DARK WEB MONITORING

“Get real-time dark web exposure alerts and find out what cybercriminals know about your employees and customers”

SOC continuously monitors your corporate domains and employee data against a database of breached data on the dark web, alerting you immediately through a triaged escalation process led by a human SOC analyst. Our team then works with yours to take corrective actions in the event of a breach. Our mission is to make the web a safer place by disrupting darknet underground activities and proactively protecting our customers against stolen corporate credentials and compromised machines, ultimately stopping bad actors from profiting off stolen corporate data.

CHALLENGE

The challenge that organizations face is that while they may conduct assessments of their network and internet-facing IT infrastructure to detect vulnerabilities, the conventional penetration testing approach often emphasizes applications and network device scanning, which is not enough to detect and prevent breaches. This is because most breaches start with compromised accounts, which makes it vital to explore and validate what data has been traded with bad actors on the dark web. This is where Dark Web Monitoring comes in, by providing real-time dark web exposure alerts and helping organizations find out what cybercriminals know about their employees and customers. It enables organizations to take timely preventive and corrective actions, as well as providing an insight into their existing threat landscape, by providing all the necessary information about the compromise.

DO YOU KNOW

- **320+ BILLION**

  RECAPTURED ASSETS

- **28+ BILLION**

  TOTAL PASSWORDS

- **35+ BILLION**

  EMAIL ADDRESSES

- **225+ BILLION**

  UNIQUE DATA TYPES

BUDDY TO A SECURITY TEAM - DARK WEB

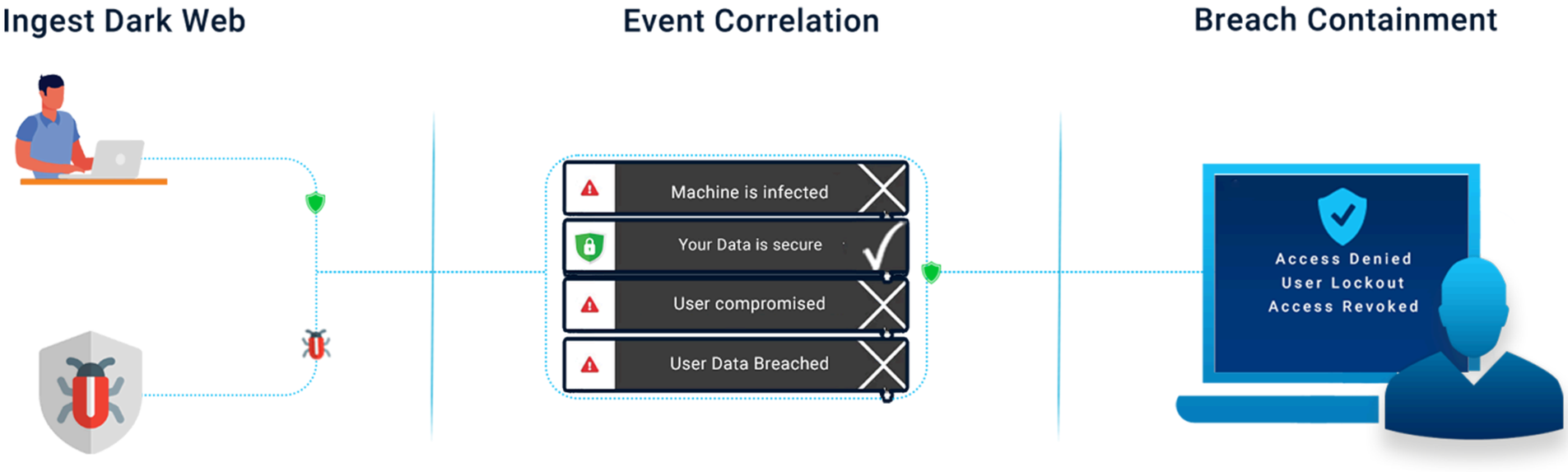
Dark Web service acts as a "buddy" to the security team by providing real-time dark web exposure alerts and helping the team take timely preventive and corrective actions accurately. It helps the team by:

- Ingesting Dark Web data into already deployed solutions such as Active Directory and SIEM, to provide a more comprehensive view of the company's security posture.

- Correlating Dark Web data with logs to identify breached users and infrastructures, which helps the team to take appropriate actions to mitigate the risk.
- Assisting Red Team in threat hunting, which provides more insight into the company's existing threat landscape and enables the team to identify potential threats before they become actual breaches.
- Implementing preventive measures to safeguard the user accounts by flagging the compromised accounts, thus reducing the risk of further breaches.
- Providing monthly reports to C-level executives to safeguard critical information, and make sure that they are aware of the company's security posture.
- Recommending steps along with the triage reports, which help the team to take appropriate actions to mitigate the risk.

DARK WEB MONITORING SERVICE PROCESS

Dark Web service helps the security team to take more informed decisions, and reduce the risk of breaches by providing real-time dark web exposure alerts and necessary information about the compromise.



DARK WEB SERVICE COMPONENTS

Dark Web Monitoring service provides you with the information available on the dark web about your company and employees before it reaches the hands of cybercriminals. By providing you with this information, the service helps you take timely action on compromised accounts, assets, and employee PII before it is compromised.

The service puts all the information together to provide a clear and comprehensive view of the compromise.

The SOC Analyst Triaged Tickets components for each Dark Web Security Alert include:

- Corporate Domains Monitoring: Monitoring of your company's domains to detect any suspicious or unauthorized activity.
- Corporate Email Account Monitoring: Monitoring of your company's email accounts to detect any suspicious or unauthorized activity.
- Exposed Active Session Cookies: Detection of any exposed session cookies, which can be used to gain unauthorized access to an account.
- Exposed SSO Session Hijacking: Detection of any exposed SSO sessions, which can be hijacked to gain unauthorized access to an account.

- Breached IPs: Detection of any IP addresses that have been compromised.
- Breached From Geolocations: Detection of the geolocation of any compromised IP addresses.
- Breached Infected Machine IDs: Detection of any infected machine IDs that have been compromised.
- Breached Corporate Username/Passwords: Detection of any compromised corporate usernames and passwords.
- Breached Employee PII - Phone-numbers: Detection of any compromised employee personal information such as phone numbers.
- Breached Employee PII - Social Handles: Detection of any compromised employee social media handles.
- Breached Employee PII - National-IDs: Detection of any compromised employee national IDs.
- Breached Employee PII - Social-Security-Numbers: Detection of any compromised employee Social
- Security Numbers.
- Breached Employee PII - Passport-Numbers: Detection of any compromised employee passport numbers.
- Breached Employee PII - Driver-Licenses: Detection of any compromised employee driver licenses.

CONTACT US

CONTACT US NOW!

+61 2 9416 0416

sales@sgen.com.au

www.sgen.com.au