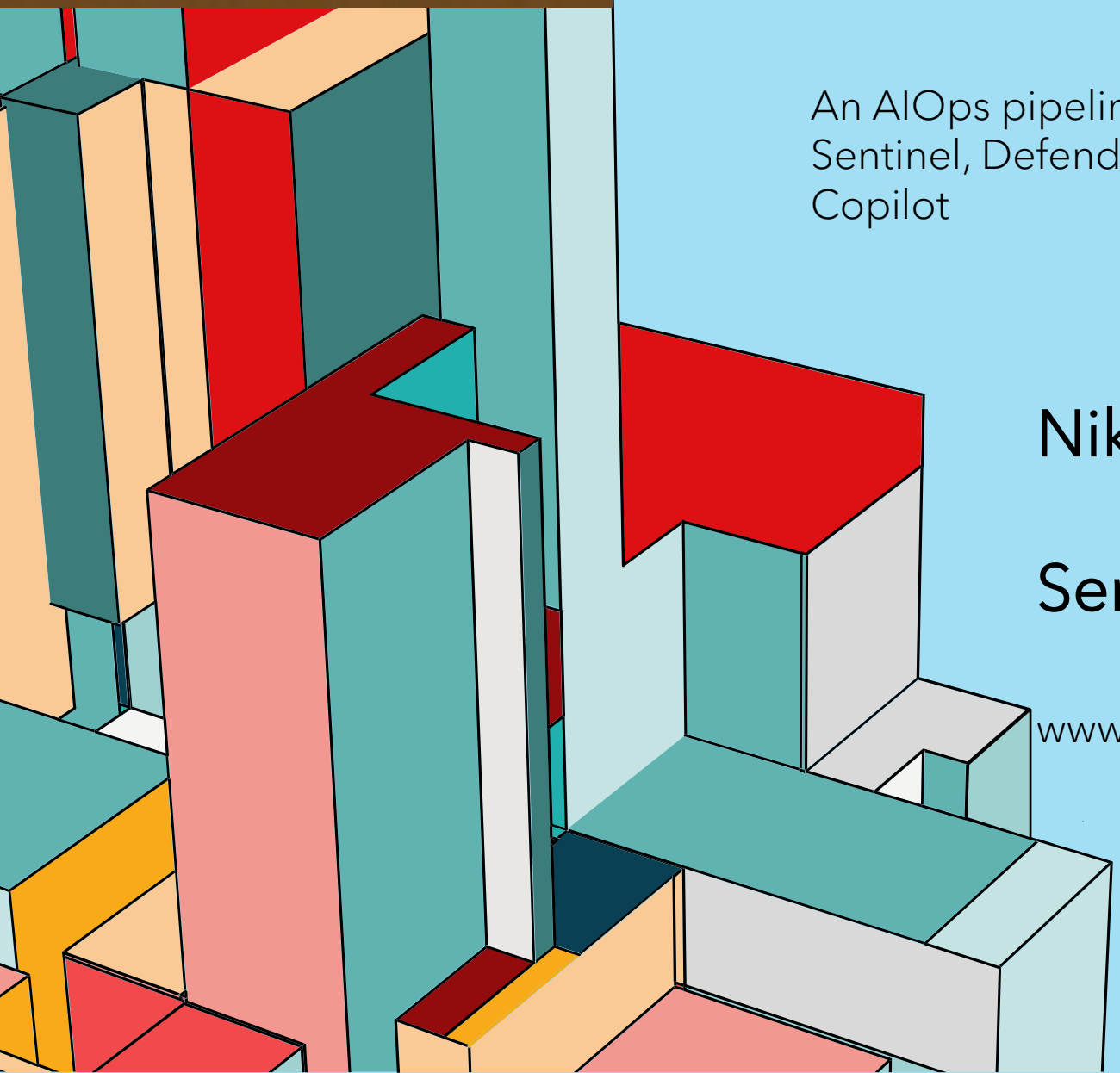
CONF42 DEVOPS 2026

JANUARY 22 • ONLINE

FROM ALERT STORMS TO MTTR

An AIOps pipeline for SecOps and SRE using Microsoft Sentinel, Defender XDR, Azure Monitor, and Security Copilot



