinking

Believing security is about technology instead of protecting an organization’s business assets

- *Ignoring burnout, collaboration, training, etc.*
- *Expecting tools solve people/process problems*

Adversaries have a goal and a plan. *Do you?*

\+ Money

Common BS

- **Too high level** *(not actionable)*
- **Too low level** *(too technical/specific)*
- **Vendor Biased**
- **Outdated or Just Plain Wrong**

Contain nuggets of wisdom, but they are buried in poop

Security Operations

Mission

Reduce organizational risk by limiting the attacker dwell time (how long attackers can access business assets) through rapid detection and response.

Key Cultural Elements

- Mission Alignment
- Continuous Learning
- Teamwork

Partner for Success

SecOps requires strong relationships and processes to help architects and engineers block preventable attacks (which otherwise flood SecOps)

Key Measurements

Metrics should never be punitive
Attackers have a vote too!

- **Attacker Dwell Time –** via Mean Time to Remediate (MTTR)
- **Responsiveness/Capacity -** Mean Time to Acknowledge (MTTA)

What Matters in Security Operations?

Microsoft CDOC is main source of best practices

Best practices and recommendations are directly sourced from Microsoft's Cyber Defense Operations Center (CDOC) or validated against current practices.

Minutes Matter – rapidly detecting and evicting attackers will limit damage and risk to your organization

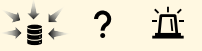
- **People matter –** Human judgement is critical. Continuous learning is required to keep up with technology, processes, and attack techniques.
- **Process matters –** clarity and execution across internal and external teams is required for accuracy, impact, and speed.
- **Technology matters –** Simplify and automate common tasks to reduce frustration/burnout and keep people focused where needed most.
- **Intelligence matters –** to provide current context for people and tools

Teamwork matters! – Collaboration across individuals & teams is critical to success!

Common Security Operations (SecOps/SOC) antipatterns

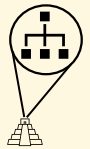
Common mistakes impede SecOps effectiveness and increase burnout

Implementation without requirements



Collection is not Detection

*Focusing on collecting data instead of **finding and removing adversary access***

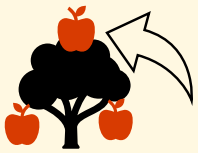


'Network is only source of truth'

false belief that you only need network data to detect and investigate attacks

Not invented here

focusing on custom solutions and queries instead of established commercial tooling



Shiny Object Syndrome

Prioritizing "cool" advanced scenarios/tools before critical basic outcomes and controls

One tool to rule them all

False belief that a single tool solves all problems (SIEM, EDR, or other)

Toolapalooza!

*Buying many tools without integration forces analysts into **swivel chair analytics** mode*

Best practice – Develop and implement a Security Operations (SecOps/SOC) strategy focused on clear outcomes across people, process, and technology

This workshop includes references to help you define and rapidly improve:

- *Mission and Metrics*
- *Organizational Functions and Teams (including use cases and scenarios)*
- *Business and Technical processes*
- *SOC Architecture, Tooling, and Integration*
- *Skill education and enablement*
- *Automation Strategy*
- *Data strategy*

Recommended SecOps Metrics

Metrics should never be punitive
Attackers have a vote too!

Direct organizational risk

Analyst capacity (for actual caseload)

Understand impact on human analysts

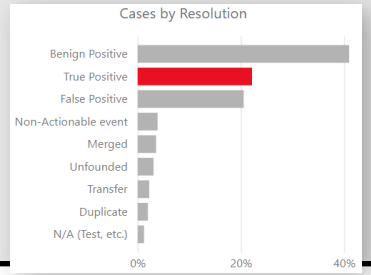
SOAR effectiveness

Detection Noisiness/Quality

How reliable are tools

General view of trends

Status	Metric	Target	Current & Previous Months			
	Dwell Time: Mean Time to Remediate (MTTR)	*<## hours*				
	Responsiveness: Mean Time to Acknowledge (MTTA)	*<## minutes*				
	Caseload: # Cases Handled by each team	*Tracking*				
	Automation: # of Cases processed by SOAR	*Tracking*				
	Detection Fidelity: % True Positive + Benign Positive	*>##%*				
	SecOps Platform Availability: % of uptime	*>##%*				
	Case Resolution: Case volume by resolution					

