



TD SYNnex



Microsoft

Microsoft InnovAlte

Unlocking Security Excellence with Microsoft Sentinel: The Keystone for Robust Controls

Greg Wilson

Solutions Architect, Azure Cybersecurity Architect

| TD SYNEX

Legacy security tools aren't keeping up



Cyberthreats increased 10X* in the last year

Growing sophistication and velocity of threats, with ransomware encounters increasing by 2.75X



Siloed technology

With organizations using an average of 80 security tools, it's increasingly difficult to stay protected and focused on what matters



Trading off costs and coverage

SIEM non-native to the cloud are complex to maintain and scale, and even cloud offerings can have limited flexibility for data management



Nearly 2/3
of security
professionals
report burn out**

Application Security

The image displays two sections of cybersecurity company logos:

- WAF & Application Security:** This section includes logos for AIO, Akamai, Cloudflare, Contrast Security, DEAP, Fortinet, Imperva, NetScarker, Netsparker, Oracle, Palo Alto Networks, PerimeterX, PortShift, Rapid7, Riverbed, Safe-T, SecWorks, SH-PB, Signal Sciences, Snyk, StackPath, Sucuri, TemplarIT, ThreatIX, Trend Micro, Trustwave, Veracode, Virsec, Warlim, and Watchdog.
- Application Security Testing:** This section includes logos for Acunetix, Beyond Security, Checkmarx, Cisscan, Fasoo, Hackerone, IBM, Micro Focus, NexStark, NewSecure, OnePentest, Parasoft, Performer, PowerSploit, Qualys, Rapid7, Secure Code Labs, SiteLock, Sonarsource, Synack, Synopsys, Tenable, Trustwave, Veracode, Whitehat Security, and WhiteSource.

Mobile Security

Messaging Security

Security Consulting & Services

[illegible]



Microsoft Sentinel

Security operations need a modern solution



Catch emergent
threats earlier



Protect
everything



Scale security
coverage



**Microsoft
Sentinel**

What does Microsoft Sentinel do?



Collect

This is all users, devices, applications, and infrastructure, both on-premises and in multiple clouds



Detect

Minimize false positives using Microsoft's analytics and unparalleled threat intelligence



Investigate

Hunt for suspicious activities at scale, tapping into years of cyber security work at Microsoft



Respond

Use built-in orchestration and automation of common tasks

Collect

Microsoft Sentinel Data Connectors

Collect data at scale

Use data connectors to ingest your data in Microsoft Sentinel.



Data Connectors out of the box

Built-in connectors enable connection to the broader security ecosystem for Microsoft native, multi-cloud, and non-Microsoft products.



Data Normalization

Collect data from any source with real-time log streaming



Custom Connectors

Create your own connector for whatever source you need

Detect

Rule Types

Microsoft Sentinel provides threat detection rules that run regularly, querying the collected data and analyzing it to discover threats.



Scheduled Rules

Rules set to run on a scheduled basis written by Microsoft security experts.



Threat Intelligence

Automatically matches Common Event Format (CEF) logs, Syslog data or Windows DNS events with domain, IP and URL threat indicators from Microsoft Threat Intelligence..



Near-real-time (NRT)

Designed to run once every minute, in order to supply you with information as up-to-the-minute as possible.



