Nvious solutions

Powered by SecurityHQ

Managed Azure Sentinel - Detection & Response

Empower your Azure Sentinel with SecurityHQ's 24/7 Security Operation Centre (SOC).

Azure Sentinel SIEM tool, together with SecurityHQ skills, analytics, and security orchestration, delivers the highest degree of threat detection and incident response.

From users, to apps and devices, to servers on any cloud, see and stop threats before the damage is done. Be it data theft, ransomware, fraud or information governance, all organisations have their own security risks. Managed Azure Sentinel is the industry-leading solution for businesses to protect against all forms of cyber threats and attacks.

SecurityHQ work as an addition to your team, by running Azure Sentinel as a service. Our security engineers are experts in advanced analytics and threat hunting, detection, and response. And operate out of Security Operation Centres (SOC's) located around the world, every minute of every day, to ensure maximum security.

- **24/7 Detection & Response.**
- **Collect data** at cloud scale.
- **Identify** previously undiscovered threats.
- **Use analytics** to minimize false positives.
- **Respond to incidents** rapidly with built-in orchestration and automation of common tasks.
- **Identify anomalous and malicious patterns** with automated recovery systems.
- **Speed up response** to threats and streamline security operations with integrated automation.
- **Up or down-scale automatically,** to meet your organisations specific needs.
- **Analyse and draw correlations** to deepen intelligence by importing Office 365 data for free.

Service Overview

How Does MDR Work? (Powered by Azure Sentinel)

01. Data Collection

- Cloud Native Integrations
  - Azure (MS 365/Defender/AAD Audit logs)
  - 3rd Party (AWS CloudTrail)
- Syslog (CEF)
- REST API
- Azure Agents (MMA/AMA)

02. Data Processing & Analytics

- Data Storage & Retention: Azure Monitor Log Analytics workspace
- Data Enrichment: Asset Criticality and Threat Intel
- Data Analytics: Analytic Rules and Workbooks

03. Advanced Analytics

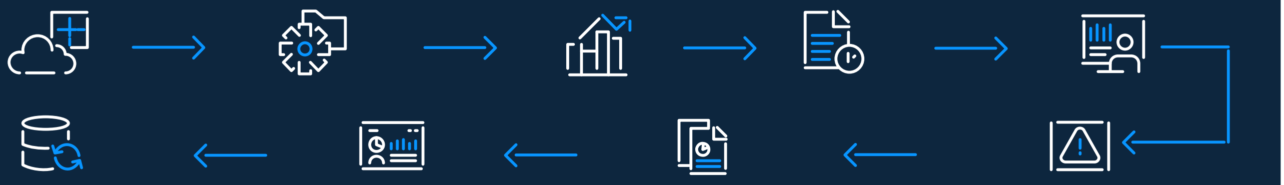
- User & Entity Behavioural Analytics (UEBA)
- Multi-staged attack detection (Fusion)

04. Proactive Threat Hunting

- Hunting Dashboard
- KQL Query Rules
- SecurityHQ Threat Advisories

05. SOC Threat Investigation & Response

- 24/7 Threat Detection & Response
- 280+ SOC Incident (Triage/Investigate/Respond)
- Eliminate False Positives



09. Long Term Data Retention (N-Year retention)

- Cloud option: Azure Data Explorer (ADX)
- On-prem: SecurityHQ London Datacentre

08. SecurityHQ IM Platform and Mobile App

- Efficient Incident Management Platform
- Orchestrate incident response, service request and SLA monitoring and
- Improve quality and context for incident response

07. Business Intelligence & Reporting

- Data driven documents created using BI tooling
- Rich analytical reports to identify risk and enhance posture

06. Threat Containment

- Mitigating risk with MS Security Stack (Defender, Antimalware, PIM)
- Leverage SystemX/Sentinel SOAR (LogicApps) to automate
  - Block Malicious IP
  - Suspend Rogue Users
  - Isolate Infected Machines

Service Features

User Risk Monitoring

Detect malicious activity and risky user behaviour that is derived from the log analysis of the Microsoft 365 suite (both E3 and E5), including Azure Active Directory analytics.

Azure Infrastructure as a Service Monitoring

Correlate suspicious host activity for server and application hosts in Azure IaaS.