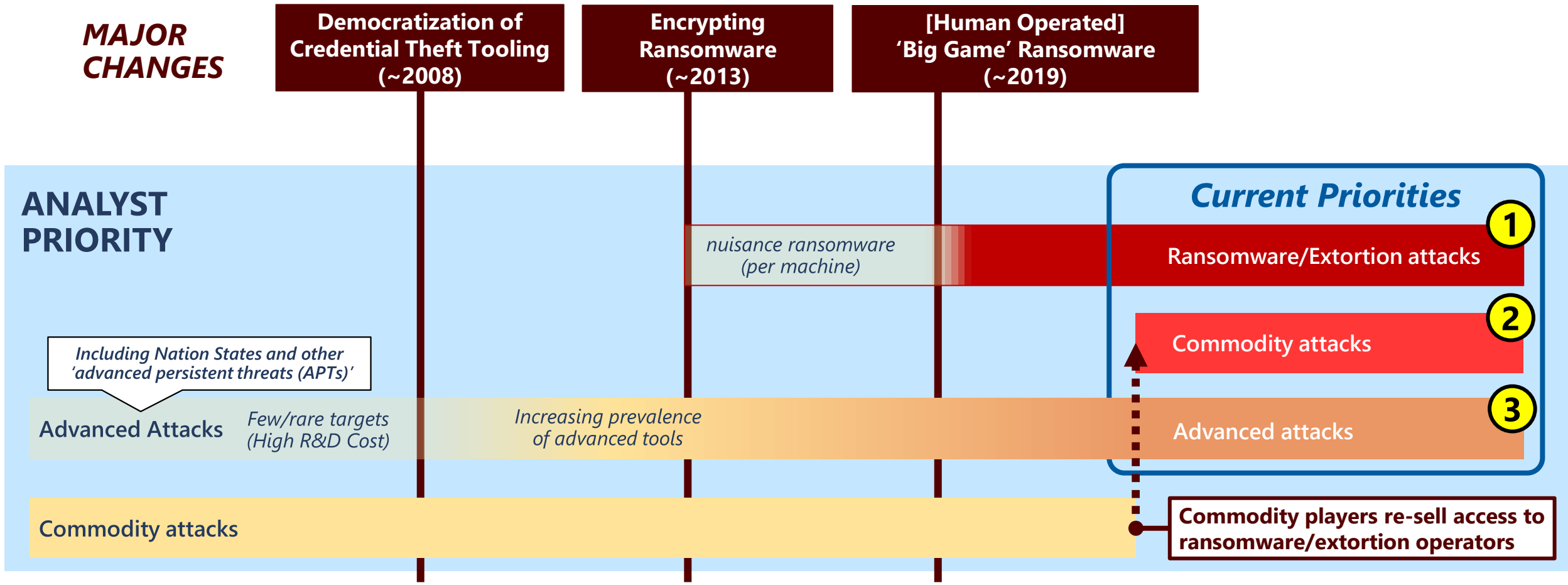


Track Trends
to understand changes from

- *Adversaries & Threats*
- *SecOps investments (detections, tools, process improvements, training, staffing levels, etc.)*

Evolution of threats and security analyst priorities

Ruthlessly prioritize: Every incident is important, but urgency will vary



The passion that drives greatness can also cause burnout

Address each source of fatigue that leads to burnout and attrition

Managers burn out too!

Schedule time for rest, learning, & self-care

Document & celebrate wins

Protecting the organization

Exhaustion
non-stop investigation and eviction of attackers

No recognition
For hard work, skills, and contributions

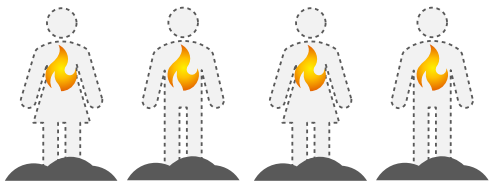
Wasted Effort
on false positives & repetitive manual tasks

Prioritize ruthlessly
What is critical vs. ***what to ignore!***

Improve Tooling and Processes
- Filter out low-quality detections *(requires hunting over them)*
- Automation & Advanced Analytics *(using SOAR, UEBA, and ML/AI)*
- Integrated Threat Intelligence *to enrich, filter, and prioritize detections*