Nikolay Milyaev

Senior Consultant

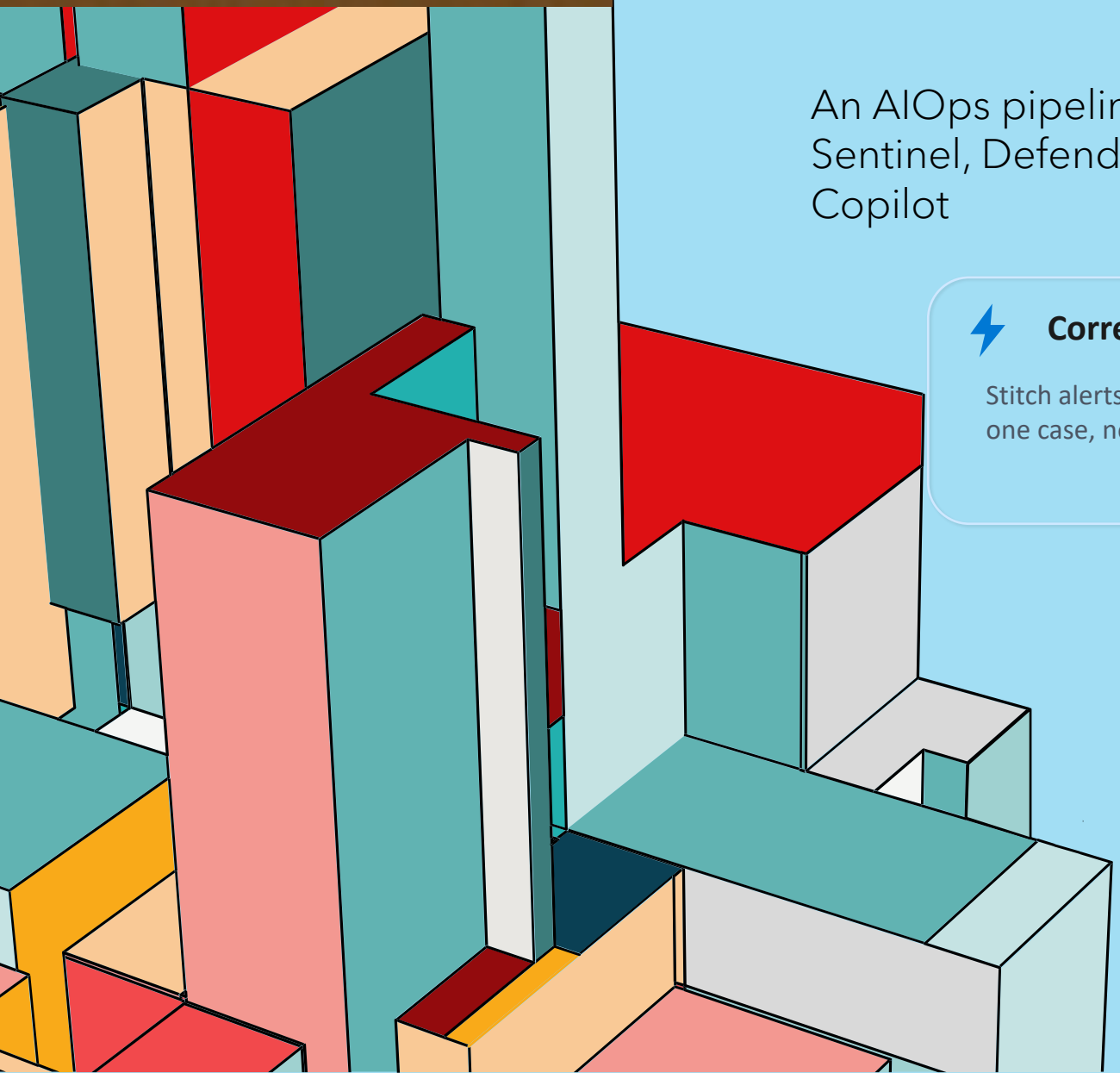
www.linkedin.com/in/n-milyaev

CONF42 DEVOPS 2026

JANUARY 22 • ONLINE

FROM ALERT STORMS TO MTTR

An AIOps pipeline for SecOps and SRE using Microsoft Sentinel, Defender XDR, Azure Monitor, and Security Copilot



Correlate

Stitch alerts into incidents so humans see one case, not fifty.

Automate

Safe first-mile playbooks: enrich, dedupe, route, and notify.

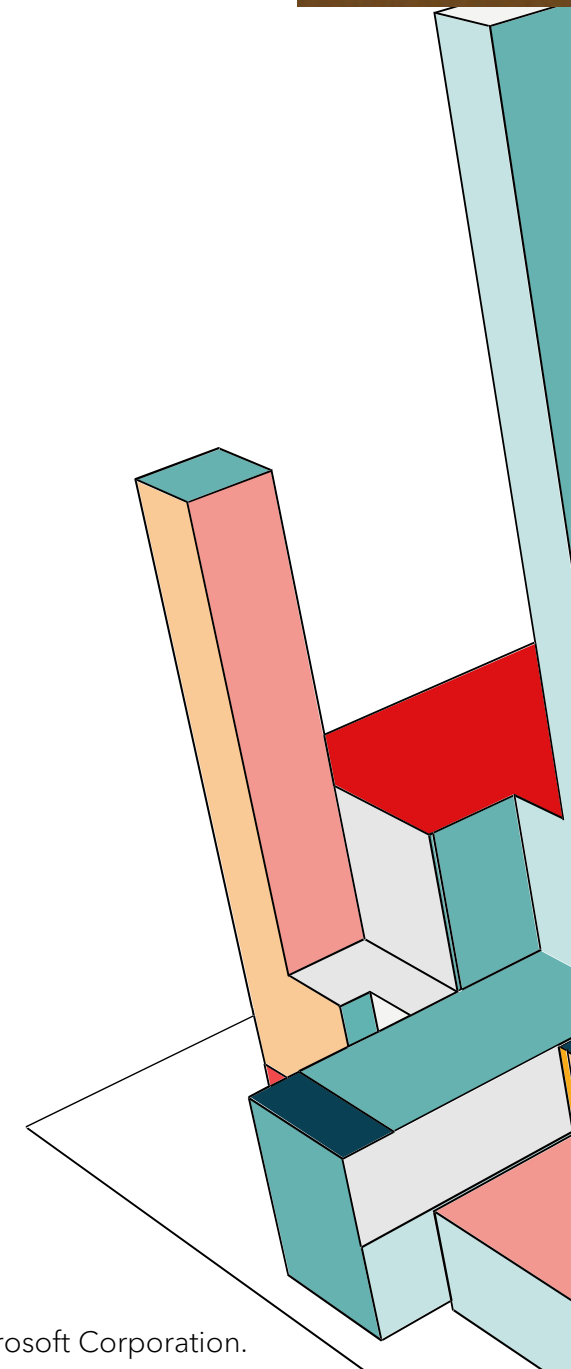
Assist

Security Copilot summarizes, answers, and suggests next steps.

The presentation/slides/information I share today represent my own personal views. I am speaking for myself and not on behalf of my employer, Microsoft Corporation.

AGENDA

- Why alert storms drive MTTR up (and morale down)
- Pipeline overview: correlate, automate, assist, measure
- Correlation options: Sentinel, Defender XDR, Azure Monitor
- First-mile automation: enrichment, deduplication, routing
- Security Copilot: summaries, guided response, natural language to queries
- Scorecard: how to prove MTTR reduction to leadership
- End-to-end example and implementation roadmap



