RANGESTORM

Bhumi iTech

RANGESTORM - THREAT DETECTION AND RESPONSE PLATFORM

> ”
>
> OUR CYBER THREAT INTELLIGENCE TEAM WILL ADD NEW DETECTION SO YOUR SOC CAN STAY AHEAD WITH ADVERSARY TARGETING YOUR ORGANIZATION.

Average time to detect a data breach is 207 days

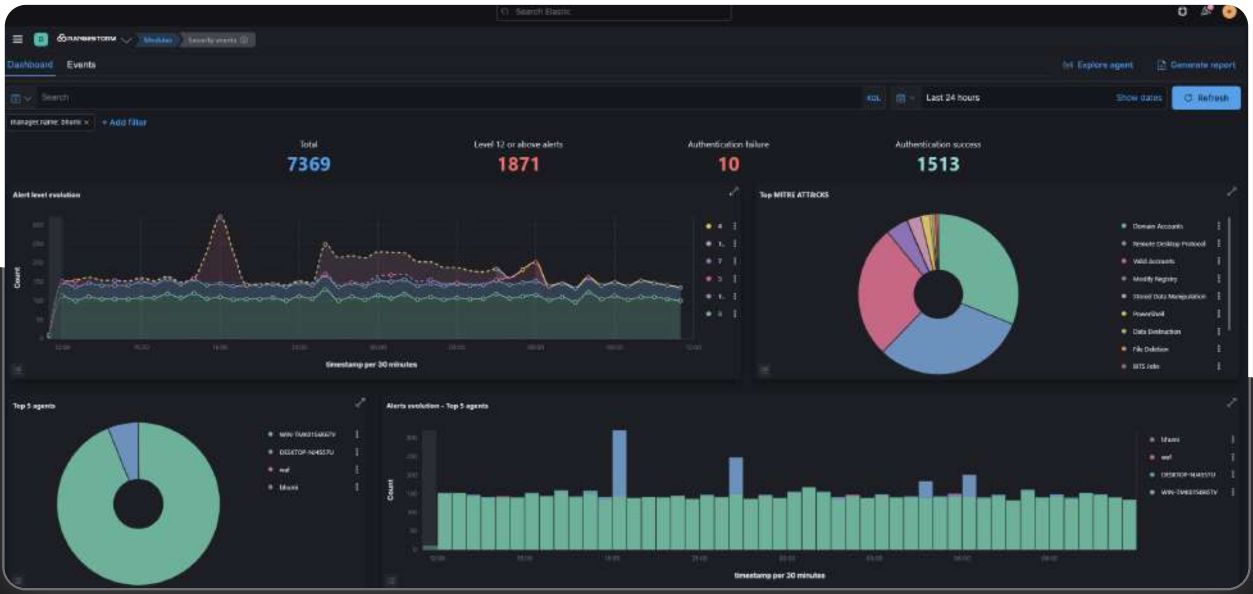
Average time to contain an attack is 70 days

> ”
>
> AVERAGE COST OF A DATA BREACH AT CRITICAL INFRASTRUCTURE, GLOBALLY IS USD 4.82 MN*. THIS FIGURE STANDS AT USD 2.32 MN IN INDIAN CONTEXT.

- Government & Defense agencies, financial institutions and various enterprises are increasingly being data breached. The probability and extent of damages keep on mounting with each passing day.

- Therefore it is extremely critical to detect the breach at the earliest and respond to it in the most efficient manner.

- Rangestorm is meant to automatically detect and respond to the incoming threats as per the playbook. Security anomalies are detected and identified for appropriate action. Security reports are generated and compliance is automated.



Features	Basic	Intermediate	Advance
1. Security Information Management			
Security Events	✓	✓	✓
Integrity Monitoring		✓	✓
2. Threat Detection & Response			
Vulnerabilities Detection	✓	✓	✓
Virus Total Analysis		✓	✓
OSQuery			✓
MITRE Att&ck		✓	✓
Data Breach Assessment			✓
3. Audit & policy Monitoring			
Security Configuration Assessment	✓	✓	✓
4. Regulatory & Compliance			
PCI DSS	✓	✓	✓
NIST 800-53	✓	✓	✓
TSC	✓	✓	✓
GDPR	✓	✓	✓
HIPPA	✓	✓	✓
5. Threat Intelligence			
Malware Bazar		✓	✓
Abuse Malware		✓	✓
Alienvolt OTX		✓	✓
MISP			✓
Virus total		✓	✓
6. Deception			✓
7. Full Packet capture			✓