Doing Other People's Jobs
Doing tasks that require different skillsets

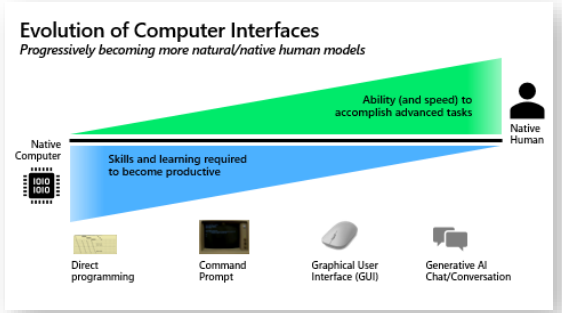
Establish and integrate supporting roles
- Implement and maintain tools *(Security Engineers)*
- Analyze/report on defense improvements *(Architects)*
- Manage & Coordinate Incidents *(Incident Management)*
- Research attacks and other questions *(Threat Intelligence)*
- Scan and report on vulnerabilities *(Posture Management)*



The Role of Artificial Intelligence (AI) in SecOps

Machine Learning is already revolutionizing SecOps

Technology integrated into XDR and SIEM technology is enabling data analysis and anomaly detection over mountains of data



Generative AI will change how SecOps works & learns

Generative AI enables a natural language computer ***interface*** that simplifies usage of complex systems and speed up learning new skills

Top Microsoft Security Copilot scenarios

Incident response capabilities are top priority
(combines Generative AI and Security-specific ML/AI capabilities)

Evolution of Computer Interfaces

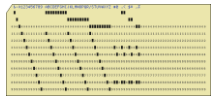
Progressively becoming more natural/native human models

Ability (and speed) to accomplish advanced tasks

Native Human

Native Computer

Skills and learning required to become productive



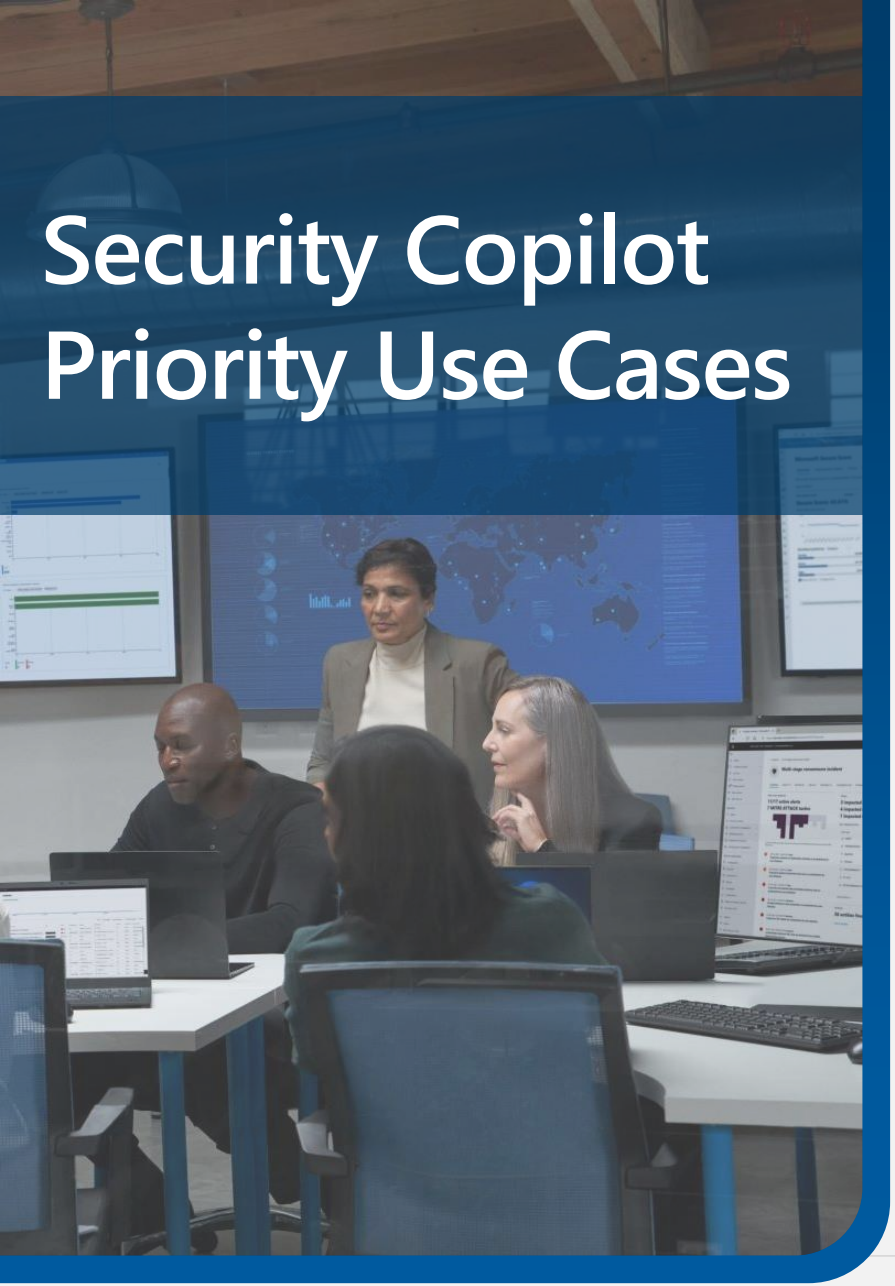
Direct programming

Command Prompt

Graphical User Interface (GUI)