Azure Platform as a Service Monitoring

Receive a visual map of the relationship between threats, hosts and key assets to ensure an overall context of threats.

Powerful SOC Technology

24/7 Transparent & auditable collaboration, Incident Management & Analytics, Dashboarding, SLA Management and Customer ITSM integration API.

Access to Global SOC & Labs

Enriched threat intelligence with an all-encompassing world view. Expert analysis, with Industry best certifications OSCP, GPEN, GWAPT, CEH and more.

On-Premise Hosts

Ingest and correlate events from traditional on-premise server hosts, firewalls and applications.

Powered by Orchestration & Automation

SecurityHQ SOAR capability will help you minimize the duration and impact of a cyber-attack by automating manual tasks and, instead, focus on high-value investigations.

Threat Intelligence Enrichment

SecurityHQ Intelligence eco system enriches event data to detect malicious connections to rogue IP's, domains and URL's.

High Scalability & Flexibility

Bespoke services tailored to the needs of our clients and partners. We supplement your team and maintain systems, to keep things simple for you.

Precise, Action-oriented & Flexible Reporting

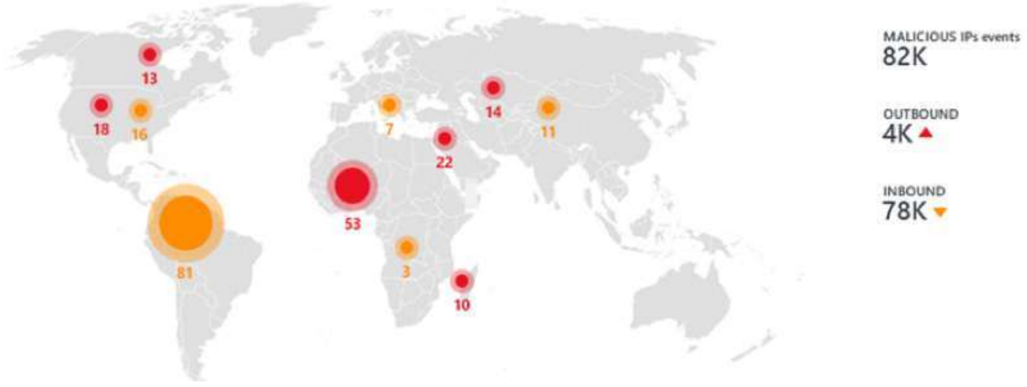
Risk based and patch prioritised time, with weekly and monthly reports. Embed a continuous governance model to ensure improvement and up/down-scale effortlessly.

Non-Azure PaaS and SaaS Monitorings

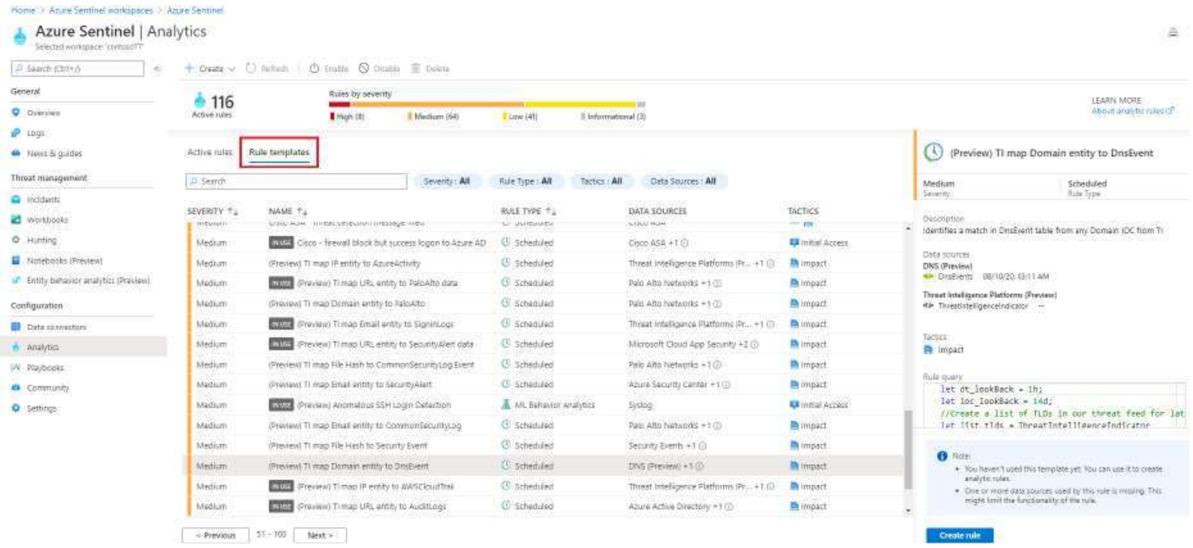
Ingest events and correlate data across Azure and Non-Azure platforms, such as