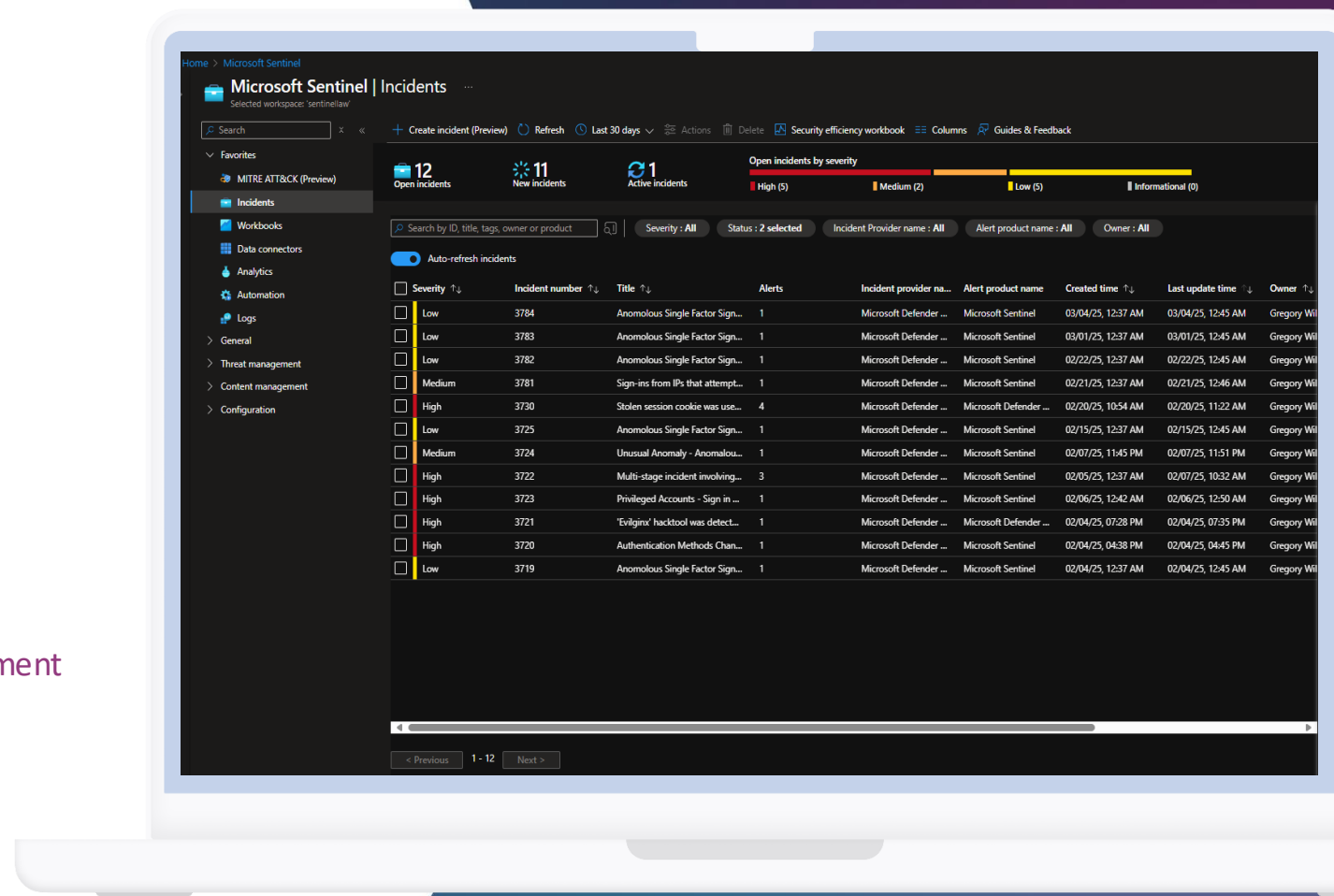
Anomaly Rules

When the rule observes behaviors that exceed the boundaries set in the baseline, it flags those occurrences as anomalous.

Investigate







Investigate Threats

Case management platform for incident investigation and management

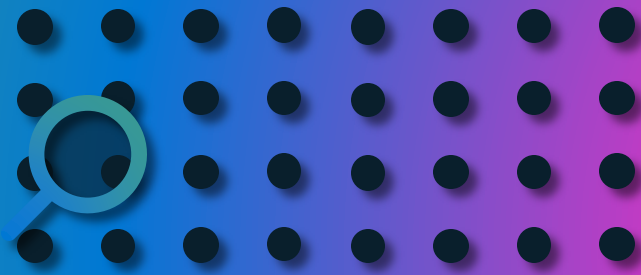


Investigate Efficiently

Similar incidents ⓘ

High	304459	Multi-stage incident involving Initial access & Lateral mov...	1/6/2023, 06:22 PM	Closed - Benig...	 Similar entities ⓘ	ajourn@seccxp...
High	309061	Preview: Possible multistage attack activities detected by ...	1/6/2023, 06:13 PM	Closed - Benig...	 Similar entities ⓘ	Unassigned
High	312677	Possible attempt to steal credentials	1/6/2023, 06:10 PM	Closed - Benig...	 Similar entities ⓘ	Unassigned
High	312676	Suspicious access to LSASS service	1/6/2023, 06:10 PM	Closed - Benig...	 Similar entities ⓘ	Unassigned
High	312662	Suspicious access to LSASS service	1/6/2023, 06:10 PM	Closed - Benig...	 Similar entities ⓘ	Unassigned
High	323924	Possible attempt to steal credentials	1/3/2023, 02:49 PM	Closed - Benig...	 Similar entities ⓘ	Unassigned