Generative AI Chat/Conversation

Security Copilot Priority Use Cases



Guided Incident response

Surface an ongoing incident, assess its scale, and get instructions to begin remediation based on proven tactics from real-world security incidents.

Impact Analysis

Summarize the impact of an incident to enable better reporting and planning prioritization of mitigations against future attacks.

Incident Summarization

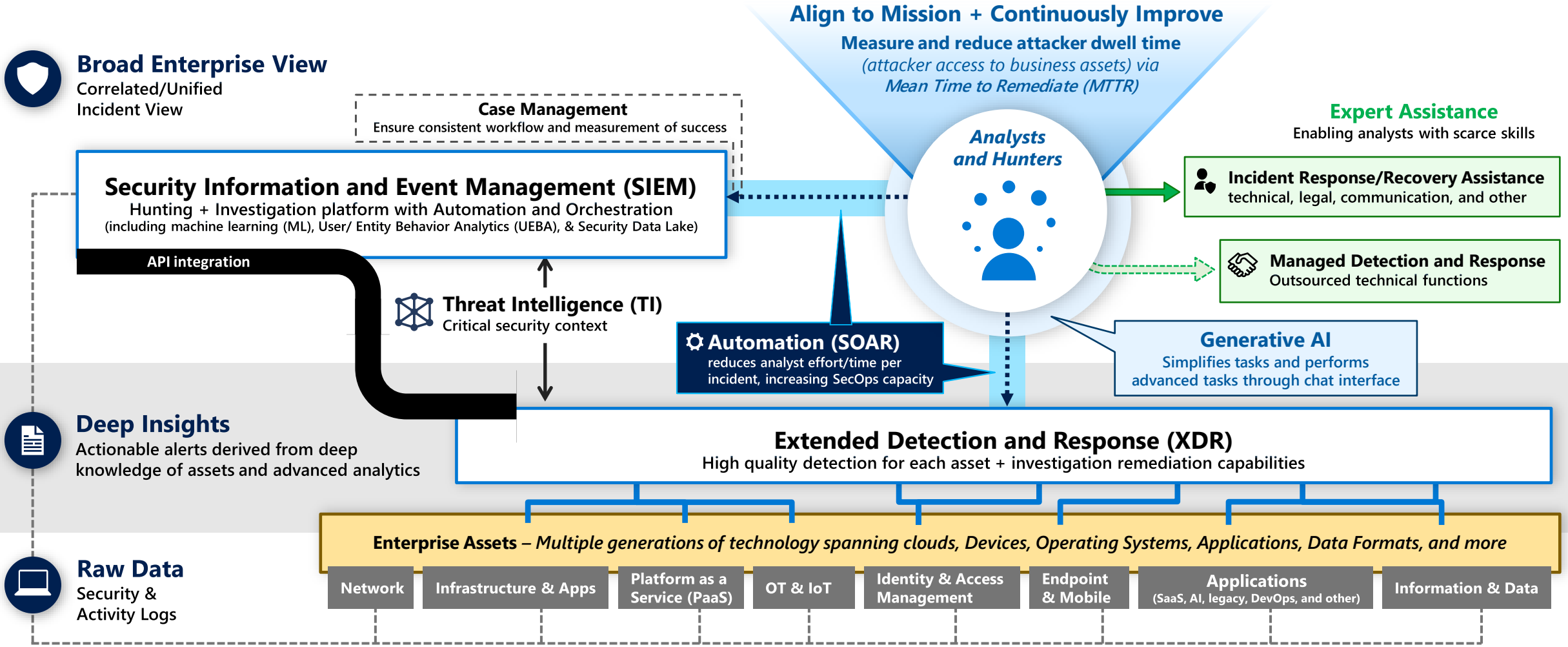
Summarize any event, incident, or threat in seconds and prepare the information in a ready-to-share, customizable report for your desired audience.

