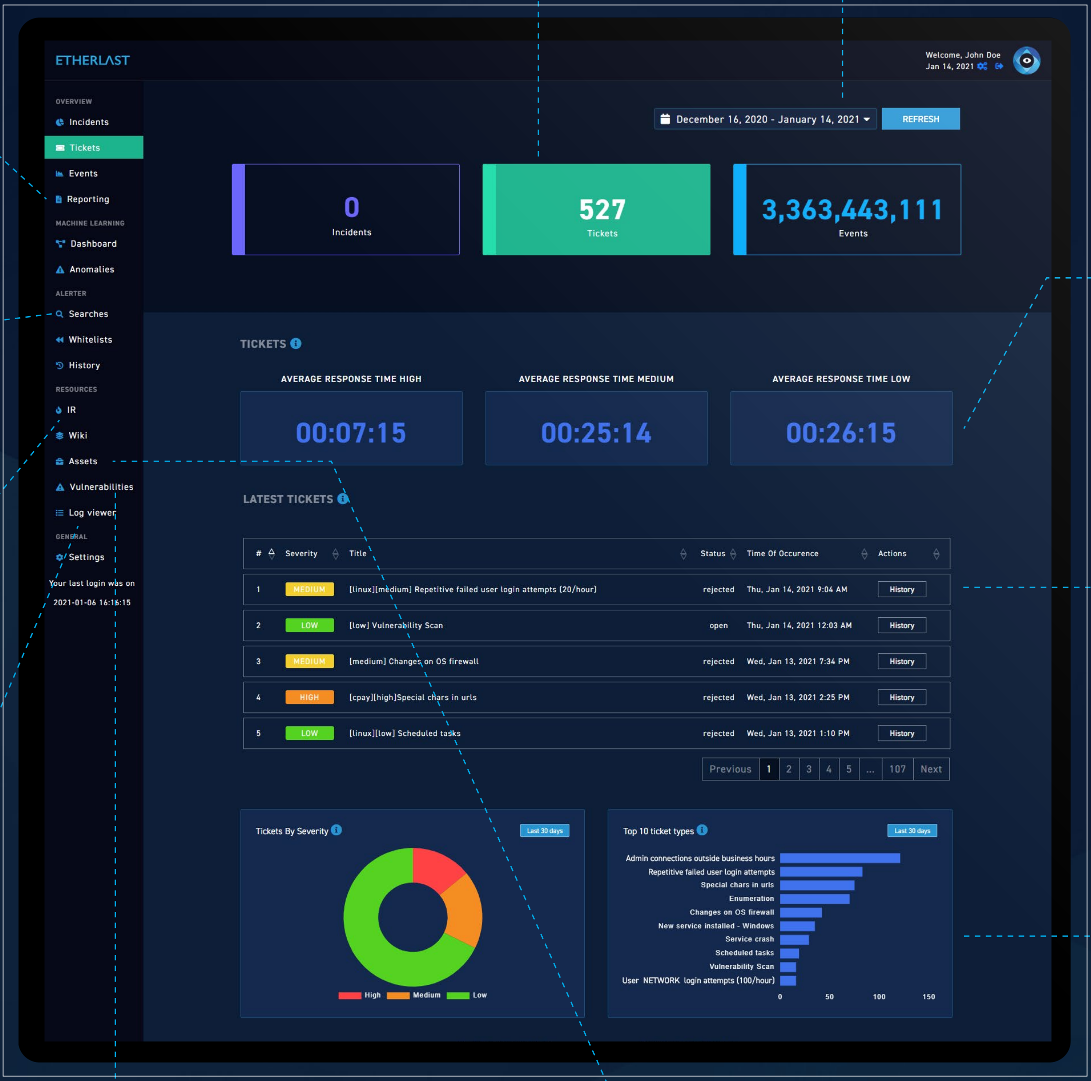
INTRODUCING

ETHERLAST

BY CYBOURN

The versatile Extended Detection & Response (XDR) Platform that allows you to promptly detect complex threats, analyze them and respond from a single pane of glass.