Detect threats at scale with Microsoft Threat Intelligence



Microsoft Threat Research

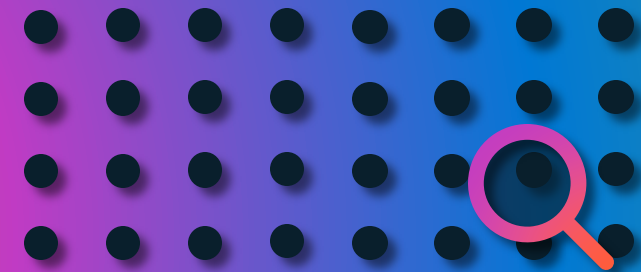
- 10,000 experts across 77 countries
- Tracking over 300 threat actor groups including 160 nation state actors
- Working with more than 15K partners in the security ecosystem
- 78 trillion signals daily



Automatic matching



Alert created



Any log source

- Common event format
- Syslog
- Office activity logs
- Azure activity logs
- DNS logs (recently announced)
- Network sessions (recently announced)

Respond

Rapid Response with Microsoft Sentinel

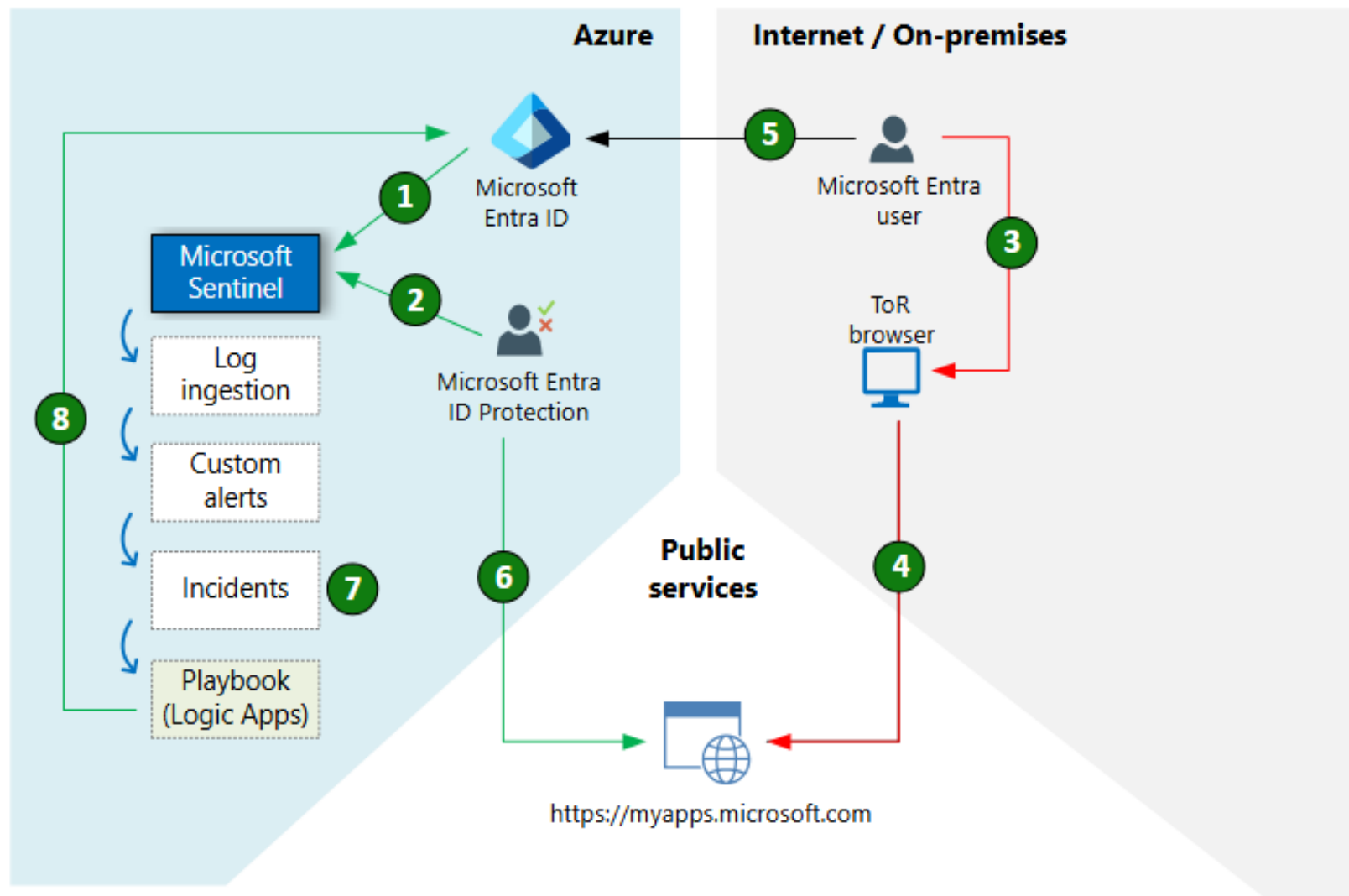
Automation rules

- Automated tag, assign, or close incident
- Assign advanced automations
- Automated responses for multiple analytic rules at once
- Create lists of tasks for triage, investigation, and remediation
- Create order of actions that are executed