Reverse engineering of scripts

Discover whether your organization is susceptible to known vulnerabilities and exploits. Prioritize risks and address vulnerabilities with guided recommendations.

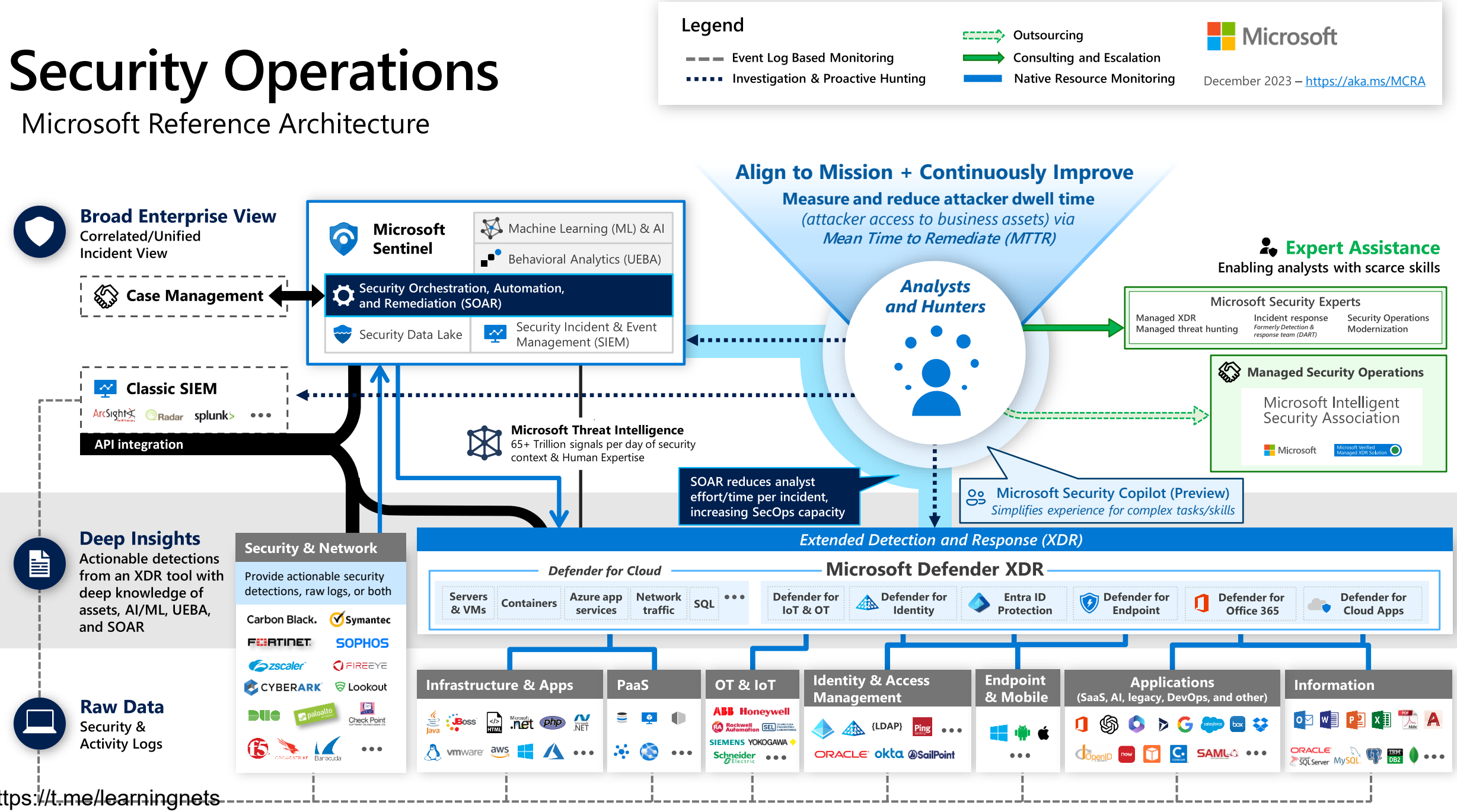
Security Operations Capabilities

Enabling a people-centric function focused rapid remediation of realized risk



Security Operations

Microsoft Reference Architecture



Evolution and Sources of SecOps Roles

As Security Operations Grows and Matures

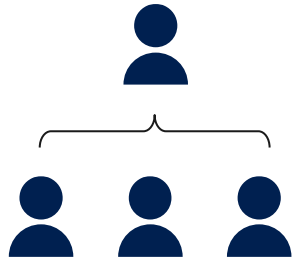
- Smaller organizations
- Large organization earlier in maturity/growth