Integrate your essential data and information security indicators to **empower your data driven decision making and response capabilities** with EtherLast.



Your last login was on 2021-01-06 16:16:15

0	527	3,363,443,111
Incidents	Tickets	Events

TICKETS

AVERAGE RESPONSE TIME HIGH	AVERAGE RESPONSE TIME MEDIUM	AVERAGE RESPONSE TIME LOW
00:07:15	00:25:14	00:26:15

LATEST TICKETS

#	Severity	Title	Status	Time Of Occurence	Actions
1	MEDIUM	[linux][medium] Repetitive failed user login attempts (20/hour)	rejected	Thu, Jan 14, 2021 9:04 AM	History
2	LOW	[low] Vulnerability Scan	open	Thu, Jan 14, 2021 12:03 AM	History
3	MEDIUM	[medium] Changes on OS firewall	rejected	Wed, Jan 13, 2021 7:34 PM	History
4	HIGH	[cpay][high]Special chars in urls	rejected	Wed, Jan 13, 2021 2:25 PM	History
5	LOW	[linux][low] Scheduled tasks	rejected	Wed, Jan 13, 2021 1:10 PM	History

1 Quick metrics overview

2 Easily select time ranges

3 Monitor SLA compliance

4 Monitor ticket evolution

5 Fully customizable metrics

6 Manage your network's vulnerabilities

7 View all integrated assets

8 View raw logs

9 Quickly respond to incidents

10 Manage correlation rules

11 Create custom reports

KEY FEATURES OF ETHERLAST

Vulnerability Management

Quick navigation — Browse through the status of vulnerabilities and track patching status

Vendor agnostic — EtherLast integrates ZAP and Open VAS Scanners that has an API

Prioritize — Assign organizational criticality levels to help prioritize remediation

Correlate — Match threats and risks with organizational assets to develop a comprehensive risk mitigation process

Security Operations

Service monitoring — Access real-time metrics such as time-to-open, time-to-resolution and uptime against the defined SLA. Visualize ticket breakdowns on actions being performed, their timing and assigned analyst

