SecurityHQ | DATRIX

Managed Endpoint Detection and Response (EDR)

Advanced threats & attacker techniques will evade traditional anti-virus. Our Managed EDR service leverages the world's best EDR tooling, together with 24/7 SOC analytics, to detect otherwise concealed malicious behaviour.

Key Features

Complete Visibility

Monitor all potential threats and behaviours. Understand how a threat appeared, what created it, if it made a connection, if the registry setting was modified, what effects this had, and more.

Real Time Response

Carbon Black Response, powered by our 24/7 SOC team allows us to stop attacks in progress by isolating infected systems, terminating processes and banning hashes across an enterprise.

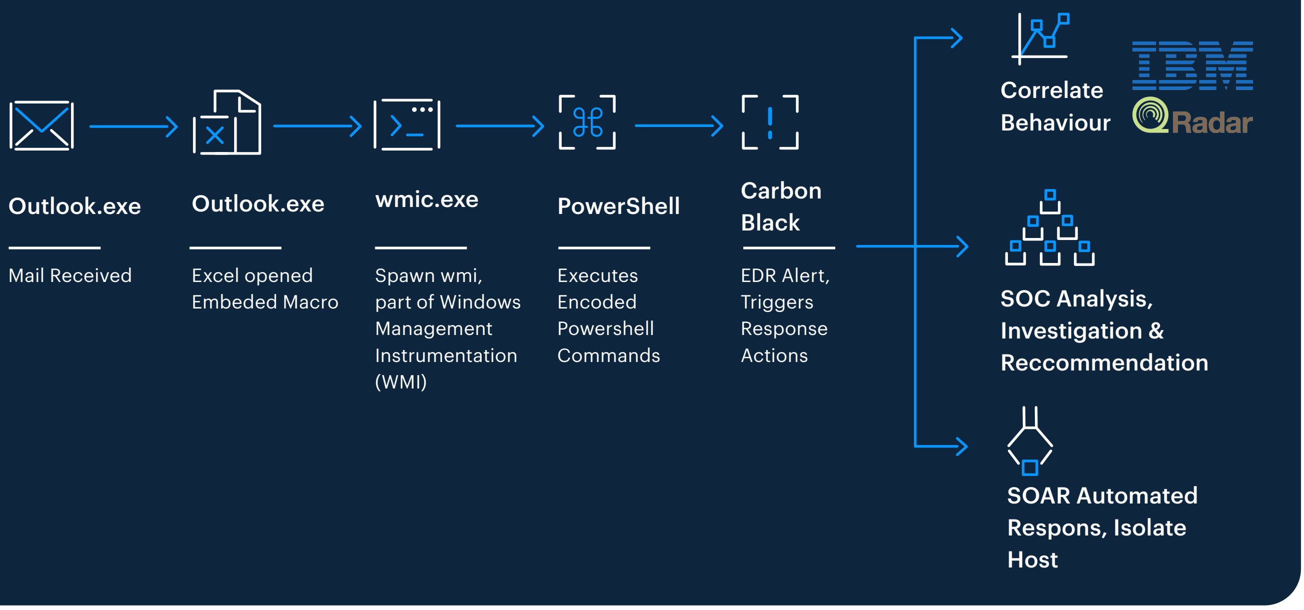
Proactive Threat Hunting

Our team will proactively locate the most advanced threats that make it past your defences. We use both Carbon Black Response, together with our Machine Learning algorithms, powered by IBM QRadar, to identify anomalous endpoint behaviour.

Benefits

- **24/7 SOC Monitoring**
- Powered by **Carbon Black Response**
- **Detect advanced threats** with thorough forensics and rapid root cause analysis.
- **Complete endpoint visibility and continuous monitoring** for transparency of all systems and processes.
- **Fully managed service** to reduce the cost of IR, with more effective remediation.
- **Decrease dwell time** from the start, without fine-tuning.
- **Identify the full scope of an attack** with advanced correlation and proactive threat hunting.
- **Real-time identification,** without signatures, to monitor and prioritise potential threats.

Sample Threat Detection & Response Flow: Spearphishing



Outlook.exe

Mail Received

Outlook.exe

Excel opened Embeded Macro

wmic.exe

Spawn wmi, part of Windows Management Instrumentation (WMI)

PowerShell

Executes Encoded Powershell Commands

Carbon Black

EDR Alert, Triggers Response Actions

Correlate Behaviour

SOC Analysis, Investigation & Reccommendation

SOAR Automated Respons, Isolate Host

Contact us at
enquiries@datrix.co.uk

For more details visit
www.datrix.co.uk

Service Features

24/7 SOC Analytics

Our 6 Security Operations Centres provide continuous monitoring, analysis and forensic Investigations. When something goes wrong, our team takes proactive actions to block, isolate and investigate threats.

