No.1
July 2021

Cyber Startup Briefing

HardenStance: Trusted research, analysis & insight in IT & telecom security

#1 Noetic Cyber (Boston, USA)

Sponsored by Noetic Cyber

- **Market Space**: Cyber Asset Management and Continuous Controls Monitoring.
- **Secret Sauce:** A declarative and extensible type system with easily customizable correlation logic (patents applied for); temporal graph technology to represent relationships between assets the way attackers view them; automation of policy-driven changes to close compliance deviations and improve security posture.
- **Competitors:** Panaseer, Galvanize, Axonius, Qualys.

The maturity of an organization's cyber security posture depends heavily on how effectively and dynamically security controls can be adjusted and mapped to changes in the threat surface.

Continuous, Automated, Protection of Assets

One of the most fundamental of all cybersecurity challenges is to identify all of the assets an organization has on premises and in the cloud; try and understand the highly complex matrix of relationships between those assets; and then somehow extract from that great morass of data an accurate view of exactly what that matrix of assets and relationships implies – at an individual and aggregate level – for the organization's threat surface.

The maturity of an organization's cyber security posture depends heavily on how granular the understanding of its threat surfaces is - and how dynamically security controls can be adjusted to respond to changes in that threat surface. And vice versa – how relationships between assets can be adjusted to reflect changes in security controls. The tighter the synchronization between the cyber security status of assets and cyber security controls, the stronger an organization's cyber security posture can be.

This is the market space being targeted by new Boston-based start-up, Noetic Cyber, whose founders also started Resilient Systems, the original first mover in the Security Orchestration Automation and Response (SOAR) market. The name is taken from the Greek 'noēsis', meaning inner wisdom, direct knowing, intuition, or implicit understanding. Where SOAR brings visibility, orchestration and automation to the threat detection and response pillars of NIST's cyber security framework, Noetic brings it to

Noetic's Team of Experienced, Not to Mention 'Resilient', Founders

Noetic Cyber emerges from stealth on July 28th, following 18 months of product development and market validation, working with design partners in the U.S. and Europe. Noetic is targeting the cyber asset management and continuous controls monitoring market (CCM) spaces. The three founders – CEO, Paul Ayers; Chief Product Officer, Allen Rogers; and Chief Architect, Allen Hadden – were all early employees of Resilient Systems Inc, first mover in the SOAR market, that was sold to IBM in 2016.

Headquartered in Boston, Noetic also has full time staff in the UK. TenEleven Ventures, Glasswing Ventures and RAZI Ventures provided initial seed funding and a Series A funding round closed recently. Niloofar Razi Howe, ex Chief Strategy Officer of RSA is on the Advisory Board, alongside other industry leaders such as Nicholas Warner, COO, Sentinel One, and Jim Reavis, CEO, Cloud Security Alliance.

the protection pillar. Where SOAR platforms help security operations be more efficient at fighting fires, Noetic seeks to prevent fires from breaking out in the first place.

Straddling the Cyber Asset Management and Continuous Controls Monitoring (CCM) product spaces, Noetic's core platform runs on any Kubernetes 1.18 cluster. It's available as a SaaS offering or it can run on public or private clouds. As depicted in **Figure 2**, the company's core value proposition is what it describes as the 'Noetic Loop'. This entails continuous monitoring of assets and asset relationships against the desired state prescribed by the organization. This is complemented by automated actions to assure continuous alignment.

Unlike a lot of asset management systems, Noetic doesn't just ingest data from compute assets. Via a portfolio of API connectors that leverage the OpenAPI Initiative's OpenAPI Specification, Noetic also plugs into a wide variety of security, IT management tools and business applications. These include, but are not limited to, a variety of public clouds; vulnerability scanners; log scanning infrastructure; endpoint products; network infrastructure; identity management systems; and Configuration Management Databases (CMDBs).

Noetic spots changes that indicate drift from the desired end state. It then triggers automated policy validation and remediation to ensure that any change in the environment aligns – or is made to align - with the desired end state.

Unlike a lot of asset management systems, Noetic doesn't just ingest data from compute assets.

A Declarative, Hierarchical Type System for Ingesting Data

A lot of available tools already make key contributions to defining exactly what it is an organization is trying to defend against. However they tend to provide visibility into silos rather than the more universal perspective that security teams need. Vulnerability scanners are important, but they can't tell you which of your assets are not currently covered by vulnerability scans. Similarly, Endpoint Detection and Response (EDR) or XDR platforms are important. However, they can't tell you which of your organization's endpoints aren't supporting their client or which don't have a correctly configured client.