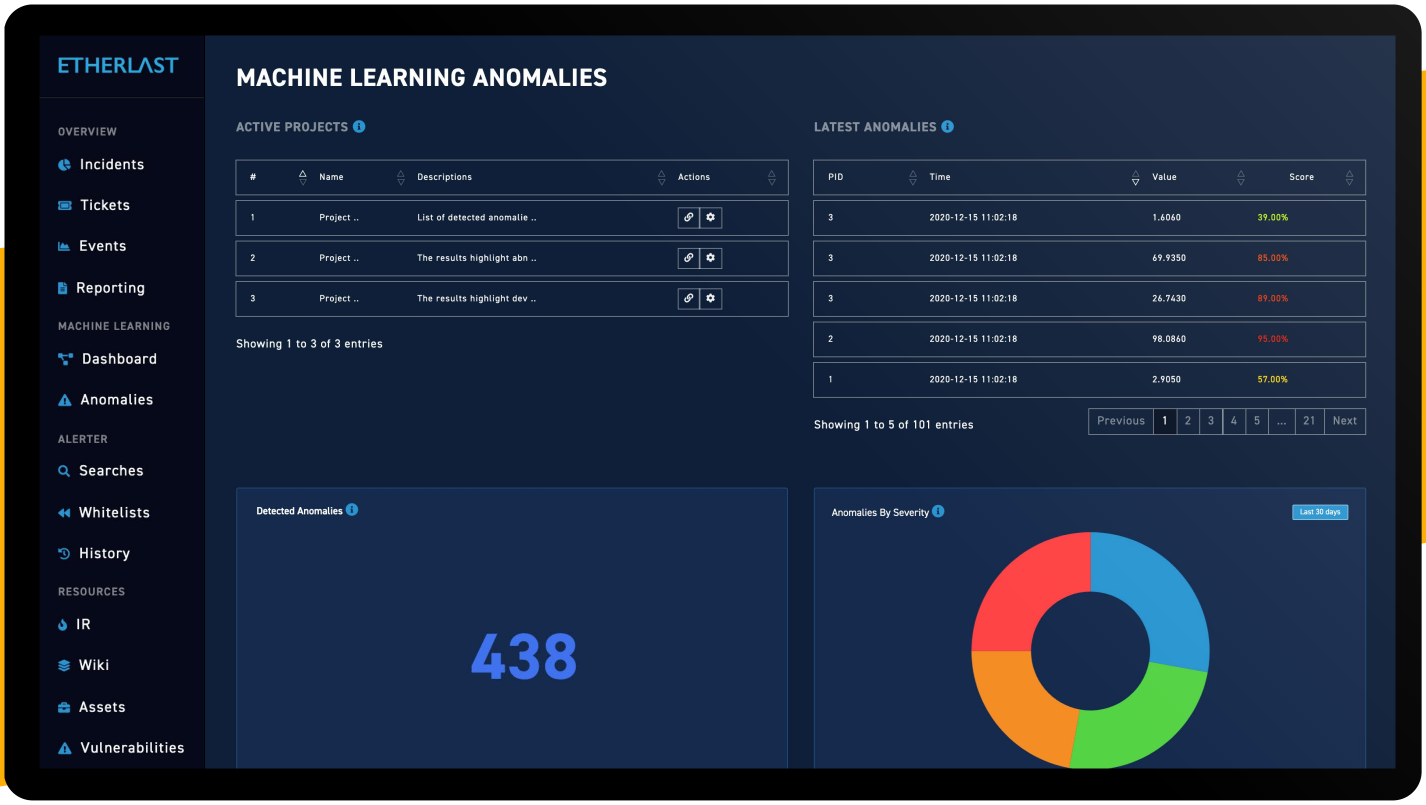
SIEM — Integrated security intelligence feeds and advanced correlation capabilities combined with machine learning supported UEBA and IR capabilities

Automation and orchestration — Use playbooks to automate tasks to minimize response time

Breakdown of alerts and incidents — Quickly evaluate where most alerts originate, root cause and trends in time, enabling task prioritization and planning

Extended visibility into your data — Endpoint, network, cloud and SaaS security events, all in one place

Case management - View details of every single alert and case, as well as track and follow analyst actions



MACHINE LEARNING ANOMALIES

ACTIVE PROJECTS

#	Name	Descriptions	Actions
1	Project ..	List of detected anomalie ..	
2	Project ..	The results highlight abn ..	
3	Project ..	The results highlight dev ..	

Showing 1 to 3 of 3 entries

LATEST ANOMALIES

PID	Time	Value	Score
3	2020-12-15 11:02:18	1.6060	39.00%
3	2020-12-15 11:02:18	69.9350	85.00%
3	2020-12-15 11:02:18	26.7430	89.00%
2	2020-12-15 11:02:18	98.0860	95.00%
1	2020-12-15 11:02:18	2.9050	57.00%

Showing 1 to 5 of 101 entries

Asset Management

All-in-one — Cybourn's SOC as a Service is based on assets being monitored enabling the build of a comprehensive asset database

Easy correlation — Alerts are matched with assets to have an integrated view between threats, security operations, and critical applications or systems

Increased visibility — EtherLast's asset module integrates all functions of an independent asset management platform, such as asset owner, data owner and custodian, versioning or financials

Reporting

Automated or manual reports — Bespoke reporting on information security incidents, aggregated metrics and dashboards. Vulnerability reports on the results of configured scanning tools

