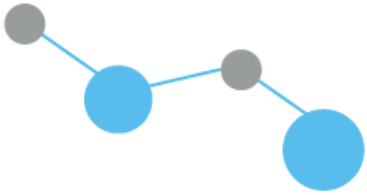
VOLON

CYBER THREAT INTELLIGENCE FOR

# HEALTHCARE / PHARMA

THREAT INTELLIGENCE USE CASES FOR
THE HEALTHCARE/PHARMA SECTOR

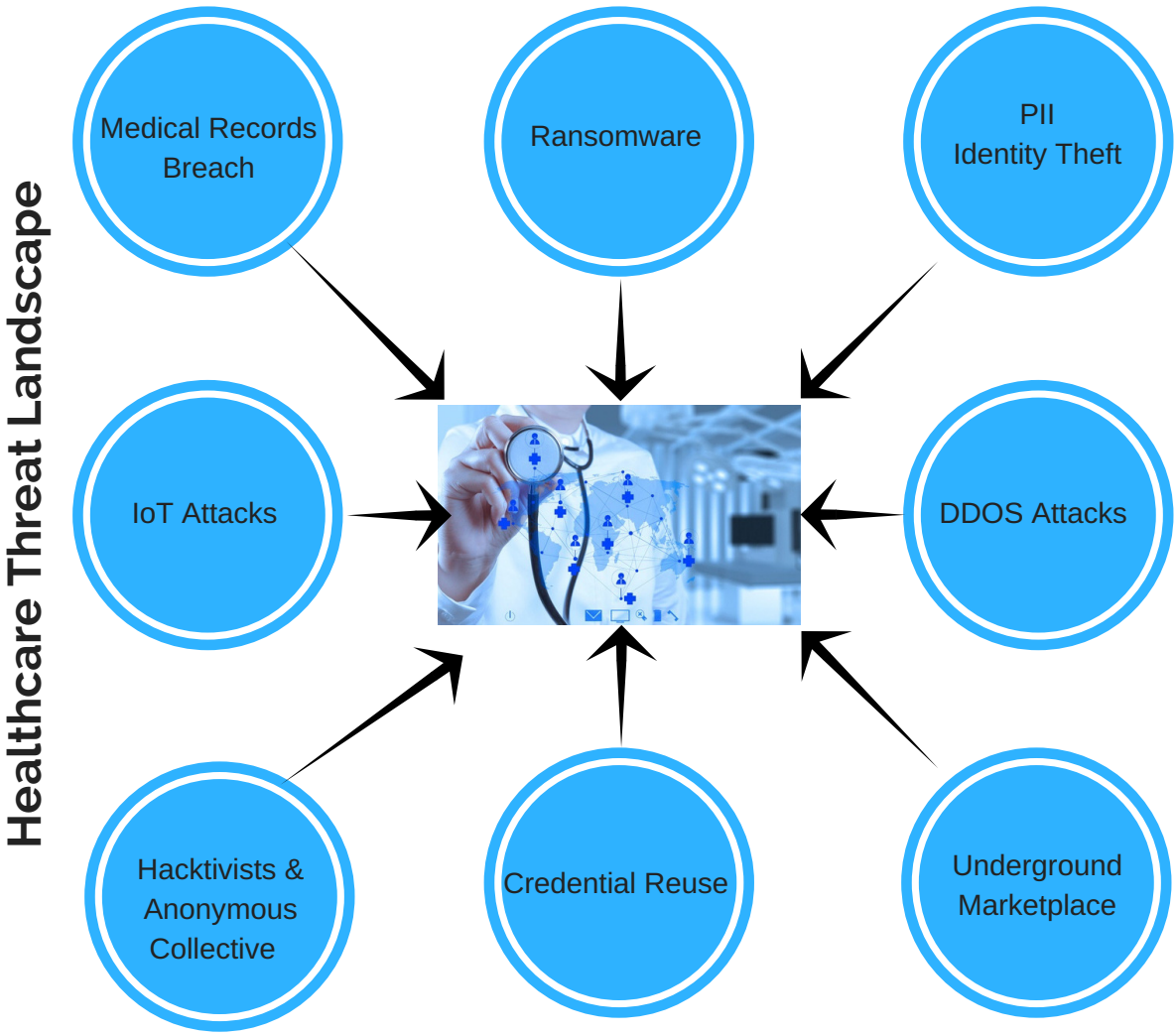


# THREAT LANDSCAPE

Over the years, Incidents of cyber attacks on Healthcare/Pharma industry has multiplied exponentially, there is also significant increase in magnitude of each attack with one of the largest data breach has impacted around 80 Million people.

Most health care organisations have limited budgets for cyber security programs and personnel to provide adequate response or protection from such attacks. In the era of electronic medical records the data becomes more easily accessible to bad actors, problems increase multi-fold with increase in number of different entities who handles medical data such as Health Care Providers , Pharma Companies , Payment processors , Medical Device manufacturers etc.