ALERT STORMS ARE A MTTR MULTIPLIER

NOISE, FATIGUE, AND SLOW RESOLUTION

What that does

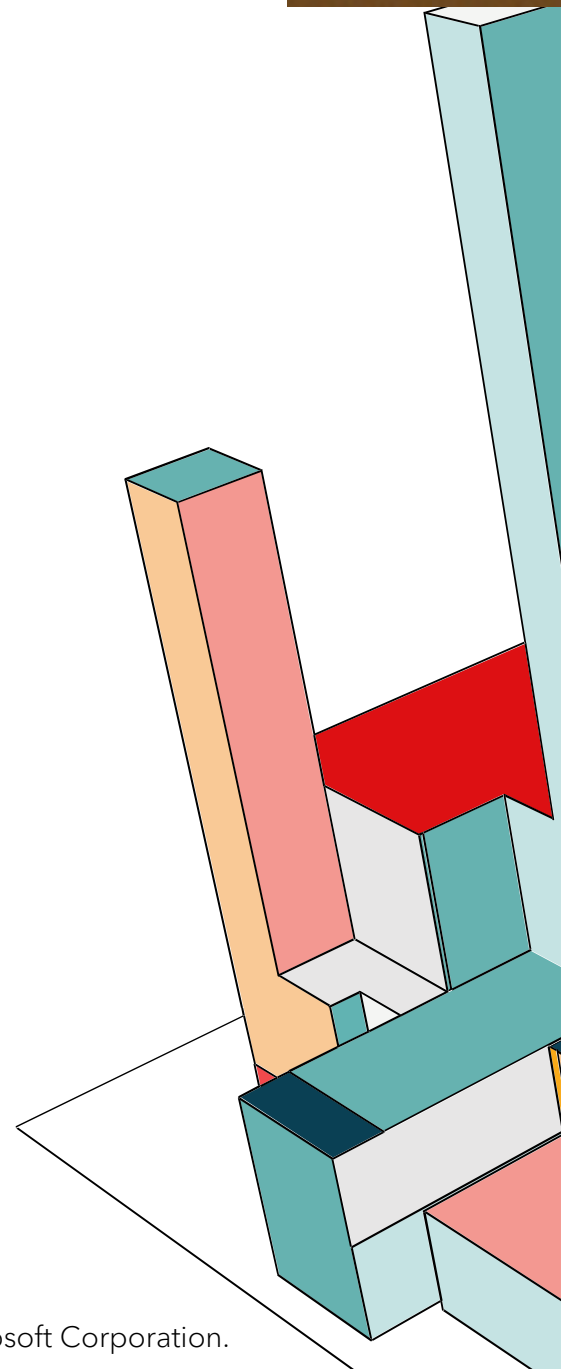
- Alert fatigue: humans stop trusting alerts
- Slow triage: time spent deduping and hunting for context
- Missed correlation: multistage attacks and cascading outages hide in plain sight
- MTTR rises because analysis and coordination are the bottlenecks

Goal for today: collapse the "time to understand" so responders spend minutes, not hours, before they act.

Typical SOC day

3,832
alerts per day (average)

62%
go unattended in some environments



THE AIOPS PIPELINE (HIGH LEVEL)

A REPEATABLE FLOW FROM NOISE TO RESOLUTION

1) Correlate

Convert raw alerts into one incident with shared entities and timeline.

2) Automate

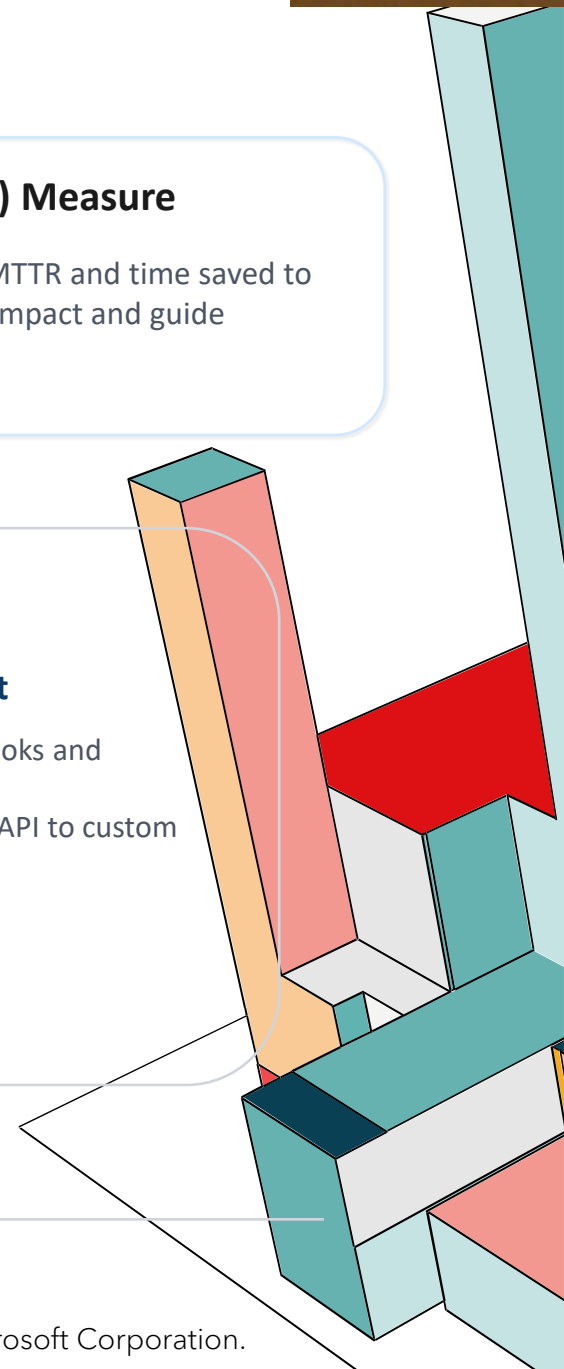
Run safe first-mile tasks: enrich, dedupe, assign, notify, ticket.

3) Assist

Use Copilot to summarize, answer questions, and suggest next steps.

4) Measure

Track MTTR and time saved to prove impact and guide tuning.



Microsoft-native building blocks

Correlation

Sentinel Fusion and incident grouping
Defender XDR correlation and merging
Azure Monitor smart groups

Automation

Sentinel automation rules
Logic Apps playbooks
Action Groups and ITSM connectors

AI assist

Security Copilot in Defender and Sentinel
Promptbooks and Logic App connector

Measurement

Sentinel workbooks and incident metrics
Export via REST API to custom tables

CORRELATION: ALERTS TO INCIDENTS

REDUCE VOLUME, RAISE FIDELITY

What changes when you correlate

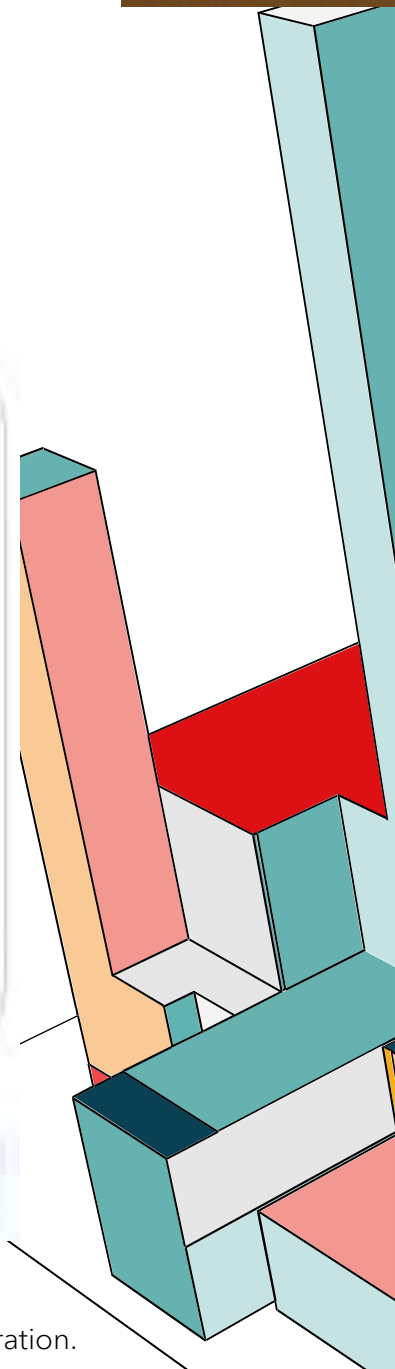
Before

- Dozens of individual alerts
- Multiple consoles and handoffs
- Duplicate investigations
- Low confidence and high noise