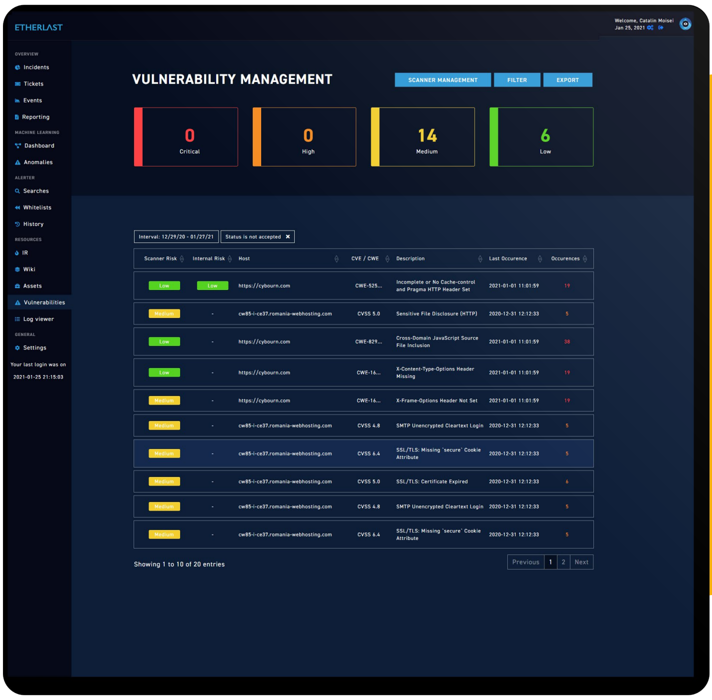
Compliance — Tracking of information security incidents and existing or remediated system vulnerabilities and correlation with standard or regulatory requirements

Infrastructure Status

Network and infrastructure security events — Visualize event trends

IT infrastructure health status — View real-time health status and infrastructure load incorporating NOC functionalities on networks and application

Data integrity, protection and defense — Visualize important data processes and monitor compliance



VULNERABILITY MANAGEMENT

0	0	14	6
Critical	High	Medium	Low

Interval: 12/29/20 - 01/27/21 | Status is not accepted ✖

Scanner Risk	Internal Risk	Host	CVE / CWE	Description	Last Occurence	Occurences
Low	Low	https://cybourn.com	CWE-525...	Incomplete or No Cache-control and Pragma HTTP Header Set	2021-01-01 11:01:59	19
Medium	-	cw85-i-ce37.romania-webhosting.com	CVSS 5.0	Sensitive File Disclosure (HTTP)	2020-12-31 12:12:33	5
Low	-	https://cybourn.com	CWE-829...	Cross-Domain JavaScript Source File Inclusion	2021-01-01 11:01:59	38
Low	-	https://cybourn.com	CWE-16...	X-Content-Type-Options Header Missing	2021-01-01 11:01:59	19
Medium	-	https://cybourn.com	CWE-16...	X-Frame-Options Header Not Set	2021-01-01 11:01:59	19
Medium	-	cw85-i-ce37.romania-webhosting.com	CVSS 4.8	SMTP Unencrypted Cleartext Login	2020-12-31 12:12:33	5
Medium	-	cw85-i-ce37.romania-webhosting.com	CVSS 6.4	SSL/TLS: Missing `secure` Cookie Attribute	2020-12-31 12:12:33	5
Medium	-	cw85-i-ce37.romania-webhosting.com	CVSS 5.0	SSL/TLS: Certificate Expired	2020-12-31 12:12:33	6
Medium	-	cw85-i-ce37.romania-webhosting.com	CVSS 4.8	SMTP Unencrypted Cleartext Login	2020-12-31 12:12:33	5
Medium	-	cw85-i-ce37.romania-webhosting.com	CVSS 6.4	SSL/TLS: Missing `secure` Cookie Attribute	2020-12-31 12:12:33	5

Showing 1 to 10 of 20 entries

Role-Based Dashboards

Executive Level — Aggregated view of organization cyber posture and business risks

IT Management Level — Overview of network and application health and security postures

IT Security Level — Action and response oriented data

Key Benefits

- Create custom dashboards and reports
- Ticketing SLA based on the level of threats
- Machine learning driven features
- NOC integration allowing a single pane of glass for SOC and NOC
- Alerting via multiple platforms such as email, Slack, and Messenger
- Bespoke risk scoring based on known vulnerabilities and threats

For more information about EtherLast and to arrange a demo contact sales@Cybourn.com

Integration and transparent reporting

CyBourn's philosophy dictates that all reporting must be simple, clear and relevant. CyBourn's EtherLast platform, a fully customizable Extended Detection & Response (XDR) platform that offers different layers of reporting for each management level ensures that managers, IT team, and executives can all view the organization's cybersecurity posture in real-time.

