SILENT BREACH INC.

INCIDENT RESPONSE RETAINER & PRO-ACTIVE MONITORING

Background

Computer security incident handling and pro-active monitoring can be interpreted in many ways by other cyber security companies, sometimes misleading the customer in thinking they are safe in case of an incident. Our approach to cyber security includes preventive measures, instead of merely offering curative solutions, we follow well established standards in Europe and North America. Silent Breach Inc. follows the NIST 800-53 framework for incident response, which includes as a subset the NIST Cybersecurity Framework and ISO 27002 standards.

Continuous monitoring

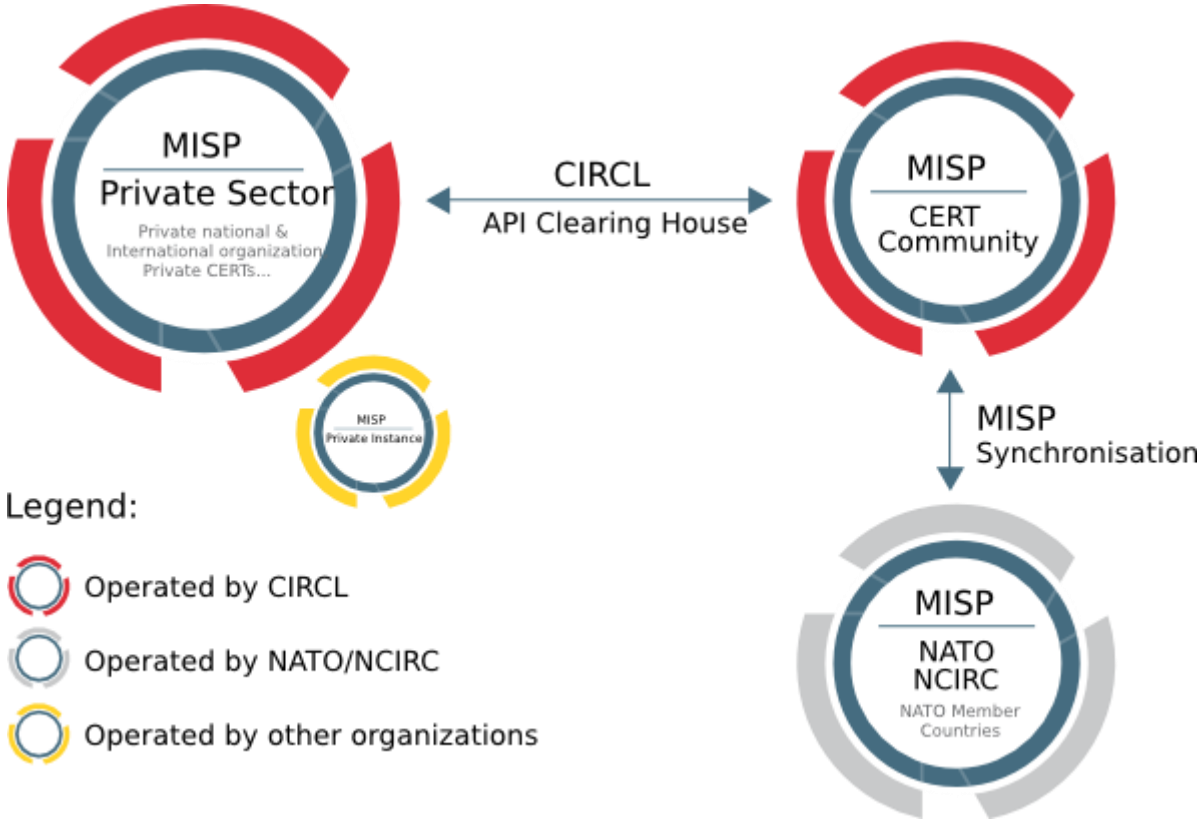
Following a Business Impact Analysis (BIA) and Risk Assessment (RA), our team will model the different threats your company might face and as a result, prioritize the continuous monitoring of your digital assets. The methodology follows the NIST standard:

1. Categorize information systems.
2. Select security controls.
3. Implement security controls.
4. Assess security controls.
5. Authorize information systems.
6. Monitor security state.

