UST

CyberProof®
A UST Company

Centralized cybersecurity command and response for healthcare providers

Rapidly detect and respond to incidents that impact hospitals operations and patient care.

ust.health

Faster time to value for your enterprise cybersecurity

Healthcare organizations are struggling quickly detect and respond to security incidents due to their expansive attack surface. Massive volumes of alerts are being generated from multiple security technologies and logs, such as Epic EHR, access, email and end-points. The ever-increasing list of products and platforms to manage your cybersecurity monitoring and detection capabilities may not always offer a clear path to maturity or return on investment for healthcare organizations.

Centralized cybersecurity command and response services are powered by CyberProof Defense Center (CDC®) Platform enables healthcare organizations to detect and respond to validated threats faster without adding any complexity to the security infrastructure.

Offerings and differentiators

Single view of security operations

- CDC platform integrates with your **existing security investments without additional infrastructure**.
- CDC ingests data from multiple sources (SIEMs, EDR, MDR, IoT, and other sensors) and correlate limitless volumes of data regardless of where it resides to provide a single pane of glass view of enriched alerts and incident handling activities.
- The data ingestion layer focuses on the most relevant detection priorities surfaced by MITRE Att&ck matrix, **generating 40% reduction in data and up to 60% in cost savings**.

Faster detection and response

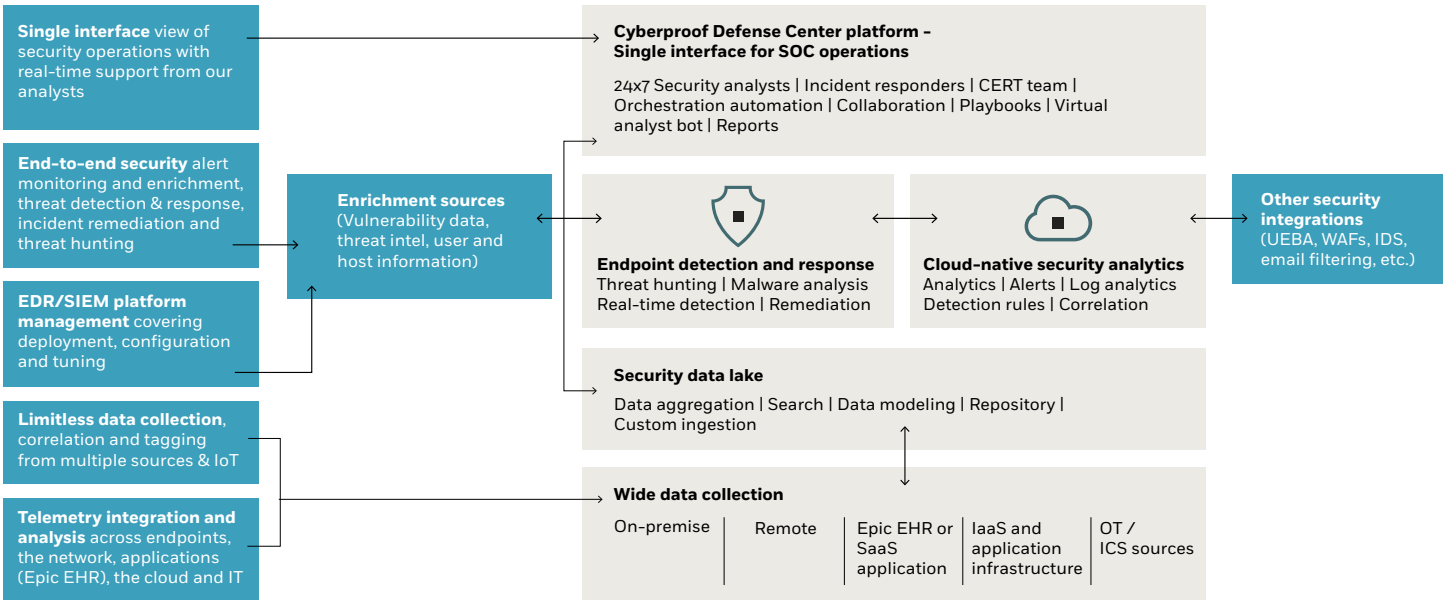
- 24x7 round-the-clock security alert monitoring, enrichment and triage
- SeeMo, our AI analyst, acts as a virtual member of your team to **automate up to 85% of L1+L2 activities,** including alert monitoring, enrichment, triage, investigation and issue containment, significantly reducing human efforts.
- Real-time collaboration — transparent activities providing you with support for issue containment, remediation, risk mitigation and personalized reporting.

Proactive incident handling

- Our global response team proactively carries out detailed investigations to search across the enterprise for signs of suspicious activity and **remediate threats using tailored responses**.
- The unique **Use Case Factory (UCF)** allows continuous configuration and tuning of customized detection rules and response procedures, leveraging our curated library of threat detection and response content.