Cybersecurity strategy with your business objectives

CyBourn creates cybersecurity strategies that are closely aligned with business objectives in order to help streamline processes, gather valuable intelligence, and leverage the power of analytics. CyBourn delivers value-added security enhancement through business optimization.

Strategic Security Partner

CyBourn recognizes that every client is unique. By closely collaborating and engaging with our clients' Security Operations, IT Operations, and Compliance teams, we provide bespoke solutions that are carefully designed to meet unique requirements. Our operational model assumes full integration and optimized alert management with an organization's internal processes.

Always in compliance

CyBourn's Extended Detection & Respoonse (XDR) services offer the monitoring of compliance indicators — a service which assists clients operating in today's ever-increasing regulated environments. CyBourn's operational procedures and controls support clients in achieving compliance with national and international regulatory standards, such as GDPR, NIS, PCI-DSS, NIST, HIPAA, and SOC2. Partnering with CyBourn ensures that XDR operations and protocols adhere to internal policies, security standards, and risk profiles from the beginning. CyBourn's clients receive a detailed monitoring guideline document at the commencement of operations, which aggregates all the information likely to be required by internal audit and compliance functions.

CYBOURN'S DATA SOURCES

IoT

Web

Gateway services

ICS

Anti-malware

Windows

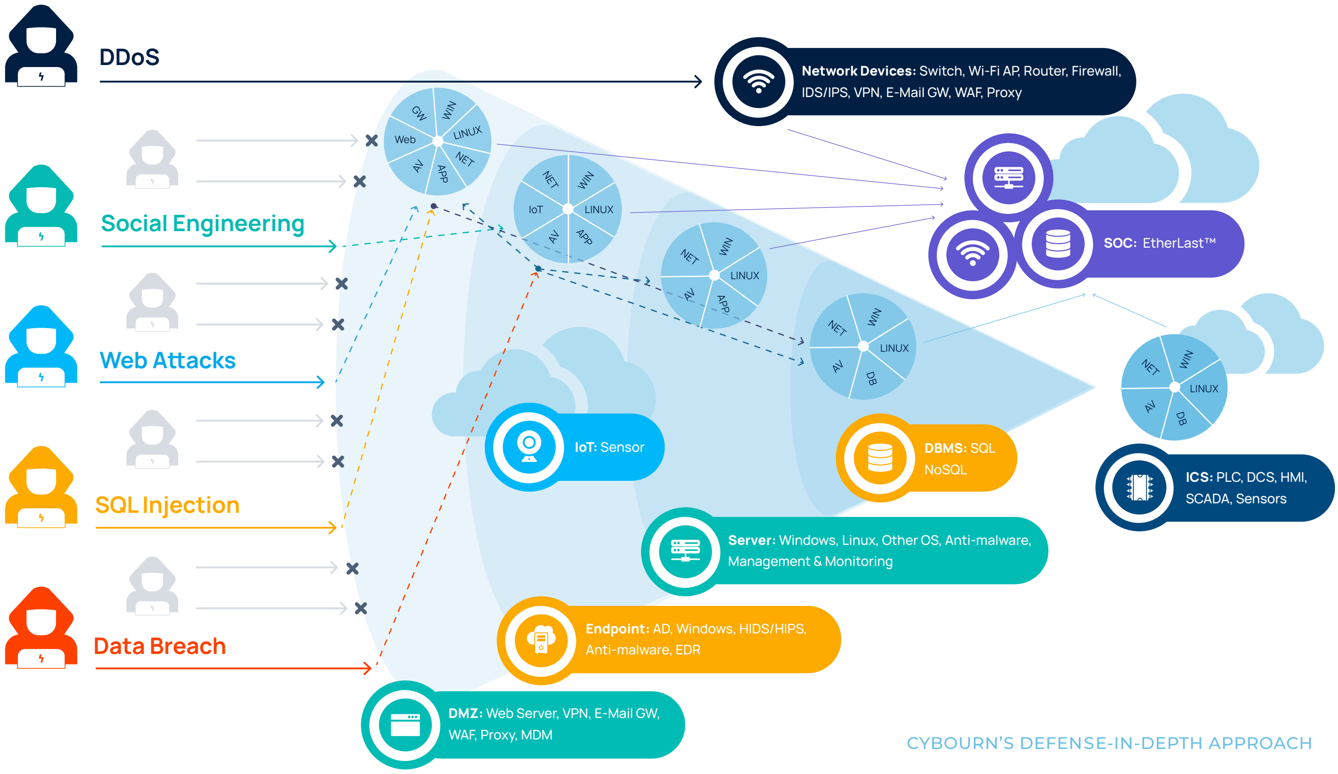
Linux

SaaS

Cloud

Network

How We Defend



DDoS

Social Engineering

Web Attacks

SQL Injection

Data Breach

Network Devices: Switch, Wi-Fi AP, Router, Firewall, IDS/IPS, VPN, E-Mail GW, WAF, Proxy

SOC: EtherLast™

ICS: PLC, DCS, HMI, SCADA, Sensors

IoT: Sensor

DBMS: SQL NoSQL

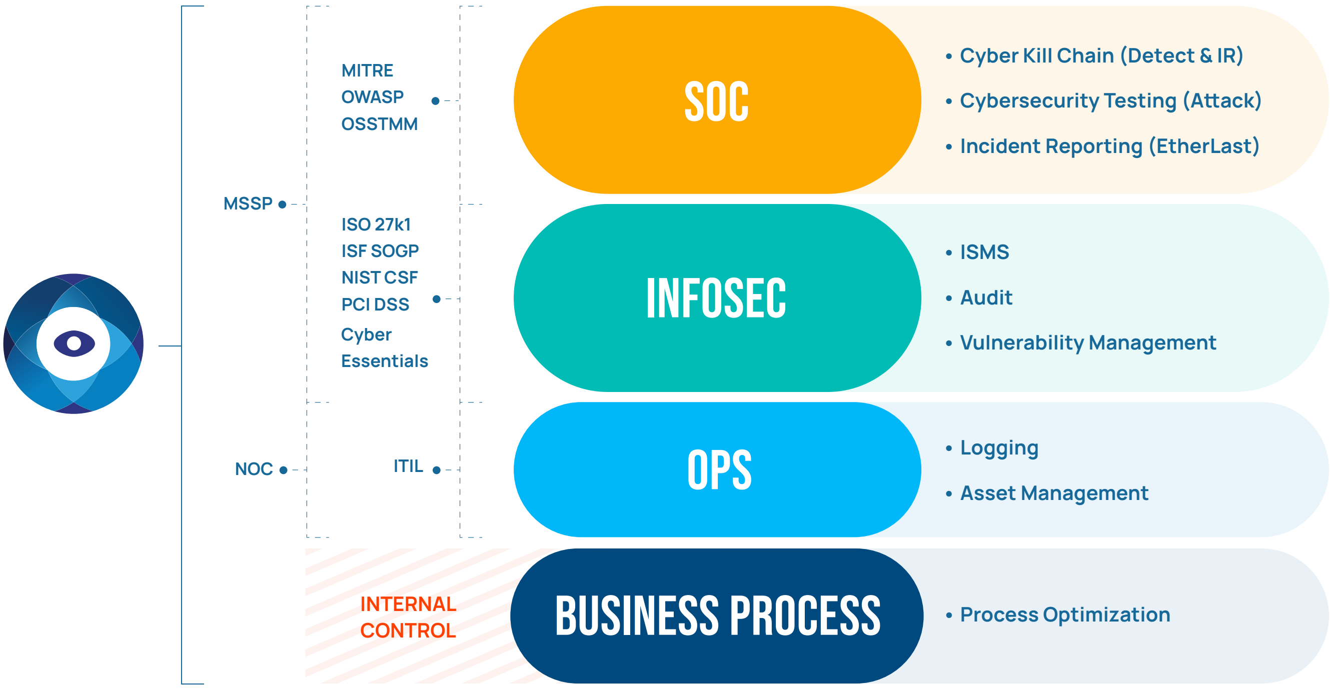
Server: Windows, Linux, Other OS, Anti-malware, Management & Monitoring