After

- One incident with all related alerts
- Shared entities and timeline
- Higher confidence, better prioritization
- Ready for automation and AI summaries

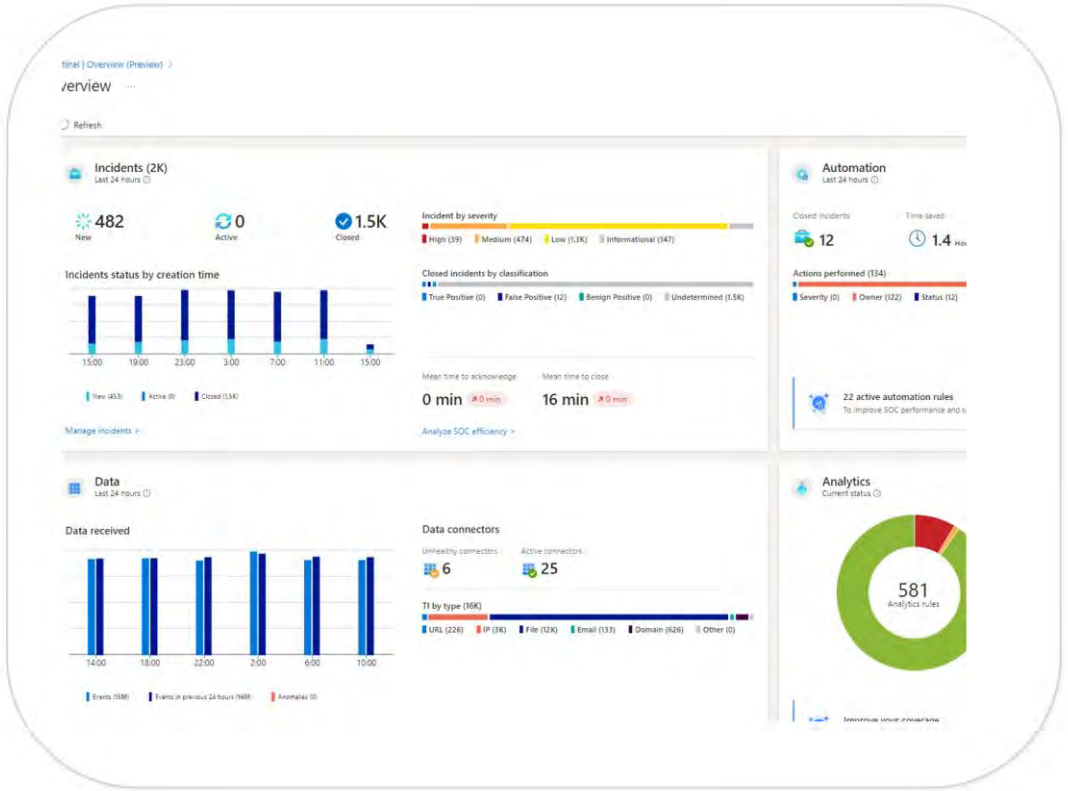
Where correlation happens: Sentinel Fusion and incident grouping | Defender XDR incident correlation and merging | Azure Monitor smart groups



MICROSOFT SENTINEL CORRELATION
FUSION PLUS RULE-LEVEL INCIDENT GROUPING

Key mechanisms

- Fusion: machine-learning correlation for multistage attacks
- Analytics rule grouping: control how alerts roll up into incidents
- Entity-centric view: users, hosts, IPs, cloud apps, and more
- SOAR-ready incidents: automation rules trigger playbooks instantly



Practical tuning tip: start with grouping to prevent floods (for example failed logons), then iterate on Fusion coverage and custom detection logic.

DEFENDER XDR CORRELATION AND UNIFIED SECOPS

INCIDENT MERGING ACROSS ENDPOINT, IDENTITY, EMAIL, AND APPS

What Defender XDR adds

- Incident-level correlation across Microsoft 365 signals
- Automatically adds related alerts to an existing incident
- Merges incidents when patterns show a broader campaign
- Unified queue when Sentinel is onboarded to the Defender portal