Our automated external agents can monitor controls from outside your peripheral network in a non-intrusive way, on a daily basis to spot any change in attack surface, and take into consideration any newly discovered threats.

NATO backed Incident Response Center

In cooperation with the CIRCL, the Computer Incident Response Center that shares its database with the NATO international organization, Silent Breach offer near real-time notifications of any new threats that appear on the internet and identified as serious by the North Atlantic Alliance.



By subscribing to our Incident Response Retainer program, you will receive notifications on new threats in near-real time, by email or RSS feed.

SILENT BREACH INC.

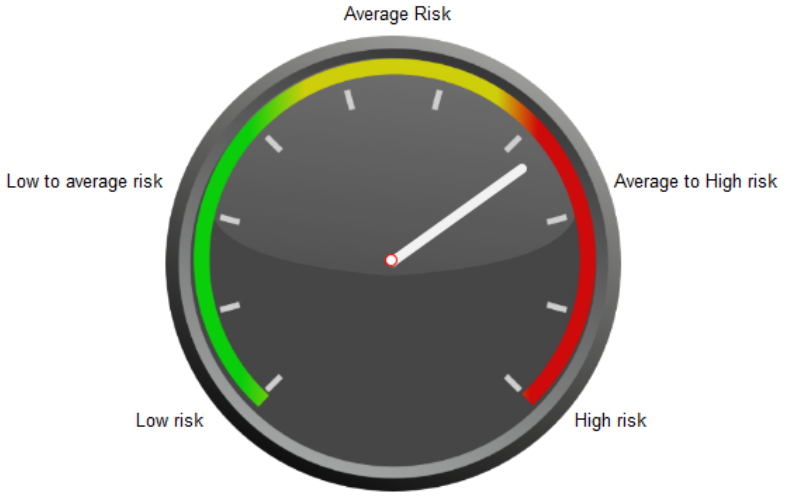
Network Penetration testing

Automated monitoring is not always enough to evaluate and harden your network perimeter, manual penetration testing is necessary to cover as much ground as possible and help prevent security incidents.

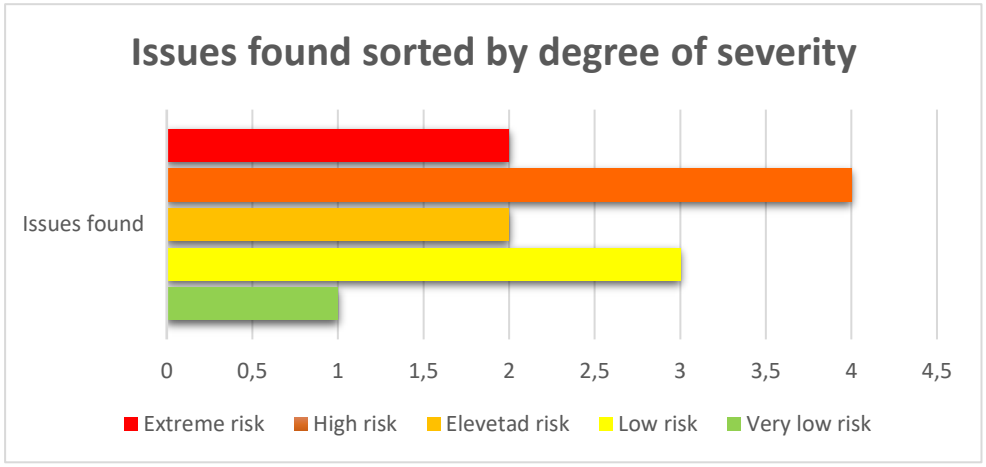
Clear and straightforward reports.

Gathering data and metrics on your security posture does not help if you don't understand the report. Silent Breach offers a 'Risk indicator' to sum up in one diagram your security posture, so that the key information is clear and straightforward.

With executive summaries and diagrams, non-technical personnel can easily navigate the report even without any technical background.



Prioritize resolutions.



Security issues are sorted to help you prioritize the patching effort. Color coded bar graph make it easier to visualize the risks, and quantify the effort.