- URL Content Gateway (e.g., ZScaler, Forcepoint, Cisco Umbrella).
- Web App Firewalls (e.g., Cloudflare, Imperva Incapsula, Akamai Kona).
- Endpoint Security Systems (SentinelOne, Crowdstrike, Carbon Black and more).

Identify Potential Malicious Traffic Geolocation



Create New Detection to Investigate Specific Threats



SEVERITY	NAME	RULE TYPE	DATA SOURCES	TACTICS
Medium	IN USE Cisco - firewall block but success logon to Azure AD	Scheduled	Cisco ASA +1	Initial Access
Medium	(Preview) TI map IP entity to AzureActivity	Scheduled	Threat Intelligence Platforms (Pr... +1	Impact
Medium	IN USE (Preview) TI map URL entity to PaloAlto data	Scheduled	Palo Alto Networks +1	Impact
Medium	(Preview) TI map Domain entity to PaloAlto	Scheduled	Palo Alto Networks +1	Impact
Medium	IN USE (Preview) TI map Email entity to SigninLogs	Scheduled	Threat Intelligence Platforms (Pr... +1	Impact
Medium	IN USE (Preview) TI map URL entity to SecurityAlert data	Scheduled	Microsoft Cloud App Security +2	Impact
Medium	(Preview) TI map File Hash to CommonSecurityLog Event	Scheduled	Palo Alto Networks +1	Impact
Medium	(Preview) TI map Email entity to SecurityAlert	Scheduled	Azure Security Center +1	Impact
Medium	IN USE (Preview) Anomalous SSH Login Detection	ML Behavior Analytics	Syslog	Initial Access
Medium	(Preview) TI map Email entity to CommonSecurityLog	Scheduled	Palo Alto Networks +1	Impact
Medium	(Preview) TI map File Hash to Security Event	Scheduled	Security Events +1	Impact
Medium	(Preview) TI map Domain entity to DnsEvent	Scheduled	DNS (Preview) +1	Impact
Medium	IN USE (Preview) TI map IP entity to AWSCloudTrail	Scheduled	Threat Intelligence Platforms (Pr... +1	Impact
Medium	IN USE (Preview) TI map URL entity to AuditLogs	Scheduled	Azure Active Directory +1	Impact

(Preview) TI map Domain entity to DnsEvent

Medium
Severity

Scheduled
Rule Type

Description
Identifies a match in DnsEvent table from any Domain IOC from TI

Data sources
DNS (Preview)
DnsEvents 08/10/20, 03:11 AM
Threat Intelligence Platforms (Preview)
ThreatIntelligenceIndicator --