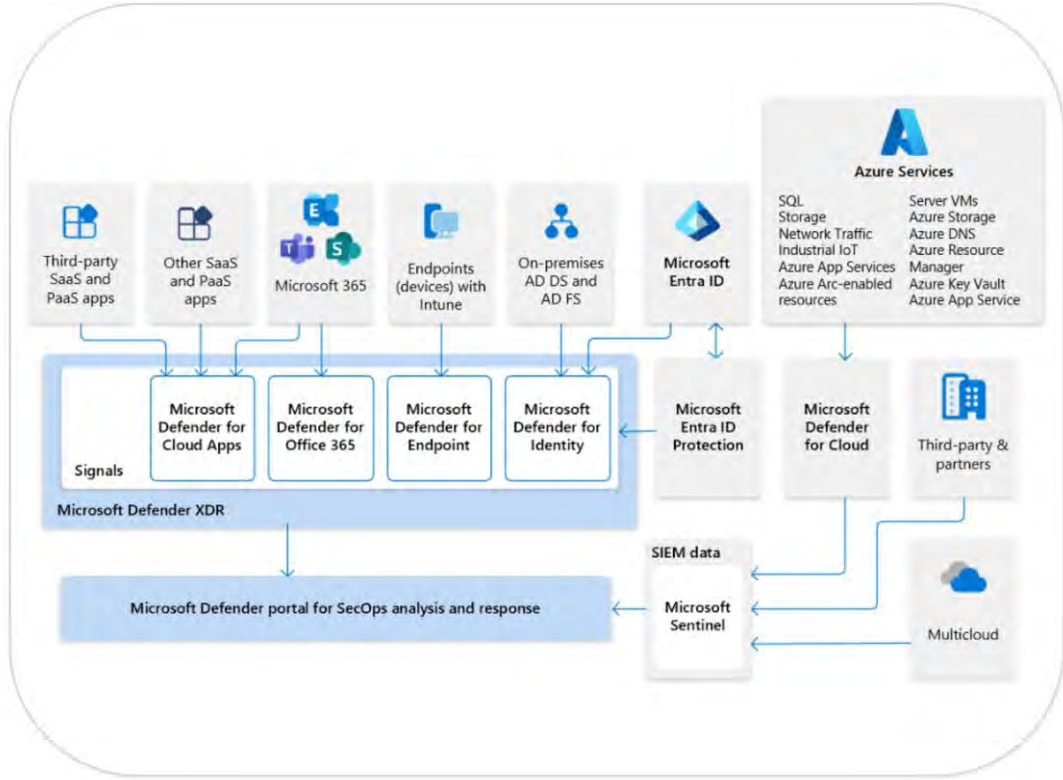
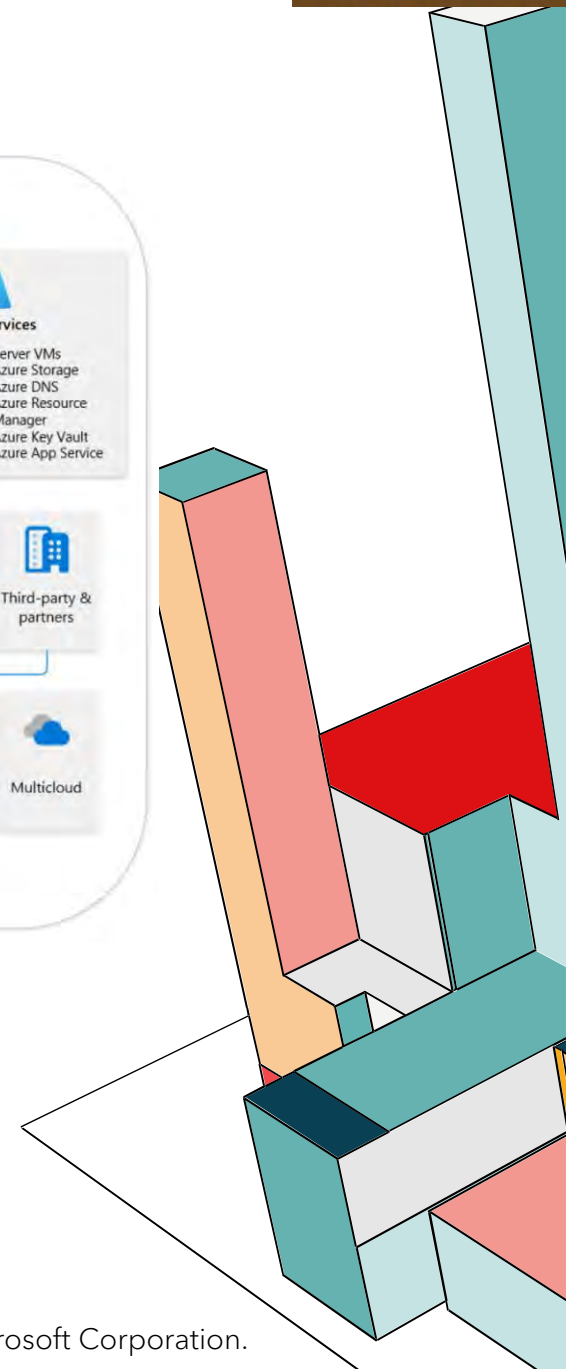


Illustration: XDR and integrated SIEM experience

Outcome: fewer incidents, each with a clearer narrative and cross-domain evidence. That is how you stop handoffs between tools from becoming handoffs between humans.