Without having to add new endpoints or sensors, the Noetic platform continuously monitors a variety of information sources that are already in the environment and looks for three core change categories. These are:

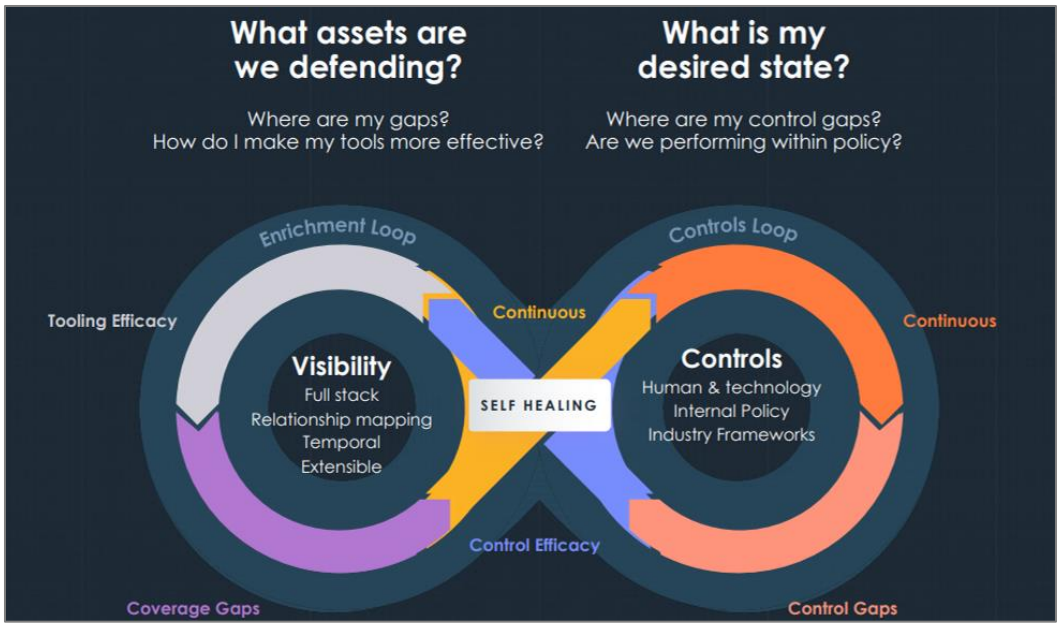
- new entities that appear (or seem to appear);
- entities that disappear (or seem to disappear);
- new relationships between entities.

At its core, the Noetic platform is a generic entity ingestion and correlation engine driven by an extensible type schema that is targeted at cybersecurity use cases. This allows users to quickly adapt and extend the platform to encompass new use cases, data sources or entity types. The closest you can typically get to something like that today is to pull data from a variety of different key platforms like your public cloud, EDR products, and CMDB or IT Service Management (ITSM) platforms, and then run some correlation algorithms across them.

Use of OSCAL and STIX

To support CCM, the platform uses the NIST-developed Open Security Controls Assessment Language (OSCAL). It uses the Structured Threat Information Exchange (STIX) standard to describe common observables like IP addresses and threat indicators for consistency between tools.

Figure 2: Noetic's Value Proposition is a Continuous Self-Healing Loop



Source: Noetic Cyber

Temporal Graph Technology

Noetic builds and adjusts temporal graphs of the environment according to the above three change categories and brings that visual representation to security teams. It was Microsoft's John Lambert who coined the term "defenders think in lists, attackers think in graphs" in a blog back in 2015. Six years on there's still a lot of truth in it.

The risk associated with being driven by asset lists is that they tend to be exhaustive, hence overwhelming.

Having executed an initial breach somewhere in the target network, attackers routinely use visualization tools to create graphs showing the relationship between assets in the network they've established a bridgehead in. That graph provides a multi-dimensional, representation of the set of security dependencies in the design of that network, the behaviours of users, and the types and versions of software and services in that network. These are necessarily created in the course of their day to day software development and deployment lifecycles by the organization's own developers.

Creating and using these graphs helps attackers discover the potential paths between assets and look for weaknesses. This can help them move laterally between assets very efficiently, until they are able to reach their target endpoint or endpoints.

The same tools that attackers use for creating graphs are available to security engineers but consistent with John Lambert's dictum, many of them still aren't using them today. Defenders still tend to prefer to leverage lists of assets. These originated in IT business operations and morphed into cyber security tools where they are still widely used as the basis for prioritizing fixing vulnerabilities. Asset lists continue to be popular for a number of reasons. In some cases it's because they're easier for some people to generate than graphs. Any number of security audit tools will provide long lists of vulnerabilities so a mindset can also develop that says 'there's plenty to be getting on with here without going to the trouble of generating additional graphs'.