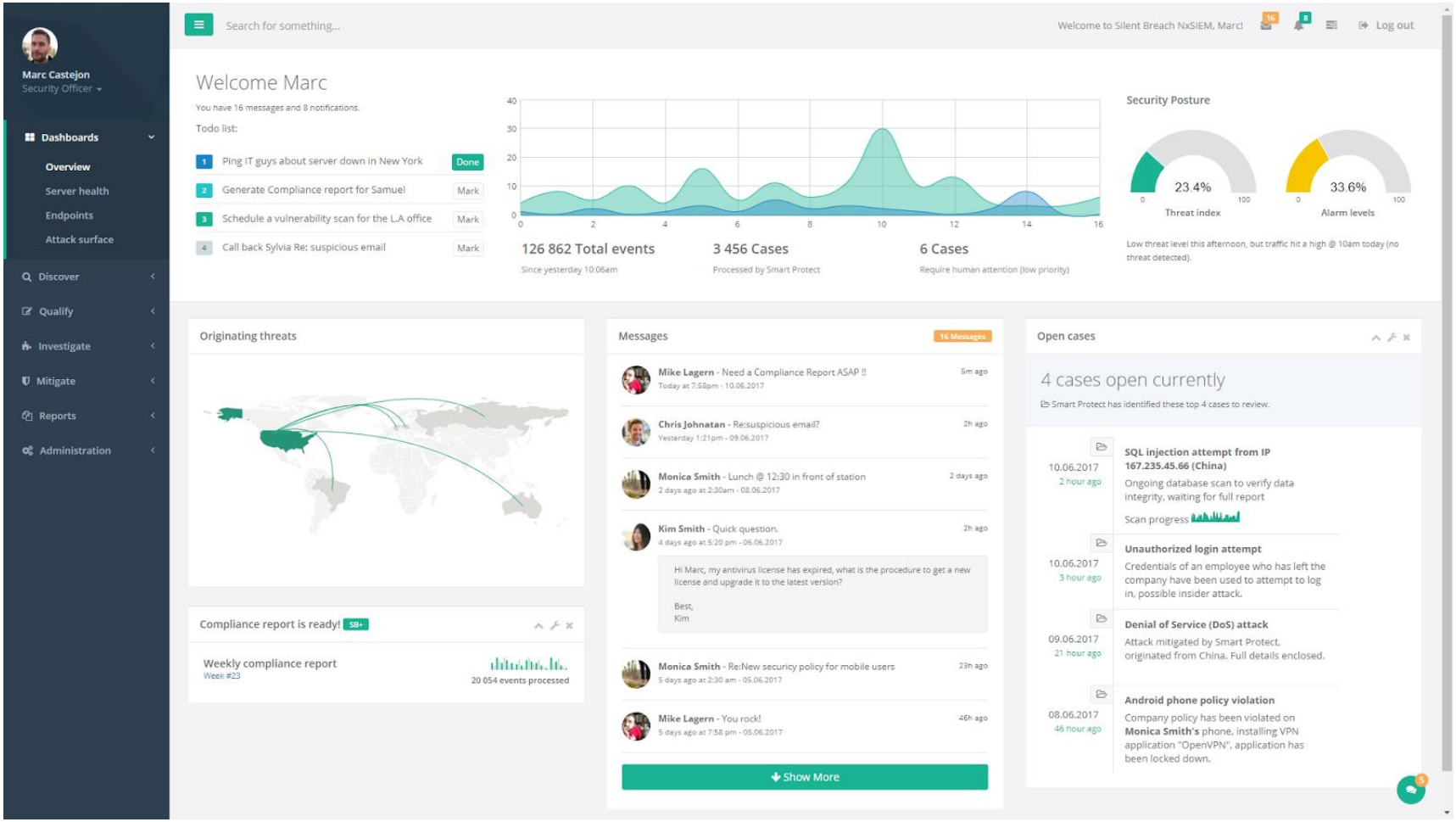
ROOTKIT AND BACKDOOR DETECTION

Periodic system sanity check allows to determine if a data breach has gone undetected or is the work of an insider. This manual or automatic swipe is recommend on all critical systems on a periodic basis and is included in the price of Tier 2 and Tier 3 packages (Optional for Tier 1).

SILENT BREACH INC.

