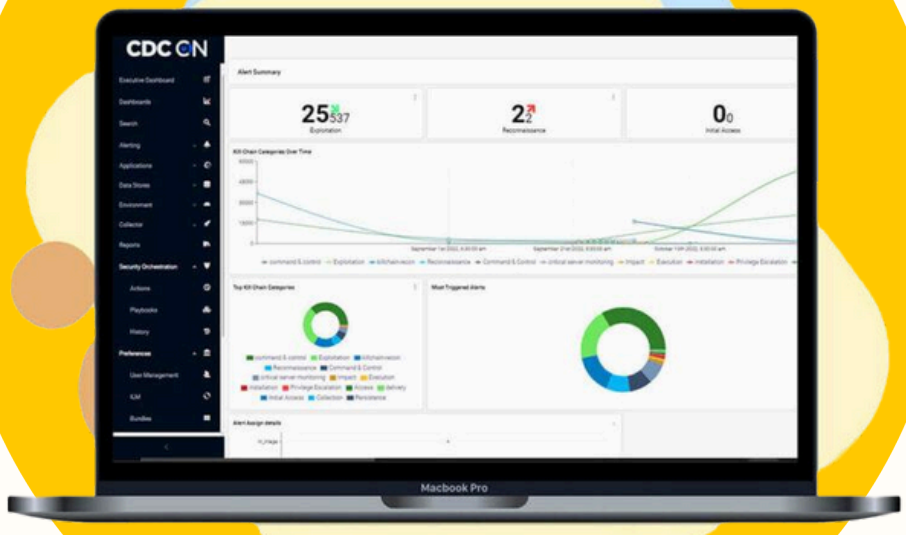
CDC ON®

A Next Generation SIEM, SOAR, EDR, XDR-MDR for Enterprises, MSSPS, and all Businesses.



Cybersecurity. Made Simple & Affordable.
IDENTIFY. PROTECT. DETECT. RESPOND. RECOVER.

CDC ON

CDC-ON® is a next generation SIEM, SOAR, EDR, XDR-MDR Platform

Zero trust. Containerized Microservices Architecture.
Highly Efficient. Highly Reliable. Highly Scalable. Highly Flexible
Enterprise-Class Cybersecurity for All.

Code Level, Fully Customizable:

Cybersecurity Platform for IT & OT.

Code, API Level Integration:

Integrate with any security tool or platform for a single security dashboard.

CDC-ON is Highly Efficient:

Extensive integration, customization and augmentation of all cybersecurity tools / technologies with advanced log correlation help **Reduce Dwell-time of an Attack.**

CDC-ON is Highly Customizable:

MSSPS can custom build niche CaaS while enterprises can have custom built features, modules, dashboards, reports.

CDC-ON is Highly Reliable:

Zero Trust Architecture with CDC proprietary Quad Server deployment makes CDC-ON support SLA & availability at 99.9999% uptime.

CDC-ON is Highly Scalable:

Deployable even on a single laptop for a small SMB or on augmentable mega Quad Servers on prem or on cloud defending millions of enterprise end-points & its infrastructure.

Flexible Deployment and Licensing:

Supports Cloud, On-Prem licensing based on number of: endpoints, EPS, or log volume of the enterprise. For MSSPS and partners license can also be based on Royalty / Revenue Share models.

Contact:
contact@cdc-on.com
www.cdc-on.in

Cybersecurity. Made Simple & Affordable.
IDENTIFY. PROTECT. DETECT. RESPOND. RECOVER.

CDC ON

CDC-ON® is a next generation SIEM, SOAR, EDR, XDR-MDR Platform

Prevents Un-known Threat & AI-Powered Polymorphic, Oligomorphic & Metamorphic Malwares:

Integrated, augmented fully configured CDC-ON platform can detect un-known threats including mutating or Large Language Model (LLM) generated polymorphic malwares capable of evading siloed EDR, XDRs & SIEMs.

Synthesis of Threat Intelligence, Full Environment Telemetry and AI-Powered User Behavior Analytics:

To effectively address current sophisticated risks, CDC-ON employs complex anomaly detection algorithms applied at various threat hunting and detection levels. CDC-ON uses baseline detection models and ventures into deep belief network multi-layer generative models.

CDC-ON Security Data Store:

Securely and reliably stores vast amounts of security event information. The data store includes built-in replication and data management features and is easily configurable from the platform UI.

Custom Dashboarding:

Fully customizable dashboard. Supports a drag & drop builder with easy visualization and configuration modes. The dashboard suite also support drill down for global filters providing additional power to analysts. MSSPs can build any compliance or stakeholder dashboard as per their client needs.

