BYTES | Smarter together

Powered by SecurityHQ

MICROSOFT SENTINEL

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

Microsoft Sentinel SIEM tool, together with Bytes and 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. Microsoft Sentinel is the industry-leading solution for businesses to protect against all forms of cyber threats and attacks.

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

Benefits

- **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

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

- 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
- 260+ SOC Incident (Triage/Investigation/ Response)
- Eliminate False Positives

06. Threat Containment

- Mitigating Risk with MS Security Stack (Defender, Anti-malware, PIM)
- Leverage SystemX/Sentinel SOAR (LogicApps) to Automate
  - Block Malicious IP
  - Suspend Rogue Users
  - Isolate Infected Machines

07. Business Intelligence & Reporting

- Data-Driven Documents Created Using BI Tooling
- Rich Analytical Reports to Identify Risk and Enhance Posture

08. SecurityHQ Platform and Mobile App

- Efficient Incident Management Platform to Orchestrate Incident Response, Service Request and SLA Monitoring to Improve Quality and Context for Incident Response

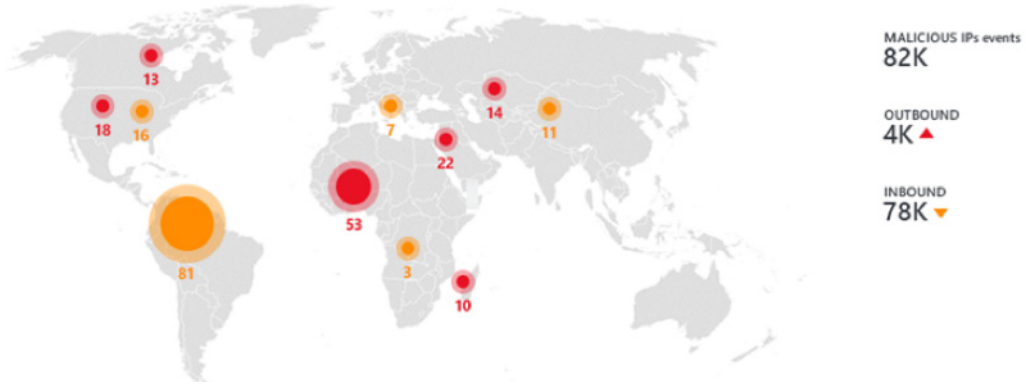
09. Long Term Data Retention

- Cloud Option: Azure Data Explorer (ADX)
- On-Prem: SecurityHQ London Datacentre