Agent based pro-active perimeter monitoring

Silent Breach's unique agent based technology combines network traffic monitoring and honeypot deceptive approaches to predict breaches before they occur or stop them in real-time. Our NxSIEM product offers unique insights in the security posture of the company, during live attacks and actual attempts to break in.

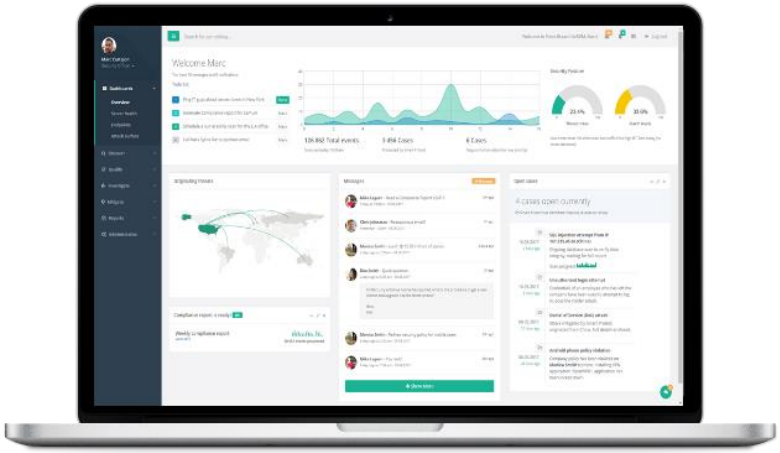


SILENT BREACH INC.

SOC Engineering support (NxSIEM SaaS)

Our Nx-SIEM can be operated by the customer or driven from one of our North American Security Operating Centers (SOC). Our engineering team will run NxSIEM from our cloud so that all the real-time detection is provided to you worry-free.

Our experienced engineers are available 24/7/365 to support you in both the Saas and on-premise deployments of our real-time NxSIEM monitoring tool.



Why choose Silent Breach Inc.?

If you have been in business long enough, then you probably already know that it is not *if* you will be compromised, it's *when*. How well you can detect an attack and how fast you can respond is key to protecting your company from a breach. Companies are compromised on a daily basis, resulting in direct financial losses, eroding customer loyalty, harming company's reputation and sometimes triggering significant fines and penalties.

Silent Breach Inc. prides itself in having the best red team on the market, with world class security officers that are ready to serve you 24/7/365. With crystal clear reports for high level executives and very detailed testing procedures for the IT teams, our documentation is very appreciated from our customers and we strive to deliver a level of service that exceeds your expectations. Many US companies have trusted us with their security needs, including to date: Walmart, Bank of America, HSBC, the Hilton group, Aetna, AT&T, etc…

Our incident response offer is based on a simple idea that an ounce of prevention is worth a pound of cure. And we apply this in our incident response approach by offering different levels of pro-active prevention, to catch vulnerabilities before they are exploited.

SILENT BREACH INC.

TIER	TIER 1 – BRONZE	TIER 2 – SILVER	TIER 3 - GOLD
FREE SETUP COST	Yes	Yes	Yes
NATO BACKED INCIDENT NOTIFICATION SYSTEM	Yes	Yes	Yes
PAY-AS-YOU-GO INCIDENT REPONSE SUPPORT HOURS	Yes	-	-
PRE-PAID INCIDENT RESPONSE SUPPORT HOURS (50% DISCOUNT)	-	40h/year	120h/year
SETUP VULNERABILITY ASSESSMENT AND PERIMETER HARDENING	(optional)	Yes	Yes
CONTINOUS NETWORK MONITORING	(optional)	Yes	Yes
PERIODIC PENETRATION TEST	(optional)	Bi-annually	Quartely
ROOTKIT AND BACKDOOR DETECTION	(optional)	Quaterly (manual)	Daily (automatic)
SLA REMOTE	Best effort	24h	8h
ON-SITE SUPPORT	(optional)	(optional)	48h
AGENT BASED REALTIME DEVICE MONITING	-	(optional)	Yes
SECURITY OPERATING CENTER ENGINEERING SUPPORT (SAAS)	-	-	Yes
COST	Contact Us	Contact Us	Contact Us

*These costs are expressed in USD, and exclude sales tax. Additional hours are billed $300/h. Late fees apply after 30 days.