CDC-ON, The Integrated, Augmented, Customized, Contextual Assured Security:

CDC- ON works as a security umbrella on top of an organization's current security implementation providing real-time visibility into its entire digital space and activities. Provides efficient threat detection with minimal false positives.

Extensive Threat Detection Techniques:

Apart from standard signature based detection, CDC-ON employs, heuristics static and dynamic approach, machine learning, malware normalization and other patent pending techniques. Easily detects fluctuating shapes and signatures of constantly evolving malware.

Advanced Data Search Language:

CDC proprietary Query Language is a simple syntax data search language with advanced correlation, mathematics, & enrichment features. The language is built for analysts by analysts.

Custom Reporting:

Fully customizable custom reports generatable within minutes. Supports drag & drop builder with easy visualization and configuration modes. Dashboarding & Reporting are used by analysts & executives for compliance and efficient governance. Provides complete security posture overview custom delivered per stakeholder needs.

Contact: contact@cdc-on.com | **www.cdc-on.in**

Cybersecurity. Made Simple & Affordable.

IDENTIFY. PROTECT. DETECT. RESPOND. RECOVER.

CDC ON

CDC-ON® is a next generation SIEM, SOAR, EDR, XDR-MDR Platform

CDC-ON Multi-tenancy for MSSPs and large Enterprises:

CDC-On has built-in multi-tenancy in multiple modes to support MSSP and large enterprise requirements. A single instance can host multiple clients, and a single console can be used to securely view and manage multiple instances.

CDC-ON Cluster Deployment:

Cluster deployment support provides load balancing and data high availability within an installation.

CDC-ON Deploy Anywhere:

CDC-On server can be deployed anywhere, on-prem (single or multiple servers), hybrid and cloud deployment models are natively supported by CDC-ON.

CDC-ON High Availability:

High availability support with DR deployment provides high availability and quick disaster recovery.

CDC-ON 24x7 Engineering and Customer Service Support:

Analyst and customer support teams: for operations support

Content engineering team: for assistance in creating dashboards, detection rules, and reports.

Threat research teams: for detecting threat scenarios & providing intelligence to CDC-ON & the security community.

Contact:
contact@cdc-on.com
www.cdc-on.in

Cybersecurity. Made Simple & Affordable.
IDENTIFY. PROTECT. DETECT. RESPOND. RECOVER.

CDC ON

CDC-ON® is a next generation SIEM, SOAR, EDR, XDR-MDR Platform

Alerting:

CDC-On's alerting module detects threats & notable events in near real-time from millions of lines of data logs & efficiently informs respective stakeholders.

In-built & Customized Rules:

Along with an inbuilt rule list, users can create customized rule lists for business and security requirements. Any fine-tuning required for the inbuilt rule list can be performed by the administrator.

Alarm Investigation Workbench:

CDC-On provides investigation workbench for each alarm with in-built SLA tracking & analyst assistance feature. This a powerful, but an easy tool that help analysts maintain focus in triaging.

Alarm Workflow and Ticketing System:

The alarm workflow & ticketing system are inbuilt within the CDC-On XDR. Using this feature, the stakeholders & analysts can communicate & view details of the tickets from a customized Role-Based-Access-Controlled (RBAC) console. This feature increases overall efficiency of the SOC.

CDC-ON Data Collection Suite:

CDC-On end-point data collection is done through a proprietary, centrally managed, data collector agent. Data collection also supports a wide variety of open-source standards & toolsets for universal data collection & ingestion. The data collection agents are an all-in-one package that collects logs of operating systems, kernel monitoring, system metrics, process execution, print, USB access, & many more.

Agent-less and Cloud Infra Data Collection:

CDC-ON can also support agent-less data collection. Collectors for agentless data, cloud infrastructure logs for Azure, AWS, etc., are easily configurable in cluster and high availability modes.

Contact: contact@cdc-on.com | www.cdc-on.in

Cybersecurity. Made Simple & Affordable.

IDENTIFY. PROTECT. DETECT. RESPOND. RECOVER.

CDC ON

CDC-ON® is a next generation SIEM, SOAR, EDR, XDR-MDR Platform

Robust Universal Threat Feed System:

CDC-On supports a wide range of threat-feed formats like TAXII, MIPS, OTX, etc., or even a simple feed format like CSV, line by line, simple URLs. This flexibility allows CDC-ON to consume threat feed data from anywhere: commercial feeds, or even a simple GitHub repository with IOC listed in a text file. Feeds are automatically kept up-to-date & tightly integrated with search & alerting system to ensure that threats are immediately as they are known.