Best Technology

Carbon Black EDR represents the best-in-class technology, that allows us to detect more threats than any other EDR solution on the market.

Continuous Visibility

Carbon Black EDR sensors collects and visualises comprehensive information about endpoint events, including:

- Activity record of every endpoint, even offline.
- Every binary, process, file, net connection, and registry modification.
- Attack chain visualisations to identify what is happening at every stage of an attack.

Rapid Incident Response

An attacker can compromise your environment in an hour or less. Carbon Black EDR gives our SOC team the power to respond and remediate rapidly, containing threats and repairing damage quickly.

- Isolate infected systems and remove malicious files to prevent lateral movement.
- Secure shell access to any endpoint with Live Response.
- Automatically collect and store detailed forensic data for post-incident investigation.

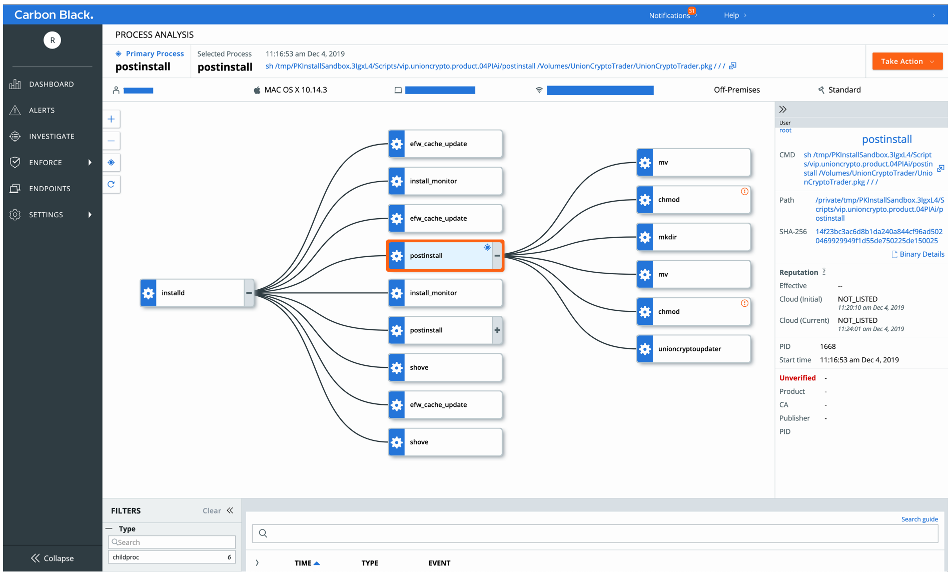
Advanced Threat Hunting

Advanced attacker methods will evade traditional Anti-Virus. We detect anomalous behavior, powered by threat intel, automated watchlists to detect advanced threats correlated to Mitre ATT&CK, attack methods.

Machine Learning

Performing threat hunting at scale requires machine analytics to ingest millions of Carbon Black sensor data to identify new behavior, patterns of anomalous activity, and an increase in suspicious use baselines. We ingest terabytes of data into our IBM QRadar analytics system, to perform machine learning and anomaly detection on Carbon Black sensor activity.

Carbon Black UI



PROCESS ANALYSIS

Primary Process: postinstall

Selected Process: postinstall

11:16:53 am Dec 4, 2019

sh /tmp/PKInstallSandbox.3lgxL4/Scripts/vip.unioncrypto.product.04PIAi/postinstall /Volumes/UnionCryptoTrader/UnionCryptoTrader.pkg / / /

MAC OS X 10.14.3 | Off-Premises | Standard

User: root

postinstall

CMD: sh /tmp/PKInstallSandbox.3lgxL4/Scripts/vip.unioncrypto.product.04PIAi/postinstall /Volumes/UnionCryptoTrader/UnionCryptoTrader.pkg / / /

Path: /private/tmp/PKInstallSandbox.3lgxL4/Scripts/vip.unioncrypto.product.04PIAi/postinstall

SHA-256: 14f23bc3ac6d8b1da240a844cf96ad5020469929949f1d55de750225de150025

Binary Details

Reputation

Effective: --

Cloud (Initial): NOT_LISTED *11:20:10 am Dec 4, 2019*

Cloud (Current): NOT_LISTED *11:24:01 am Dec 4, 2019*

PID: 1668

Start time: 11:16:53 am Dec 4, 2019

Unverified: -

Product: -

CA: -

Publisher: -

PID

FILTERS Clear

Type

Search

childproc 6

How Does the Service Work?