Larger organizations (later in maturity/growth)

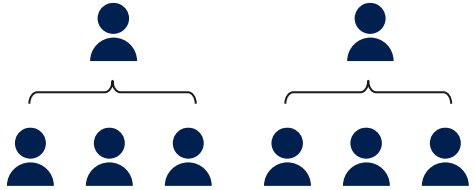
Growth Path of Security Operations

typical stages as the team grows and matures

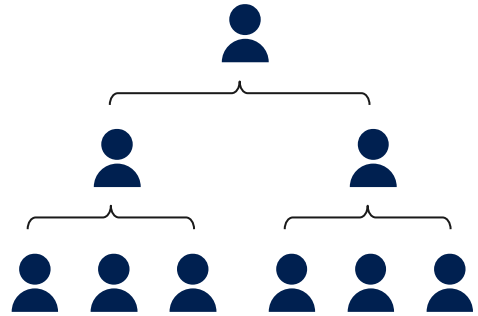
Part Time
Part time analyst duties



Small
Dedicated Team with Single Manager



Medium
Multiple SOC Managers



Large
24x7 coverage
Dedicated specialized teams

Not all organizations need (or can afford) a large team

Partnership with IT Operations and other teams is critical for any size team

Building a SecOps team – Stage 1

Part-time staffing

Legend

- Mandatory
- Optional
- On Call
- Same as Previous Stage
- Strongly Recommended
- Multiple Shifts

Detection response by part-time analysts

- *Often seen in small organizations or early stages of building a capability*
- *Sometimes staffed by non-security teams (IT Operations, Support, etc.)*

XDR is ideal for starting out (vs. SIEM)

- Simpler to install & use (less time/expertise)
- Produces results immediately
- Includes automation (SOAR) for common tasks

Many Security Operations teams started out with SIEM because it was the only technology available at the time.

Core Functions

- IR from single alert queue
- Basic Hunting
- Enforce detection quality
- 24x7 On Call

Tooling

- XDR (Endpoint/Email/Identity + Automation)
- Case management
- Security Information and Event Management (SIEM)

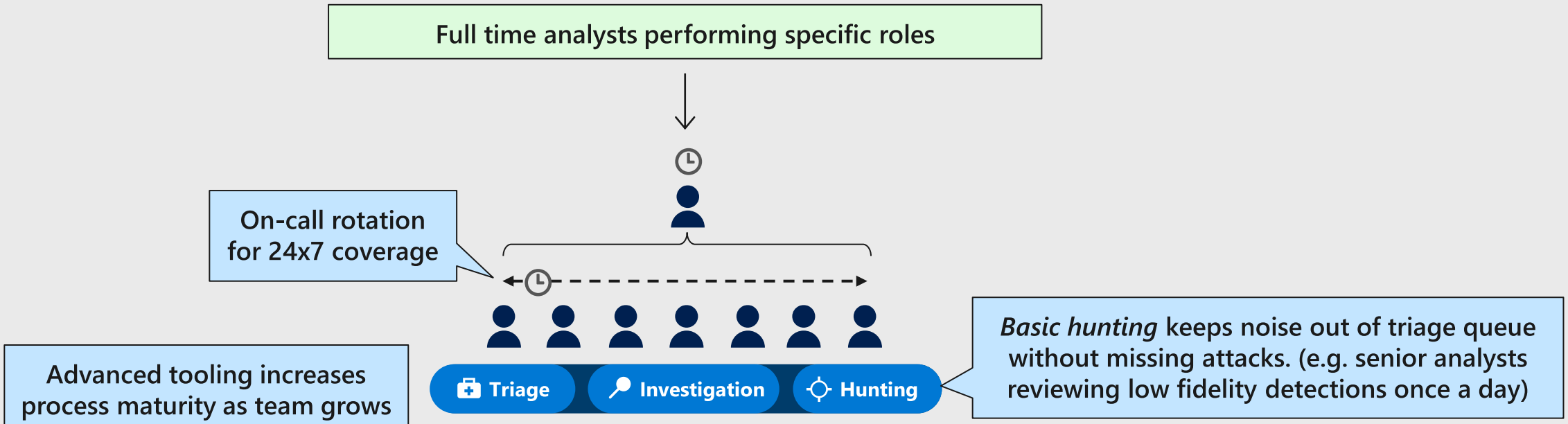
Insider Risk investigation capabilities are often incubated in security operations teams

Building a SecOps team – Stage 2

Full-time staff (small team)