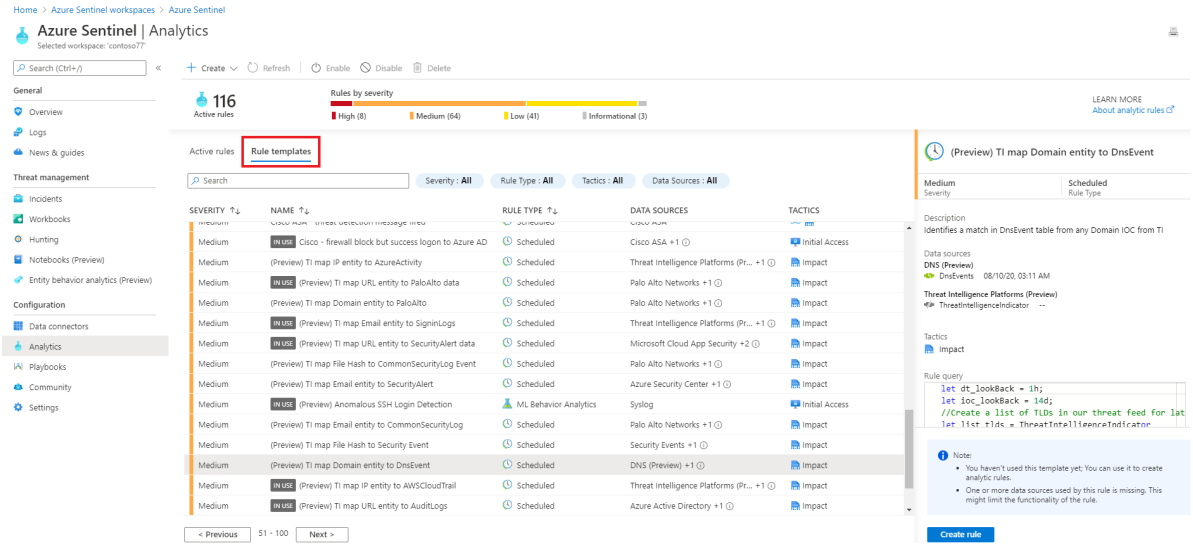
Contact us at
tellmemore@bytes.co.uk

For more details visit
bytes.co.uk/security

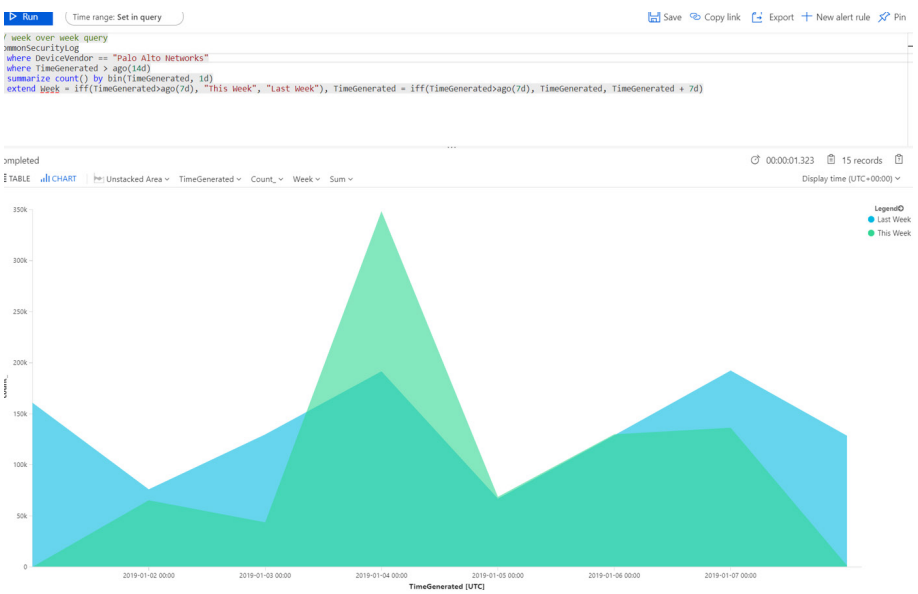
Identify Potential Malicious Traffic Geolocation



Create New Detection to Investigate Specific Threats



Use Built-in Workbooks



BYTES | Smarter together

Powered by SecurityHQ

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.

Powered by Orchestration & Automation

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

Azure Infrastructure as a Service Monitoring

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

Threat Intelligence Enrichment

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

Azure Platform as a Service Monitoring

Monitor malicious activity from Azure PaaS systems such as IIS, SQL, Defender ATP and Azure WAF platforms.

High Scalability & Flexibility

Bespoke services tailored to the needs of our clients and partners.

Zero Complexity & Low Maintenance

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.

Access to Global SOC & Labs

Enriched threat intelligence with an all-encompassing world view.

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).

On-Premise Hosts

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

Contact us at
tellmemore@bytes.co.uk

For more details visit
bytes.co.uk/security

Expert Analysts

Achieve immediate transparency of all your systems and processes.

Knowledge Transfer

Get the complete picture of detection techniques used to detect vulnerabilities, associated risk, and recommendations for remediations.

Powerful SOC Technology

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

Continuous Governance Model

Embed a continuous governance model to ensure improvement and up/down-scale effortlessly.

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

Reach us

tellmemore@bytes.co.uk | 01372 418 500

bytes.co.uk/security

Follow us