AZURE MONITOR FOR SRE: GROUP THE NOISE

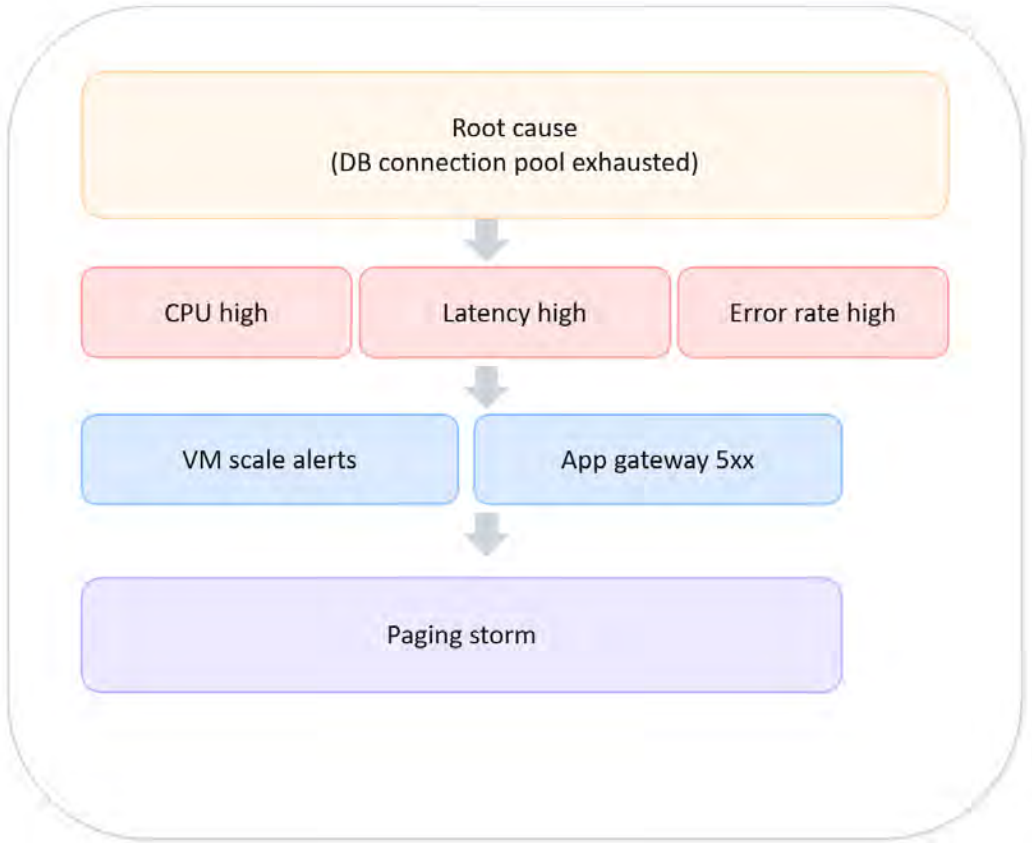
SMART GROUPS AND AIOPS FEATURES

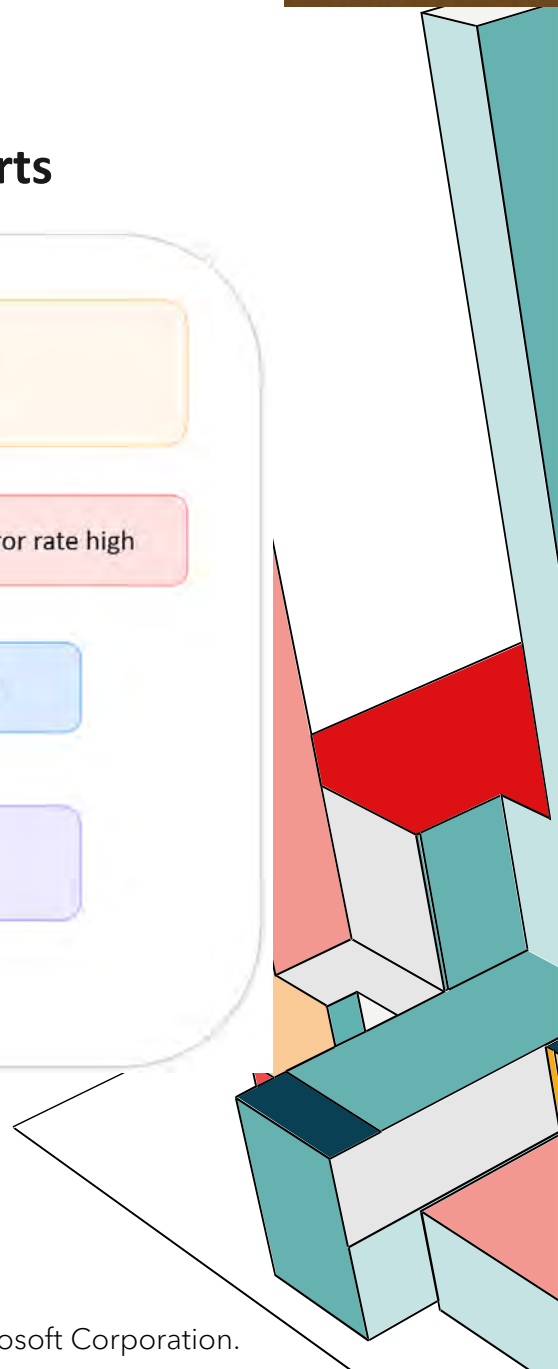
Azure Monitor AIOps features

- Smart Groups cluster related alerts into one group
- Anomaly detection and dynamic thresholds reduce false paging
- Correlate metrics, logs, and traces to speed investigation
- Same AIOps idea: make incidents actionable, not noisy

SecOps and SRE can share the same playbook pattern: group signals, enrich context, then act with guardrails.

Same problem, different alerts





FIRST-MILE AUTOMATION (SAFE BY DESIGN)

ENRICHMENT, DEDUPLICATION, ROUTING

Automate what is routine, keep humans for judgment

Enrich

- Threat intel for IPs, URLs, hashes
- User and device context (Entra, Intune)
- Historical context: seen before, known benign?

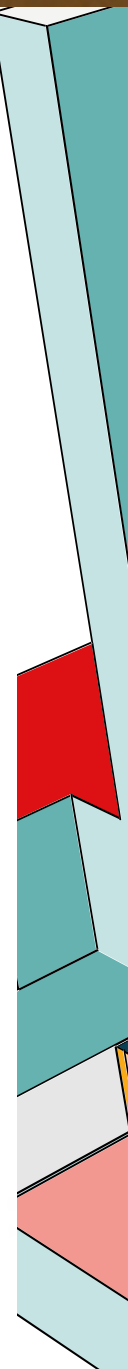
Dedupe

- Suppress obvious repeats
- Group by entity and time window
- Auto-close true duplicates with traceability

Route

- Assign owner and severity
- Notify Teams or paging
- Create ITSM ticket and attach context

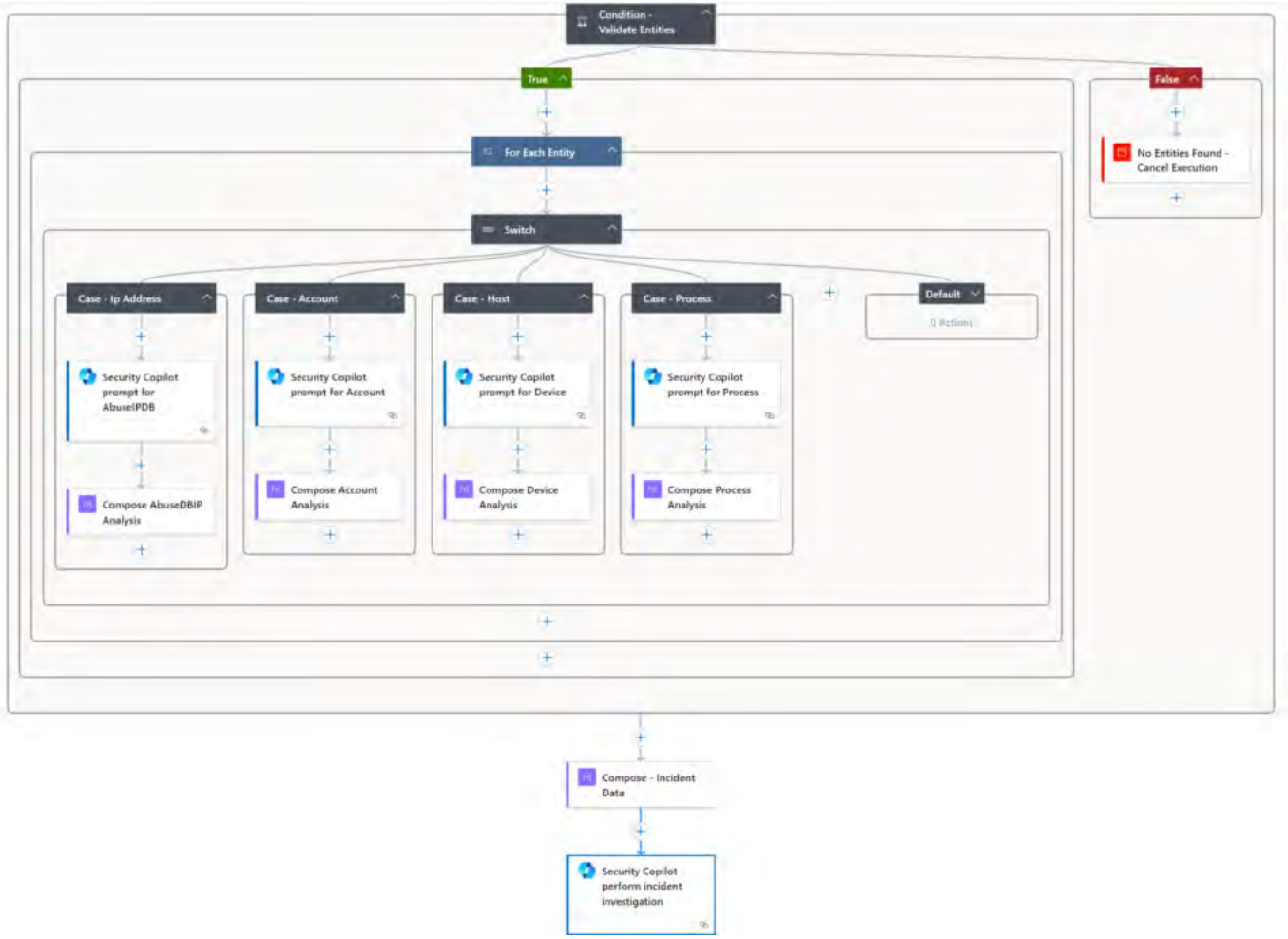
Guardrails: prefer read-only enrichment first, log every action, and make any containment step reversible or require approval.