Legend

- Mandatory
- Same as Previous Stage
- Optional
- Strongly Recommended
- On Call
- Multiple Shifts



Core Functions

- IR from single alert queue
- Basic Hunting
- Advanced Hunting
- Enforce detection quality
- 24x7 On Call

Tooling

- XDR (All Assets + Automation)
- Case management
- Security Information & Event Management (SIEM)
- Advanced SOAR and Analytics (AI/ML, UEBA, etc.)
- BI/Reporting Tools

Advanced/Support Functions

- (Major) Incident Management
- Threat Intelligence
- Business Intelligence/Reporting

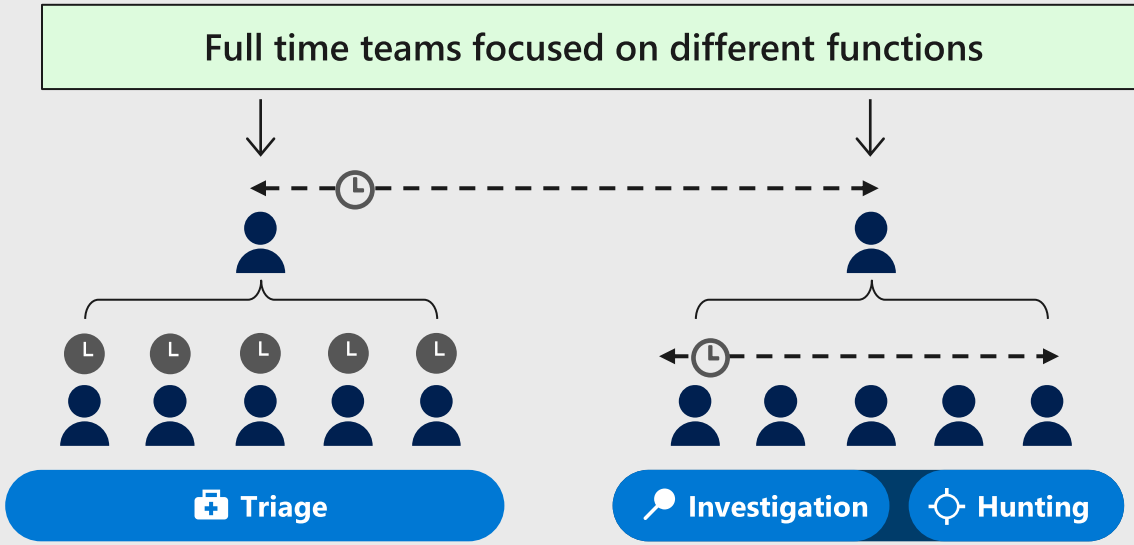
Building a SecOps team – Step 3

Full-time staff (medium team)

Legend

- Mandatory
- Same as Previous Stage
- Optional
- Strongly Recommended
- On Call
- Multiple Shifts

- Triage often extends to multiple shifts.
- On-call rotation for managers, investigation, hunting



Increasing focus on advanced SOAR automation/orchestration, advanced hunting, and Detection Engineering

Core Functions

- IR from single alert queue
- Basic Hunting / Advanced Hunting
- Enforce detection quality
- 24x7 On Call or On Shift

Tooling

- XDR (All Assets)
- Case management
- Security Information & Event Management (SIEM)
- Advanced SOAR and Analytics (AI/ML, UEBA, etc.)
- BI/Reporting Tools

Advanced/Support Functions

- (Major) Incident Management
- Threat Intelligence
- Business Intelligence/Reporting

- Define inter-team processes, metrics, tooling
- Build advanced/support functions for multi-team operations

Building a SecOps team – Step 4

Full-time staff (large team on shifts)