Faster time to maturity for your enterprise cybersecurity

How it works?



Case study: Cybersecurity centralized command and response services for a multinational insurance company

Client challenge

The client's goal is to ensure business operations remain secure by transforming the firm's current cyber practices and establishing an innovative, next-gen cybersecurity SOC operation.

In its search for a security solution, client was not looking for a traditional MSSP, but rather a partner willing to work in a hybrid model where cloud and on-site resources and assets would complement each other.

UST solution theme

- Adoption of a holistic & risk-based approach to threat detection and response to increase security resilience
- Integration of orchestration and automation platforms to minimize business impact
- Development of streamlined SOC processes and innovative tools that drive operational efficiencies and reduce costs
- Implementation of a cloud-native SIEM to enable a hybrid cloud architecture

Benefits

- **Fewer false positives** as data and logs are collected from multiple sources, reducing errors and time to detect
- **Cloud-native and hybrid deployment** providing greater operational efficiency, by leveraging cloud-native tools and automations
- **Reduced risk** with orchestration & automation capabilities that provide faster time to response and increased visibility
- **Single view** supporting multi-team SecOps collaboration, with real time alerts and recommendations
- **Extended security monitoring** for Office 365 and other web applications

Impact

90%
increase in public cloud monitoring

70%
reduction in operating and licensing costs

>12%
YoY operational efficiency gains

Faster time to detection for your enterprise cybersecurity

Independently recognized leader

Our CyberProof Defence Center (CDC) is a MDR award winner and recognized as a “Leader” by Forrester in the midsize managed security services market. HIPAA, GDPR compliant. HITRUST CSF ready

Tailored healthcare threat intelligence

Active monitoring of multiple threat sources across the clear, dark, and deep web.

Realtime visibility of targeted threats to organizations’ specific assets, data and people

Multi-layered threat hunting

Usage of a unique combination of sources to search for threats lurking in your environment including known IOCs, incident information, proprietary threat intelligence, MITRE blind spots and behavior

HOW WE RESPONDED TO BLACKCAT RANSOMWARE ATTACK?

Real-life examples that will empower your security teams

L1 initial response and triage

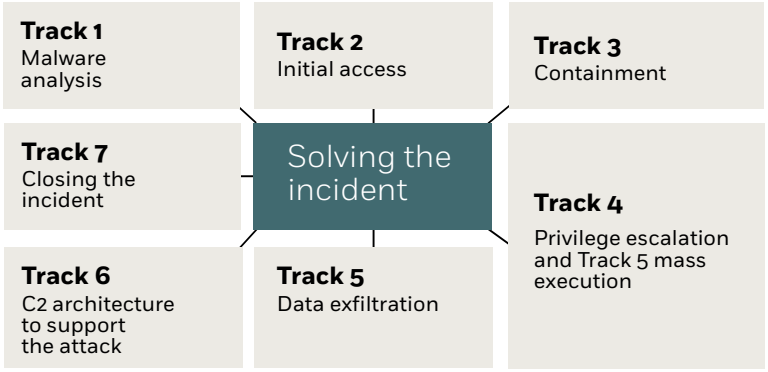
CyberProof’s Security Operations Center (SOC) received hundreds of alerts in a short period of time regarding the detection of a BlackCat ransomware attack on one of our clients.

The L1 team started to investigate the suspicious alerts. CyberProof’s managed EDR was able to prevent the execution of two malicious files, but the L1 team escalated the severity to a critical level after they realized that large numbers of assets were encrypted. The team received additional alerts regarding behavior across the environment, an indication of infection.

Based on the above, the L1 team confirmed with the L2 team that the client was faced with an active ransomware infection.

Managing incident response

As soon as the incident was confirmed as representing an active intrusion, the response team kicked into action across 7 tracks, starting from analysis, containment, futureproofing and incident closure.



For detailed report and more real-life examples, ask for our 2023 Cyber defenders playbook.

About UST Health

15+
Years delivering healthcare services, 12+ years of Epic EHR

100+
Healthcare provider and payor clients

70%
Reduction in operating and licensing costs with CyberProof platform

10-15%
YoY operational efficiency gains with Cyberproof automation and Use Case Factory

100%
Outcomes based contract (risk sharing)

17
Global healthcare delivery centers, 5 delivery centers in the United States

Engineering connections to better healthcare

About us

UST offers health tech solutions that enhance trust, connectivity, personalization, and efficiency for healthcare and life sciences enterprises. Our human-centered approach creates a more caring and connected future at physical and digital health convergence. Our deep domain experts ensure clients swiftly adapt to evolving tech and regulatory landscapes so they can focus on their core objective of promoting better health and care.

Discover our healthcare and life sciences work at
ust.health

Safeguard operations and protect data

Learn more now →

Accelerate Azure adoption and migration

Learn more now →

U ▪ S T