Endpoint: AD, Windows, HIDS/HIPS, Anti-malware, EDR

DMZ: Web Server, VPN, E-Mail GW, WAF, Proxy, MDM

CYBOURN'S DEFENSE-IN-DEPTH APPROACH

The difference in CyBourn's approach



MSSP

MITRE
OWASP
OSSTMM

ISO 27k1
ISF SOGP
NIST CSF
PCI DSS
Cyber Essentials

NOC

ITIL

INTERNAL CONTROL

SOC

- Cyber Kill Chain (Detect & IR)
- Cybersecurity Testing (Attack)
- Incident Reporting (EtherLast)

INFOSEC

- ISMS
- Audit
- Vulnerability Management

OPS

- Logging
- Asset Management

BUSINESS PROCESS

- Process Optimization

Vendor Agnostic

CyBourn offers bespoke integration solutions from technical infrastructure all the way to reporting.

We can utilize existing client tools, or act as security integrators to recommend and implement open-source, commercial, or off-the-shelf products. We deploy SOAR (Security Orchestration, Automation, and Response) solution stack to ensure deep visibility, continuous analysis, and rapid response. If an existing product or solution does not offer the needed level of visibility for you, CyBourn can build custom tools to collect relevant data.

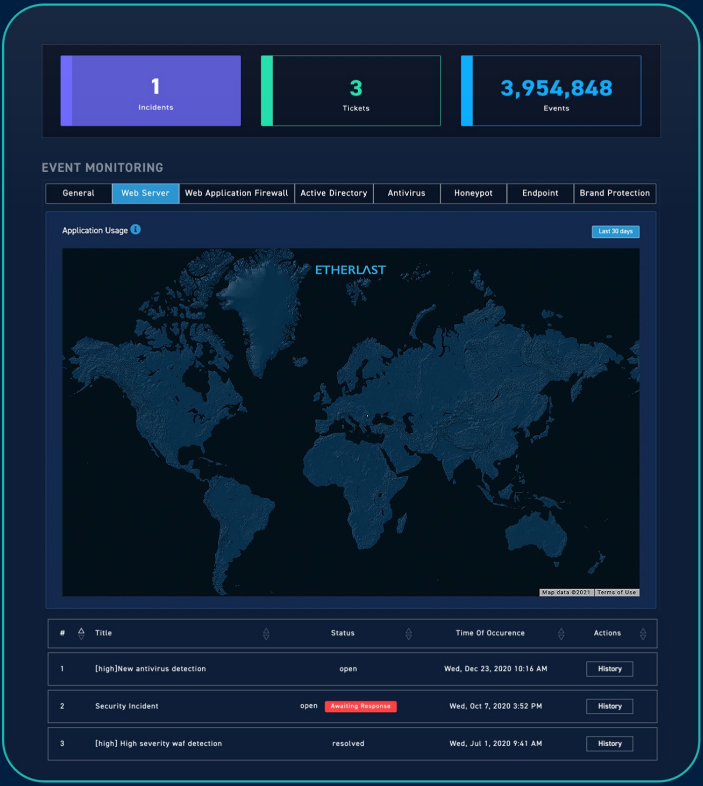
Driven by Machine Learning (ML)

CyBourn leverages bespoke ML algorithms.