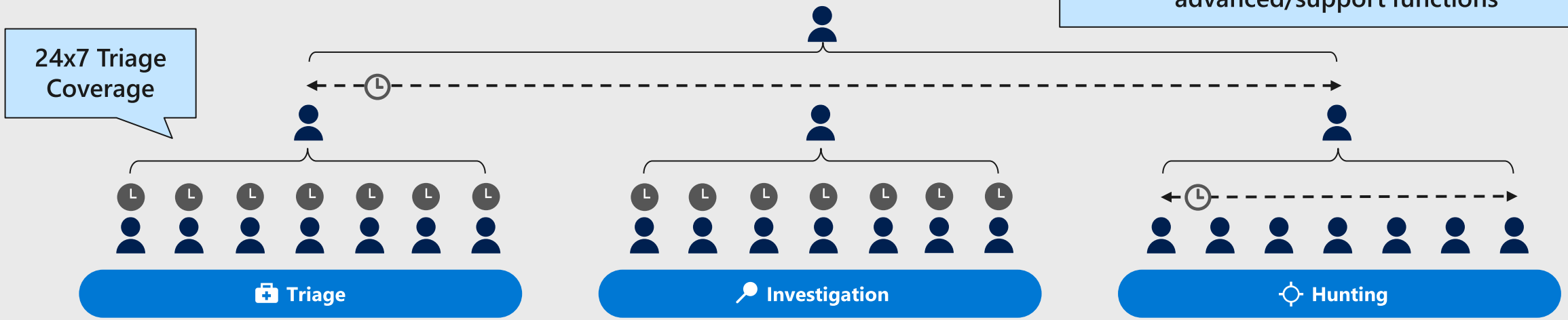
Legend

- Mandatory
- Same as Previous Stage
- Optional
- Strongly Recommended
- On Call
- Multiple Shifts

24x7 Global Operations

Complex operations require sophisticated inter-team processes, metrics, tooling, & advanced/support functions

24x7 Triage Coverage



Core Functions

- IR from single alert queue
- Advanced Hunting
- Enforce detection quality
- 24x7 On Shift

Tooling

- XDR (All Assets + Automation)
- Case management
- Security Information & Event Management (SIEM)
- Advanced SOAR and Analytics (AI/ML, UEBA, etc.)
- BI/Reporting Tools

Advanced/Support Functions

- (Major) Incident Management
- Threat Intelligence
- Business Intelligence/Reporting

Dedicate BI function enables continuous improvement

Stay Focused on what matters!

Microsoft CDOC is main source of best practices

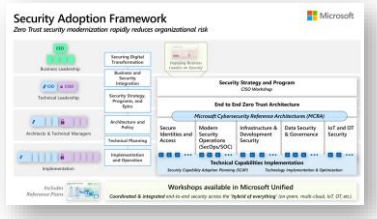
Best practices and recommendations are directly sourced from Microsoft's Cyber Defense Operations Center (CDOC) or validated against current practices.

Minutes Matter – rapidly detecting and evicting attackers will limit damage and risk to your organization

- **People matter –** Human judgement is critical. Continuous learning is required to keep up with technology, processes, and attack techniques.
- **Process matters –** clarity and execution across internal and external teams is required for accuracy, impact, and speed.
- **Technology matters –** Simplify and automate common tasks to reduce frustration/burnout and keep people focused where needed most.
- **Intelligence matters –** to provide current context for people and tools

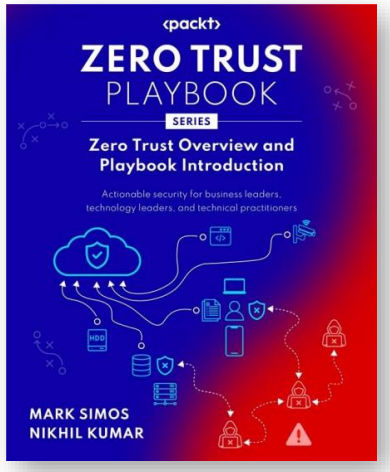
Teamwork matters! – Collaboration across individuals & teams is critical to success!

Resources. Questions?



aka.ms/SAF

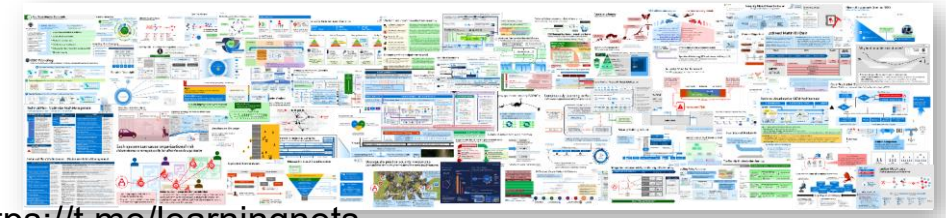
Security Adoption Framework (SAF) - *Guides Zero Trust security modernization and business alignment using recommended initiatives*



ZeroTrustPlaybook.com

For *all* roles - *Simple language and description of concepts that everyone from the board room to technologists need to understand*

- **Zero trust overview**
  Security for the modern world we are in
- **Playbook introduction**
  Methodology to get there and do it well



aka.ms/MarksList

Mark's List *...of Cybersecurity Resources frequently sent to customers and colleagues.*