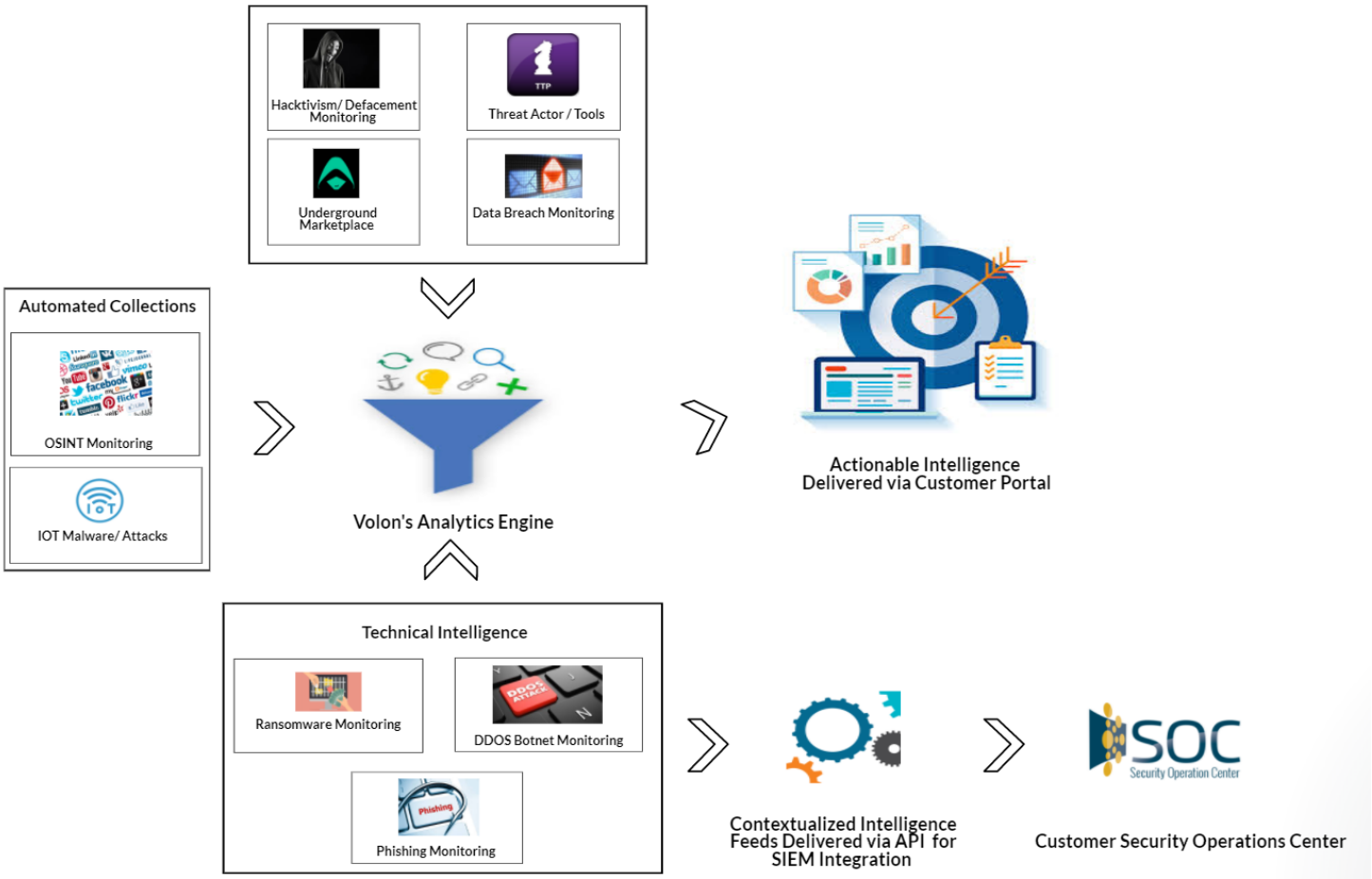
According to the study, $6 Billion is estimated costs towards cyber attacks in healthcare industry and around 47% of the health care providers have accepted to had security related events in their setup.



# THREAT INTELLIGENCE OFFERINGS

Volon's dedicated threat research team for healthcare services curates specialized output for customers. With unmatched monitoring capabilities linked to threat landscape of every customer to provide actionable intelligence.

Managed Threat Intelligence clubbed with contextualized technical feeds along with real-time alerts and reporting backed with specialized Human Intelligence (HUMINT) , Open Source Intelligence (OSINT) and Technical Intelligence (TECHINT) will ensure end to end coverage of external threat and adversary insights.




## Outcomes

Volon's unique process of initial customer threat scoping helps to identify customer specific actionable intelligence insights. Healthcare sector specific observable via specialized HUMINT operations are delivered via customer portal. Volon's HUMINT research capability provides adversary focused insight with context such as Intent, Motivation and TTP.

Data generated via Technical Intelligence can be consumed via Volon's Intelligence Portal or can also be directly ingested by customer's SIEM platform to integrate with SOC operations.

VOLON

## CONNECT WITH US FOR MORE INFORMATION

https://www.volon.io

info@volon.io