Tactics
Impact

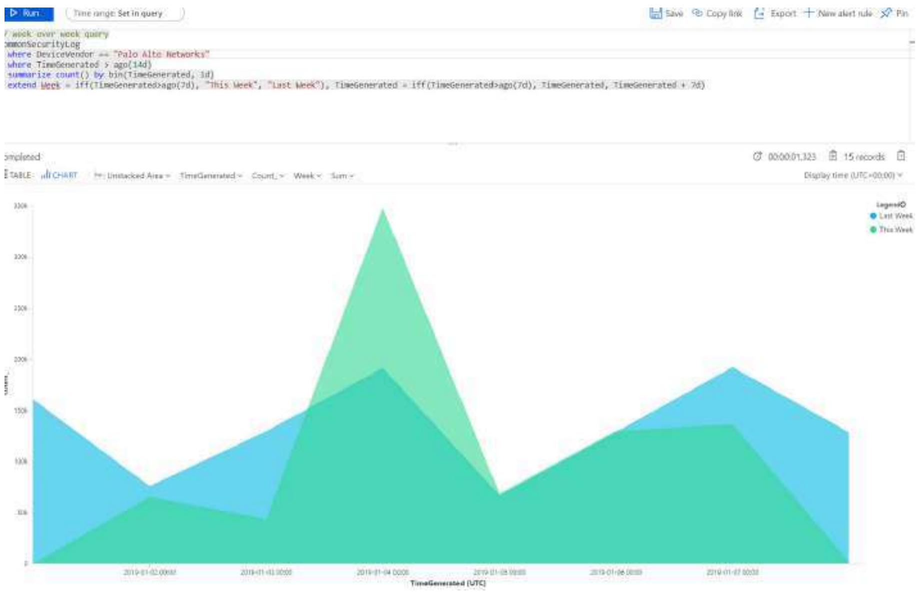
Rule query

```
let dt_lookBack = 1h;
let ioc_lookBack = 14d;
//Create a list of TLDs in our threat feed for lat
let list_tlds = ThreatIntelligenceIndicator
```

Note:
- You haven't used this template yet. You can use it to create analytic rules.
- One or more data sources used by this rule is missing. This might limit the functionality of the rule.

Create rule

Use Built-in Workbooks



```
// week over week query
CommonSecurityLog
| where DeviceVendor == "Palo Alto Networks"
| where TimeGenerated > ago(14d)
| summarize count() by bin(TimeGenerated, 1d)
| extend Week = iff(TimeGenerated>ago(7d), "This Week", "Last Week"), TimeGenerated = iff(TimeGenerated>ago(7d), TimeGenerated, TimeGenerated + 7d)
```

Completed 00:00:01.323 15 records

Common Customer Challenges and How We Solve Them

Challenges

Our Solutions

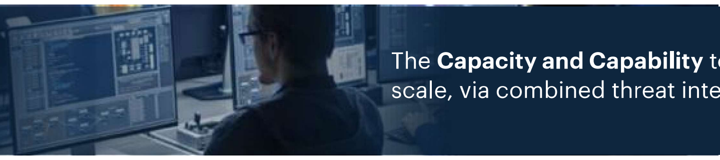
A lack of **Visibility** and awareness.

By visualising risky behaviour and misconfigurations, target the threat at its source, for **Complete Visibility & Peace of Mind.**

Cost and **Risk Reduction.**

Likelihood of a breach is reduced & **24/7 Detect & Response** delivered at a fraction of the cost of DIY.

Peace of mind... **Assurance.**



The **Capacity and Capability** to deliver bespoke services at scale, via combined threat intelligence and human expertise.

A need for **Rapid Response.**

Incident Response playbooks, SOAR platform, and Certified Incident Handlers to contain threats and watch your back!

A **Partner** to depend on.

A partnership that works as an **Extension of Your Team**, to expose patterns of illicit behaviour and reduce risks.

How Does SecurityHQ Differ?

SecurityHQ is a Global MSSP, that detects, and responds to threats, instantly. As your security partner, we alert and act on threats for you. Gain access to an army of analysts that work with you, as an extension of your team, 24/7, 365 days a year. Receive tailored advice and full visibility to ensure peace of mind, with our Global Security Operation Centres, and utilize our award-winning security solutions, knowledge, people, and process capabilities, to accelerate business and reduce risk and overall security costs.

New York SOC
London SOC
Dubai SOC
Pune SOC
Johannesburg SOC
Brisbane SOC

About Nvious Solutions

We are a South African ICT integrator we help create smarter businesses for customers locally and increasingly into the African continent. Our technical expertise combined with operational proficiency, allow us to design solutions that help our clients become more efficient and agile. Our solutions are secure by design ensuring network applications and enterprise security.

We are aligned with best practice service management frameworks, which ensures that you receive optimal value, access to specialised skills, as well as sound management practice. We maintain a constant focus on improving service quality, increasing user satisfaction and delivering increased business value.

Nvious Solutions is 100% Black owned and managed business with a Level 1 BBBEE rating.

Have a question? We would love to hear from you.

☎ **phone**	+27 (0) 11-327 6344
✉ **email**	info@invious.co.za
website	www.nvious.co.za