CyBourn leverages machine learning algorithms to build network and user behavioral patterns, detect anomalies accurately, perform in-depth investigations, and act swiftly to contain potential threats, enhance proactive analysis, and map behavior.

Flexible Deployment

Clients can choose to work with us in one of three ways: Your infrastructure, Our infrastructure, or in a hybrid environment while building critical playbooks and evaluating threats.



#	Title	Status	Time Of Occurence	Actions
1	[high]New antivirus detection	open	Wed, Dec 23, 2020 10:16 AM	History
2	Security Incident	open Awaiting Response	Wed, Oct 7, 2020 3:52 PM	History
3	[high] High severity waf detection	resolved	Wed, Jul 1, 2020 9:41 AM	History

EtherLast™

The only Extended Detection & Response (XDR) platform you need to track your security posture

ONE-CLICK REPORTING

BESPOKE ARCHITECTURE

VIDEO-WALL READY

01. Executive Level

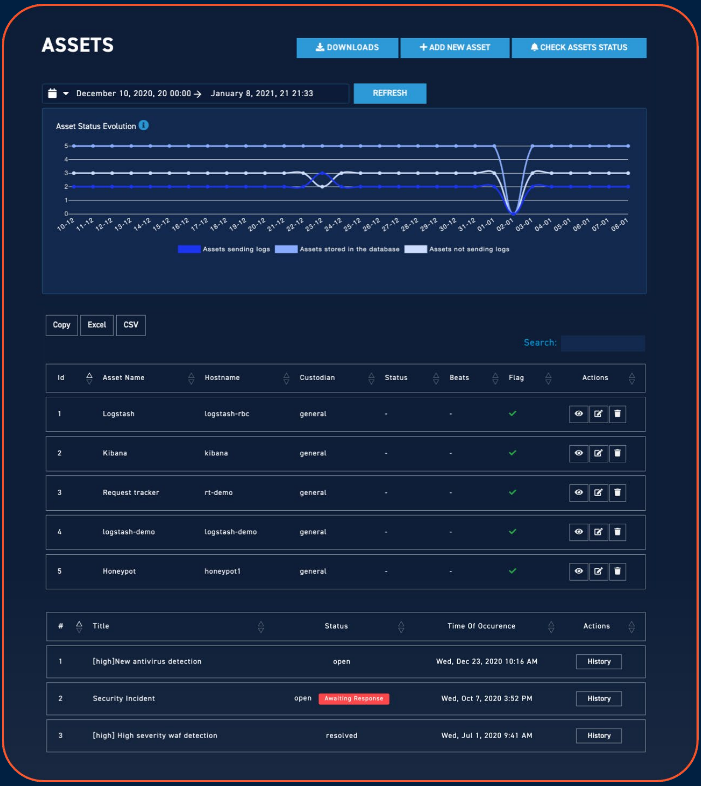
Aggregated view of organizational risks

02. IT Management Level

Overview of infrastructure health and security postures

03. IT Security Level

Action and response oriented data



Id	Asset Name	Hostname	Custodian	Status	Beats	Flag	Actions
1	Logstash	logstash-rbc	general	-	-	✓	
2	Kibana	kibana	general	-	-	✓	
3	Request tracker	rt-demo	general	-	-	✓	
4	logstash-demo	logstash-demo	general	-	-	✓	
5	Honeypot	honeypot1	general	-	-	✓	

#	Title	Status	Time Of Occurence	Actions
1	[high]New antivirus detection	open	Wed, Dec 23, 2020 10:16 AM	History
2	Security Incident	open Awaiting Response	Wed, Oct 7, 2020 3:52 PM	History
3	[high] High severity waf detection	resolved	Wed, Jul 1, 2020 9:41 AM	History

Offices

Enabled by our R&D and continuous internal development process that are deeply integrated with operations, we cover the entire cybersecurity landscape for enterprises across industries, sectors and geographies 24/7.

London, UK

Washington D.C., USA

Ashburn, Virginia, USA

Bucharest, Romania

Naples, Italy

CYBOURN