Security Orchestrations and Response (SOAR):

Drag and drop playbook-based SOAR is built within CDC-ON XDR. SOC can automate analysis and response process using this robust SOAR. Using the easy to use drag and drop playbook builder users can build playbooks. These playbooks can be triggered manually or automatically.

Process, File, Registry, Network Events Natively Captured by Agent:

CDC-On agent has end-point EDR level data collection feature inbuilt to collect events like process creation, process trees, registry modification details, network connection events etc., directly from the operating system kernel.

Incident Investigation Workbench:

Allows an analyst to group and visualize events & alarms related to an incident or in a threat hunting scenario to easily spot security risks. Workbenches can be saved & updated any time in the process. Workbench includes special visualizations to identify and security risks.

Entity Relationship Explorer:

Built-in entity relationship is an interactive workflow explorer for analysts to visually understand the relationships & similarities between varied entities in security analysis.

Process Explorer:

Gives the timeline view of process monitoring events captured by CDC-On agents. Events are represented in the timeline, IOCs are highlighted as malicious library loads. The process tree is available for the analyst to click & navigate between parent & child processes & their timelines.

Contact: contact@cdc-on.com | www.cdc-on.in

Cybersecurity. Made Simple & Affordable.

IDENTIFY. PROTECT. DETECT. RESPOND. RECOVER.

CDC ON

CDC-ON® is a next generation SIEM, SOAR, EDR, XDR-MDR Platform

CDC-ON Additional Features:

- Pre-built content bundles with updates from CDC-On central repositories
- RBAC on all components and features with multi-tenancy support
- Integration with ticketing systems and third-party solutions like email, intelligence search systems, Applications, ERP, Databases
- Enterprise authentication models with LDAP and ADFS
- Multiple color themes look and feels
- Backup and export/import features
- Data ingestion and parsing from UI
- Data ingestion pipeline with conditional parsing and branching in pipelines
- Direct mapping to security analytics framework like MITRE with framework level visualizations
- Lookup lists and asset DB
- Data lifecycle management from UI
- Separate admin UI for multi-tenancy management
- System management and health dashboards
- Notifications from UI user on critical events
- Alarm throttling and grouping filters
- Packet collection and analytics capability for OT technologies and protocols
- Inbuilt SLA tracking and enforcement

CDC-ON Key Feature Updates:

- CDC-On EDR: EDR features to CDC-On with cloud intelligence and local malware detection, with both static and user behavioral detection models making CDC-On a complete XDR
- CDC-On Compliance monitoring: CDC-On will monitor and validate a wide range of compliance needs for IT (On-premise/Cloud/Mainframe systems), OT and IoT systems with respect to industry standards and best practices
- CDC-On Agent for mobile OS: Android
- Better out-of-the-box integration support by collaborating with other system vendors in MDM, Patch Auditing etc
- Wizards for system onboarding and analysis use-cases
- CDC-On easy ML rule builder suite
- Revamped ticketing and ticket management solution
- CDC-On SaaS model with auto-instance provisioning and easy setup
- AI/system-assisted analysis and incident handling for SOC analysts
- Features for MDR service delivery
- CDC-On customer support portal with documentation and ticketing

Contact:
contact@cdc-on.com
www.cdc-on.in

CDC ON

The Only Code-level customizable Security Operation Centre Platform.

Build your own custom features, modules, dashboards, reports, and even niche custom SOCaaS. CDC-On integrates/replaces any SIEM, EDR, XDR, Antivirus, providing a full-service SOC platform custom built for your business.

A complete active defense platform with in-built SIEM, SOAR, EDR, XDR-MDR.

Highly scalable: CDC-ON is lightweight and can be deployed on a laptop for small businesses with few end points or on high-end servers deployed on-premise or on -cloud supporting more than million endpoints!

API and code-level integration with any client application, database, security tool to provide an integrated enterprise dashboard.

Supports IT, OT, IoT.CDC-ON can be a full-fledged SOC, or an integrated enterprise-wide umbrella security dashboard integrating and augmenting current and future client security tools and platforms.

The only SOC platform by analysts for analysts.

USA	MENA Region	India
Flanders, NJ	Abu Dhabi & Dubai, UAE	Technopark, TRV
Cedar Rapids, IA	Muscat, Oman	Govt. Services, HYD
	Yerevan, Armenia	Govt. Services, DEL

Contact: contact@cdc-on.com | www.cdc-on.in