QUANN PROTECT

QUANN DETECTION BY DECEPTION

Outsmarting attackers with an alternate reality network environment

Cyber breaches are inevitable in today's highly connected world. Threat actors are smart and persistent and if an attack fails they will try again until they succeed. Businesses are also vulnerable to threats from within, which may be attributed to insider attacks or human error.

Detecting and mitigating these threats is no easy task, with networks becoming increasingly complicated and exhibiting all kinds of anomalies that could trigger real or false alarms. At the same time, sophisticated attackers could be operating in a "low-and-slow" way that mimics normal network behaviour and thus go unnoticed.

With these new developments in the threat landscape, businesses will have to protect themselves by going on the offensive. One way to do this is to create an alternate reality environment that is able to detect threats continuously in real time and outsmart the attackers without affecting the network.

QUANN DETECTION BY DECEPTION

Quann Detection by Deception solution presents attackers with a falsified view of the business network environment which tricks them into believing that what they are seeing is valid. Attacks are foiled because without reliable data, threat actors will not be able to make decisions.

Quann helps businesses design a complex deception architecture which incorporates deception technologies to divert illegal attempts at accessing the network. Once an attack is detected, Quann gathers information about the attackers' ongoing activities without being noticed, carries out forensic analysis and helps businesses to put remediation measures in place. This provides businesses with effective safeguards against targeted and advanced attacks such as zero-days as well as insider threats.

FEATURES

A deceptive alternate reality

- A deceptive layer is created across the entire network covering every endpoint, server and network component.
- Attackers are presented with an alternate world with false data about the network environment.
- The deceptive layer can be changed constantly to reflect the dynamic nature of actual networks.
- Attacks are paralysed by the bombardment of fake or false data.

Reliable alerts and real-time forensics

- There are no false positives because real users will not wander into the alternate reality created by deception technologies.
- Attackers can be detected instantly when they act on the false information.
- Real-time forensic analysis is carried out based on information that is collected when the attackers act on false data.

Stealthy deployment

- Deception traps are set remotely without introducing any agents into the system and with no disruption to the business.
- The deceptive layer can be deployed without anyone knowing and cannot be seen by internal users, including those managing the business' IT function.
- The stealthy deployment helps mitigate insider threats.

Scalable

- The solution platform is highly scalable and can be seamlessly integrated with existing security products.
- It can be deployed in the user networks and data centres across private, public and hybrid cloud environments to deliver "deception anywhere".

BENEFITS

Boosts end-to-end security from detection to remediation

Quann helps businesses design a complex deception architecture which tricks and paralyses threat actors by creating a falsified view of the business network and bombarding them with fake data. We also provide forensic analysis and help businesses put remediation measures in place.

Enhances the protection of real assets

The deception approach presents attackers with attractive fake targets, diverting threats from actual systems which may hold critical data. At the same time, actionable breach reports provide real-time forensics information that is needed to contain the attack.

Increases the productivity and effectiveness of enterprise IT and cyber security teams

Cyber security teams can operate more effectively as they no longer have to expend valuable time and resources dealing with false positives.

QUANN
THE ART AND SCIENCE OF BEING CYBER SECURE

For more information, please contact us at **info@quannsecurity.com**
or visit our website at **quannsecurity.com**