The Problem with Asset Lists

The risk associated with being driven by asset lists is that they tend to be exhaustive, hence overwhelming. Unlike graphs, asset lists are also pretty one-dimensional. Basic asset lists will only point to huge numbers of vulnerabilities in servers, for example, although some will provide some level of a prioritization.

Where the value of graphs kicks in is that they can tell you whether a vulnerable server is Internet-facing or not or whether a system that has a vulnerability is accessing a specific data store. Acting on additional context in that way can be pivotal in focussing resources on the most critical weaknesses to harden cyber security posture. A core failing of traditional asset list approaches is therefore that they tend to be a bottom-up, technology-centric, perspective on cybersecurity rather than a top down, risk based approach driven by what business leaders care about most.

Embedded Temporal Graph Technology

Noetic has incorporated temporal graph technology in its platform to provide defenders with the same view of relationships and dependencies that attackers use. This also serves to align the bottom-up perspective of the security team with the top-down perspective of the business. Importantly, the graphic tools in Noetic's environment offer more value than using dedicated tools for the same purpose, and not just because of the integration with the platform's type system and automation engine.

As well as shipping with an initial suite of queries out of the box, Noetic's embedded graphic tooling also supports advanced querying features to request specific information from the platform. Examples include what systems are not currently being subjected to vulnerability scanning or what systems on production networks are accessing a specific type of Personally Identifiable Information (PII).

Because the graph is temporal, queries can be historical – e.g. "what did this graph look like three months ago when an attacker first infiltrated my environment?" As well as in day to day cyber security operations, this has value for compliance audits in terms of demonstrating how compliance has evolved over time as well as showing current status.

Due to its extensible open architecture, in a future release, customers will be able to write their own apps to run on Noetic.

Automation of Policy-Driven Changes

Noetic orchestrates and automates workflows within the environment in the background to continuously update the graph and fix weaknesses. This is the end goal of modern cyber security in terms of alleviating menial but important tasks from the security team. Queries and any associated remediations can be undertaken as one-offs. Alternatively they can be scheduled to run automatically so that security policy is implemented as code in the form of queries against the graph.

Due to its extensible open architecture, in a future release, customers will be able to write their own apps to extend and exploit the capabilities of the Noetic graph. Meantime the first release supports the company's own initial suite of applications. The following are a couple of key examples of the types of queries that can be run against new entities discovered in the environment:

- If it's not clear what the entity's configuration is, Noetic can run a workflow to discover its' IP address and what ports are open. That information doesn't get acted on immediately, but it gets tucked away for context.
- If it identifies common cloud misconfiguration issues, such as unencrypted storage volumes, it can trigger the remediation.
- If it identifies breaches of a common policy, such as all machines with access to PII must have an EDR agent deployed, it can trigger the enrolment and deployment of the endpoint agent.

With Noetic's first release, customers create their own policy definitions. In the near future the platform will also support industry standard frameworks like CIS and NIST.

More Information

- www.noeticcyber.com
- HardenStance Briefing: "New STIX and TAXII Releases Approved" (April 2020)

- HardenStance Principal Analyst: patrick.donegan@hardenstance.com
- Register for free email notifications whenever HardenStance publishes new content.

About HardenStance

HardenStance provides trusted research, analysis and insight in IT and telecom security. HardenStance is a leader in custom cyber security research and leading publisher of cyber security reports. HardenStance is also a strong advocate of industry collaboration in cyber security. HardenStance openly supports the work of key industry associations, organizations and SDOs including NetSecOPEN, AMTSO, The Cyber Threat Alliance, The GSM Association, OASIS, and ETSI. www.hardenstance.com

HardenStance Disclaimer

HardenStance Ltd has used its best efforts in collecting and preparing this report. HardenStance Ltd does not warrant the accuracy, completeness, currentness, non-infringement, merchantability or fitness for a particular purpose of any material covered by this report.

HardenStance Ltd shall not be liable for losses or injury caused in whole or part by HardenStance Ltd's negligence or by contingencies beyond HardenStance Ltd's control in compiling, preparing or disseminating this report, or for any decision made or action taken by user of this report in reliance on such information, or for any consequential, special, indirect or similar damages (including lost profits), even if HardenStance Ltd was advised of the possibility of the same.

The user of this report agrees that there is zero liability of HardenStance Ltd and its employees arising out of any kind of legal claim (whether in contract, tort or otherwise) arising in relation to the contents of this report.