AUTOMATION + AI IN PRACTICE

A PLAYBOOK THAT CALLS SECURITY COPILOT

Pattern: trigger on new incident, enrich entities, ask Copilot, post summary back



What to implement

- Trigger: incident created (Sentinel automation rule)
- Loop over entities: IP, account, host, process
- Collect signals: TI lookup, Intune or Entra context
- Call Security Copilot prompt or promptbook
- Write back: incident comment with summary and next steps

Why it works: by the time a human opens the incident, the case already contains context, prioritization cues, and an AI generated investigation summary.

SECURITY COPILOT: ANALYSIS AT MACHINE SPEED

Example prompts

Summarize for leadership

Provide an executive summary of this incident and the remediation steps taken.

Hunting question

Did this file hash appear on any other devices in the last 30 days?

Next steps

List the top 5 containment actions to take next, with rationale and checks.

How it fits the pipeline

- Turns incident data into readable narrative
- Converts natural language into KQL and hunting steps
- Generates draft reports and handoff notes
- Provides guided response suggestions in Defender
- Human stays in control: advice, not autonomous action

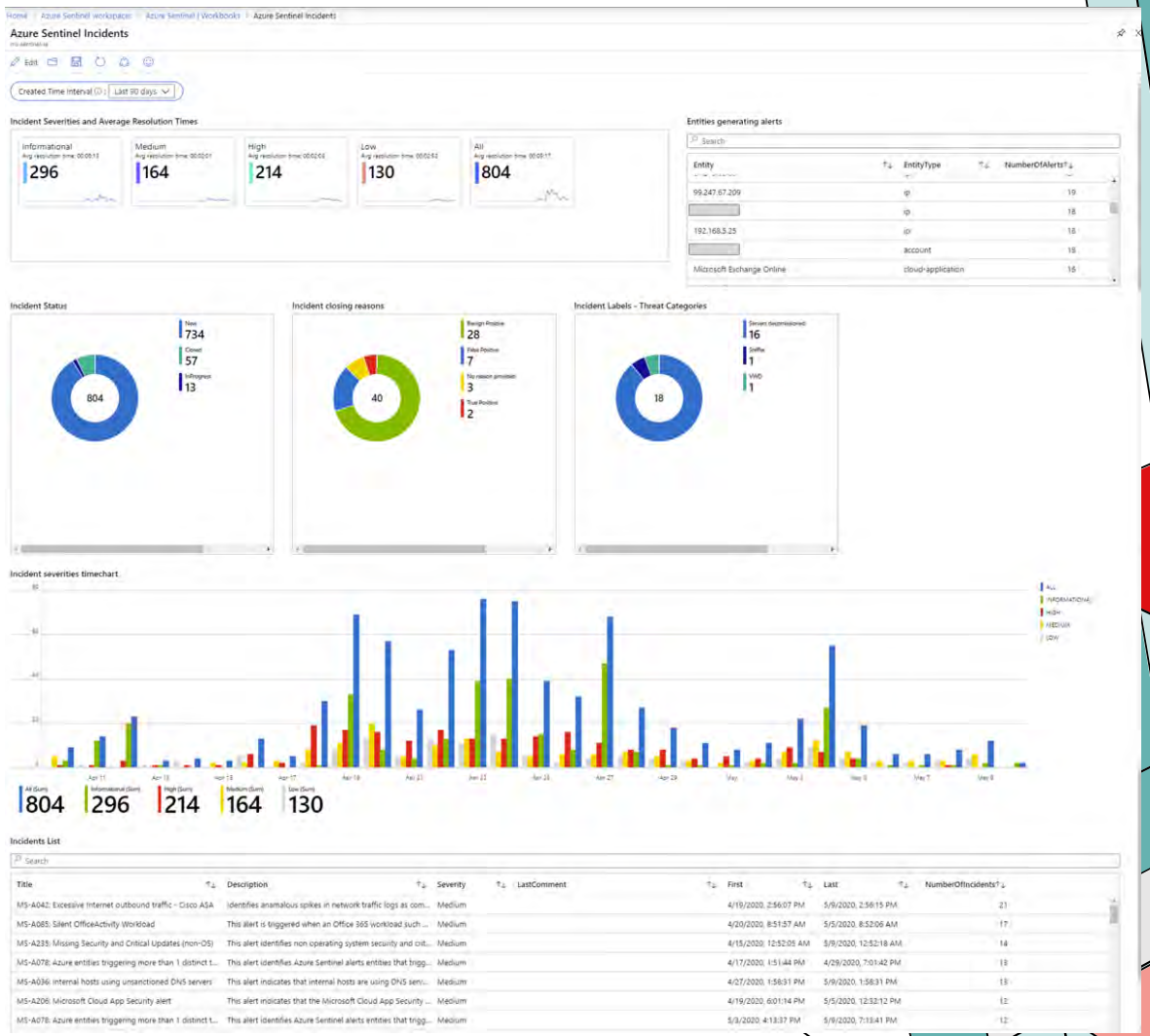
Best practice: attach Copilot outputs to the incident so the team captures knowledge, not just chat transcripts.