Endpoint Light Weight Sensor

Binaries

File & Registry

Net cons

Processes

01. Sensor Collection

Cb Response sensor captures net cons, binaries, file & Regmods & ties activity to specific processes.

Carbon Back Server (On-prem or Cloud)

MITRE ATT&CK

02. Index & Store

Cb Response pushes the events to the Carbon Black Server for indexing & storage.

03. Correlate

Cb correlates the behaviour against a library of suspicious threat actions.

04. Attack Mapping

Attacker behaviour is tagged to Mitre ATT&CK techniques & tactics.

IBM Resilient SOAR

Machine Isolation

Hash Banning

07. Containment

Using IBM Resilient & Carbon Black, the SOC team isolates infected hosts or bans known bad actors.

IBM QRadar Security Analytics (Cloud)

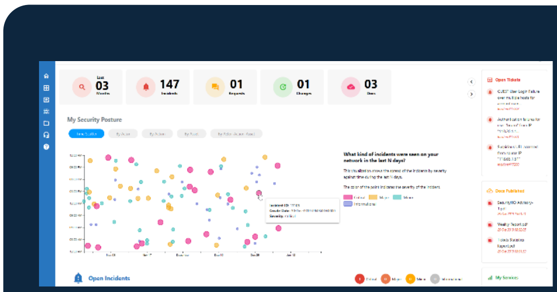
06. Analysts

qualify, investigate and act on offenses to provide a response, 24/7.

05. Machine Learning

& Correlation is used to prioritise alerts into notifiable offenses.

Incident Management & Analytics Platform



08. Reporting & Dashboards

Visualising incident metrics, SLA, workflows.

09. Incident Response Workflows

Orchestrating IR workflows to detect, investigate, contain and resolve incidents.

Customer ITSM Integration

servicenow

Jira Software

10. Customer ITSM Integration

Integrate the workflow with any API integration from SecurityHQ to your ServiceNow or Jira.

How Does SecurityHQ Differ?

Founded over 15 years ago, SecurityHQ prides itself on its global reputation as an advanced MSSP, delivering superior engineering-led solutions to over 150 clients, around the world. We think in terms of business. Specifically, how what we do is going to impact you. We learn about what our clients do, speak their language, understand what systems/processes they have, and provide tailored solutions and improvements, backed by a team of professionals, to ensure complete resiliency against cyber threats.

Our mission is to provide world-class security operations to our clients and partners, to integrate processes seamlessly, and act as an extension of our user's own teams. The result is a bespoke service that seeks to address the users specific risks and challenges, that empowers their cyber safety.

Bespoke

Every customer is different. Your risks, industries, geolocations, regulatory requirements and processes demand a bespoke response. SecurityHQ customises your services, based on your requirements.

Business Intelligence

SecurityHQ relates all incidents to CIA impact against your systems, data and users.

Integrity & Transparency

SecurityHQ builds relationships on trust, built on a foundation of complete transparency in our operational delivery.

Incredible People

Our analysts are some of the most experienced and qualified in the industry.

Incident Management Platform

Collaboration is critical for effective security operations. SecurityHQ's Incident Management Platform is an arena for incident workflows, SLA management, data visualisation and documentary repository.

World's Best Technology

We only use Gartner Magic Quadrant technology, such as IBM QRadar, Resilient, X-Force.

Global Reach

SecurityHQ operates 6 Security Operation Centres globally and has unrivalled regional expertise with international oversight.

Personalised Service

Clients receive dedicated Service Managers and Senior Analysts who are available 24/7, every day of the year.

About Datrix

Established over 25 years ago, digital transformation is the driving force behind the evolution of Datrix services and solutions. Our professional and technical services teams adopt a consultative, client-centric approach that sees us design, build and manage superior solutions. Our critical networking, communications and cyber security solutions are the preferred choice for the nation's key institutions, as well as public and private sector organisations seeking to address the business challenges of compliance, performance, availability and affordability.

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

Reach us

enquiries@datrix.co.uk | +44 (0)20 7749 0800

Follow us