Playbooks

- Heart of the SOAR
- Integrate with both internal and external systems
- Configure to run automatically
- Harness the power of Azure Logic Apps

Microsoft Sentinel automated response



What does this mean for my organization?

Microsoft Sentinel Partner Ecosystem Multiplier

A Study by Canalys

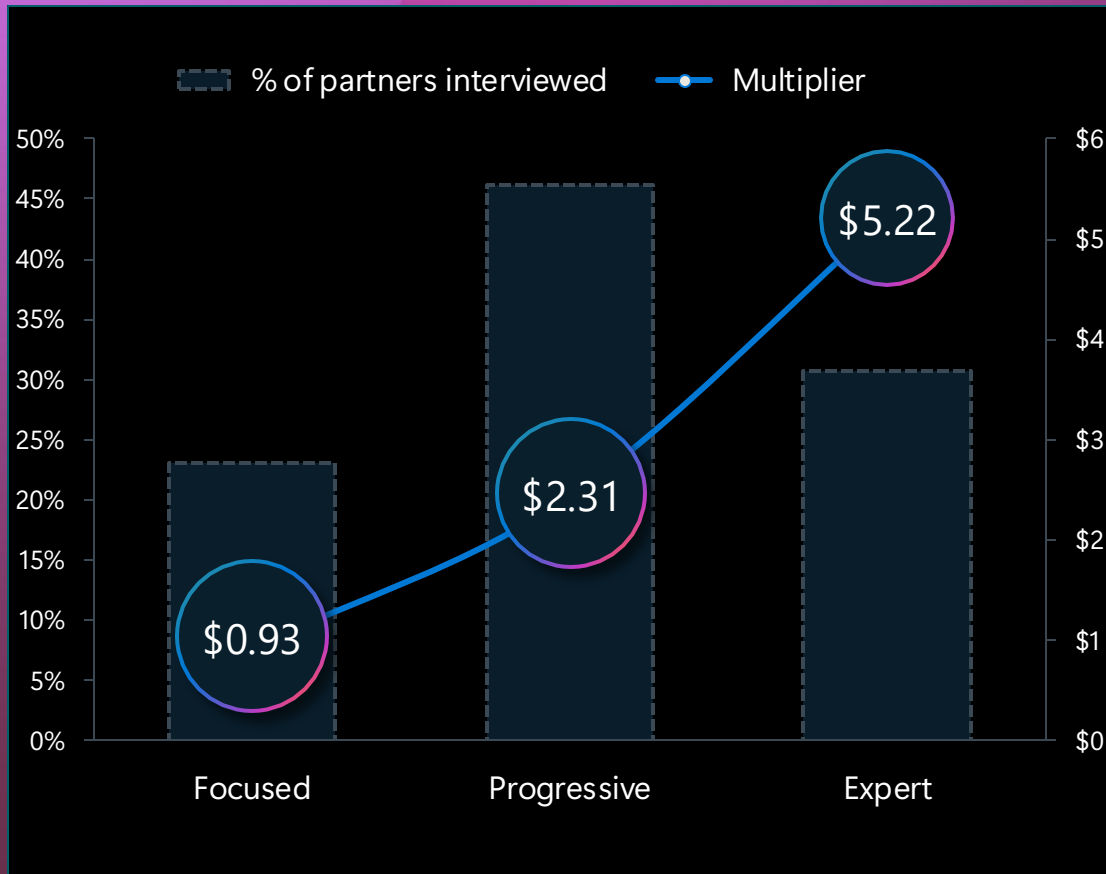
US\$5.22

US\$1.00

Microsoft Sentinel partners can achieve a \$5.22 multiplier

Sentinel partner ecosystem are capturing **\$5.22** for every dollar a customer consumes on Sentinel solutions

Services multiplier emerging in ecosystem



Focused

Focusing on simple Sentinel migrations with few or zero attached services



Progressive

Focus primarily on Sentinel migrations but attach a significant amount of managed services. However, they are immature in Advise and Adopt services.



Expert

Providing highly mature service offerings across the entire flywheel, except Build.

Demo

Q and A