Vigilocity | Cyber Opportunity
Confirming Material Breach Through Threat Actor Infrastructure Disruption
https://www.vigilocity.com/

- Confirmed evidence of breach (hack) before the victim or anyone else knows.
- Zero software, hardware or configuration changes needed by the customer.
- First party and third-party (supply-chain) continuous breach monitoring.
- The first cyber actuarial modeling data set for cyber insurance companies to use with their existing policy holders as well as potential policyholders.
- Confirmed understanding if security controls/investments are working as advertised.
- Pre-cognitive understanding of threat actor intent and proactive prevention of breach/ransomware.

Value Proposition:

- Next generation platform that automatically identifies, surveils, and remediates malicious implants before victims are even aware of breach.
- No hardware, software, or installation requirement of any kind.
- Utilization of advanced machine learning models to predict and preempt sophisticated threat actor attacks. (Cybersecurity use cases)
- Revolutionary supply-chain and third-party risk mitigation. (Cyber insurance and M&A use cases)

Core Use Cases:

- Cyber Insurance: A zero-touch ability to identify confirmed compromise and breach of existing policy holders as well as potential policy holders rather than merely delivering vulnerability and survey compilations and scoring.
- Supply-chain Contagion Mitigation: A holistic view of the breach status of not only first-party organizations, but also their supply chain and third-party partner ecosystem again with no hardware, software or configuration changes required.
- Pre-cognitive Intelligence: Early identification of first stage infections allowing the incident response teams to rapidly act and mitigate a breach before it gains a foothold.
- Global Threat Context & Decision Support: Global visibility of infrastructure including on-premises, cloud, IoT/OT, and mobile.The technology is device agnostic and provides high fidelity threat context and materiality of breach delivering powerful decision support.

Opportunity:

Vigilocity exhibits considerable potential for substantial returns on investment. Notably, one of its initial clients is a Fortune 10 company boasting a vast supply chain of 600,000 entities. Envisaging an annual charge of $50,000 per company within this supply chain yields a potential revenue of $30 billion. Even a conservative estimate, capturing 10% of this clientele, would generate $3 billion. The ripple effect of

these companies engaging with their own suppliers could further amplify these figures. It is crucial to note that this scenario involves just one corporation.

Projections:

Projections indicate that operational monitoring costs for this endeavor would amount to a modest $3 million annually, alongside additional administrative expenses. The proposed joint venture holding company, currently under development, includes a supplementary business with a team of 30 cybersecurity experts addressing cyber threats. Notably, this individual has previously set up the cyber training infrastructure for the FBI and maintains close ties with defense contractors, presenting additional opportunities.

Structure:

The contemplated investment structure involves a total capital injection of $200 million. Of this, $180 million is earmarked for the purchase of Vigilocity and $20 million as working capital spanning two years. The latter would serve to sustain cash flow for potential acquisitions or the incubation of other enterprises.

Share/Ownership Allocation:

Upon the infusion of initial funds and disbursements, ownership would follow an allocation of 1/3 to each of the involved parties: the chosen investor, my partner and me, and Karim Hijazi, who contributes his company's technology and software. A pivotal aspect of understanding this initiative involves a detailed Zoom call, offering real-time demonstrations of cyber-attacks, the subsequent AI-generated insights, and the strategic process for remediation. It is emphasized that this information is pivotal for companies to address and rectify cyber threats promptly, thereby mitigating potential costs in the millions.

Confidentiality and Timeline:

It is imperative to treat this information with utmost confidentiality. Further details, including financials, will only be disclosed upon the execution of a Non-Disclosure Agreement (NDA) and the formalization of the deal structure. While the current valuation stands at $200 million, swift action is encouraged to secure this investment, with proof of funds, a Letter of Intent (LOI), and a lockup agreement facilitating due diligence.

My partner and I have diligently been establishing the corporate framework and LOI structure, engaging top intellectual property attorneys to ensure the robustness of the venture. The anticipated revenue figures for this enterprise are remarkable, grounded in a sound methodology. Additionally, prospective collaborations with industry leaders such as Cisco, Deloitte, Live Nation, and others are being explored, adding further layers of potential growth and diversification to this venture.

Alexander Grikitis
Founder / CEO of Grikitis Group
https://grikitisgroup.com/