PROVE IT: MTTR AND THE EXECUTIVE SCORECARD

MEASURE, REPORT, AND TUNE

KPIs that actually move

- MTTR (time to close) by severity and category
- MTTA (time to acknowledge) and response SLA compliance
- Incidents closed by automation and estimated time saved
- False positive rate and closure reasons
- Incident volume trend after rule tuning and grouping

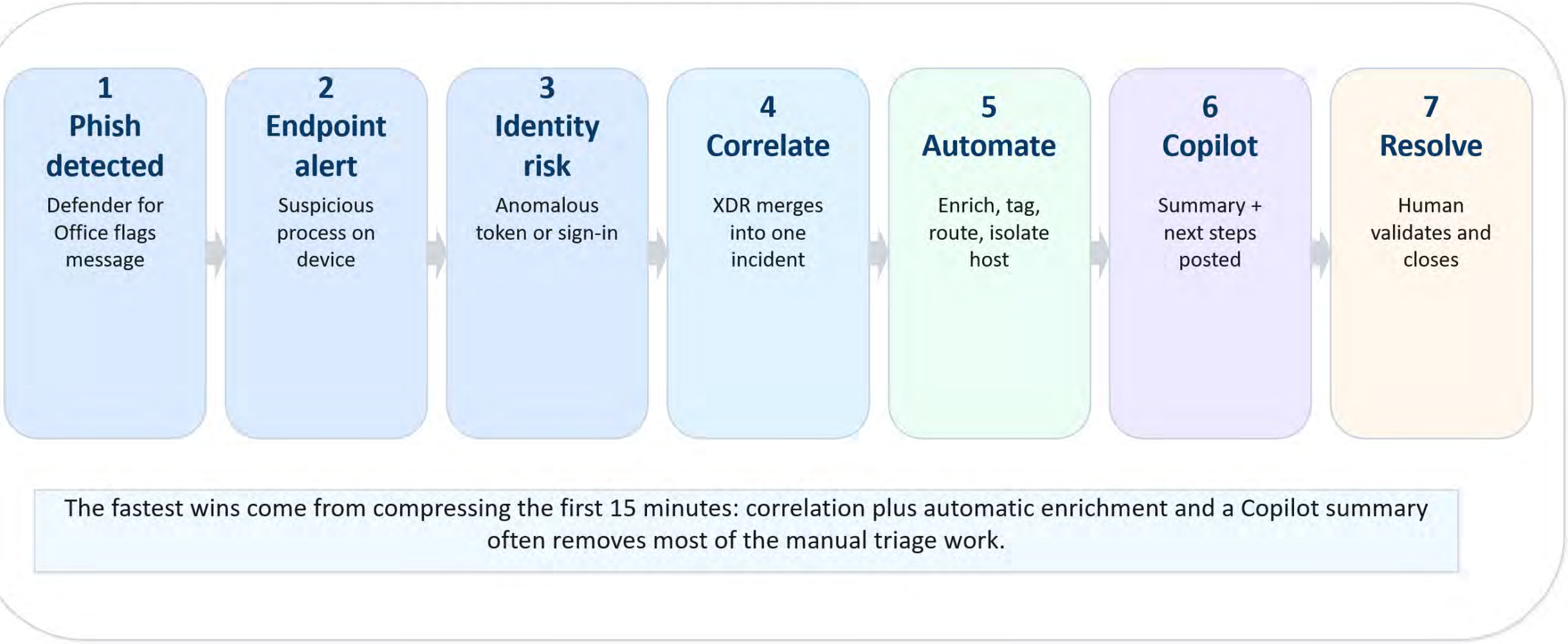


Measurement is not just reporting. It is a feedback loop: the scorecard tells you which incident types still have high MTTR and deserve new playbooks.

END-TO-END EXAMPLE: PHISH TO CONTAINMENT

CORRELATION + AUTOMATION + COPILOT

Scenario: phishing email triggers endpoint and identity signals



The fastest wins come from compressing the first 15 minutes: correlation plus automatic enrichment and a Copilot summary often removes most of the manual triage work.

IMPLEMENTATION ROADMAP AND GUARDRAILS

START SMALL, BUILD TRUST, THEN SCALE

A practical rollout in 4 phases

Phase 1

Baseline and hygiene

- Measure MTTA and MTTR
- Tune obvious noisy rules
- Turn on grouping where possible

Phase 2

Safe automation

- Enrichment playbooks first
- Auto routing and ITSM tickets
- Document rollback steps

Phase 3

Copilot acceleration

- Standard promptbooks
- Attach summaries to incidents
- Train analysts on validation

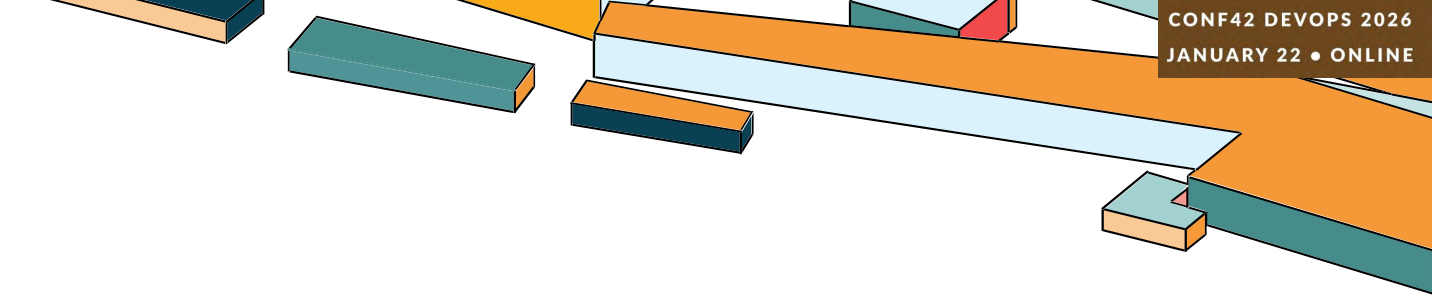
Phase 4

Optimization loop

- Scorecard reviews
- Automate frequent remediations
- Expand to SRE alerts and on call

Governance checklist: least privilege identities for playbooks, change control for automation, audit logs, and clear criteria for when automation can take containment actions.

KEY TAKEAWAYS: FROM STORMS TO FAST RESOLUTION



- Correlation is the first win: fewer cases, higher confidence
- First-mile automation buys time and reduces manual toil
- Security Copilot compresses analysis and reporting
- A scorecard turns improvements into measurable outcomes
- Start with safe steps, add power only after trust is earned

Next step: pick one noisy incident category and implement correlation + enrichment + a Copilot summary.

Measure MTTR before and after.

CONF42 DEVOPS 2026

JANUARY 22 • ONLINE

THANK YOU

Nikolay Milyaev

www.linkedin.com/in/n-milyaev