

FROM A REACTIVE SECURITY TO PROACTIVE HUNTING

*– Endpoint & Intelligence the new security
pillars*

Evolving Challenges

Macro trends imply a shifting and complex environment for enterprise security teams

**New surface,
new usage to monitor and protect**



+

**Lack of qualified
talent, Retention**



+

**Increasing number
of sources creating
huge volumes of data**



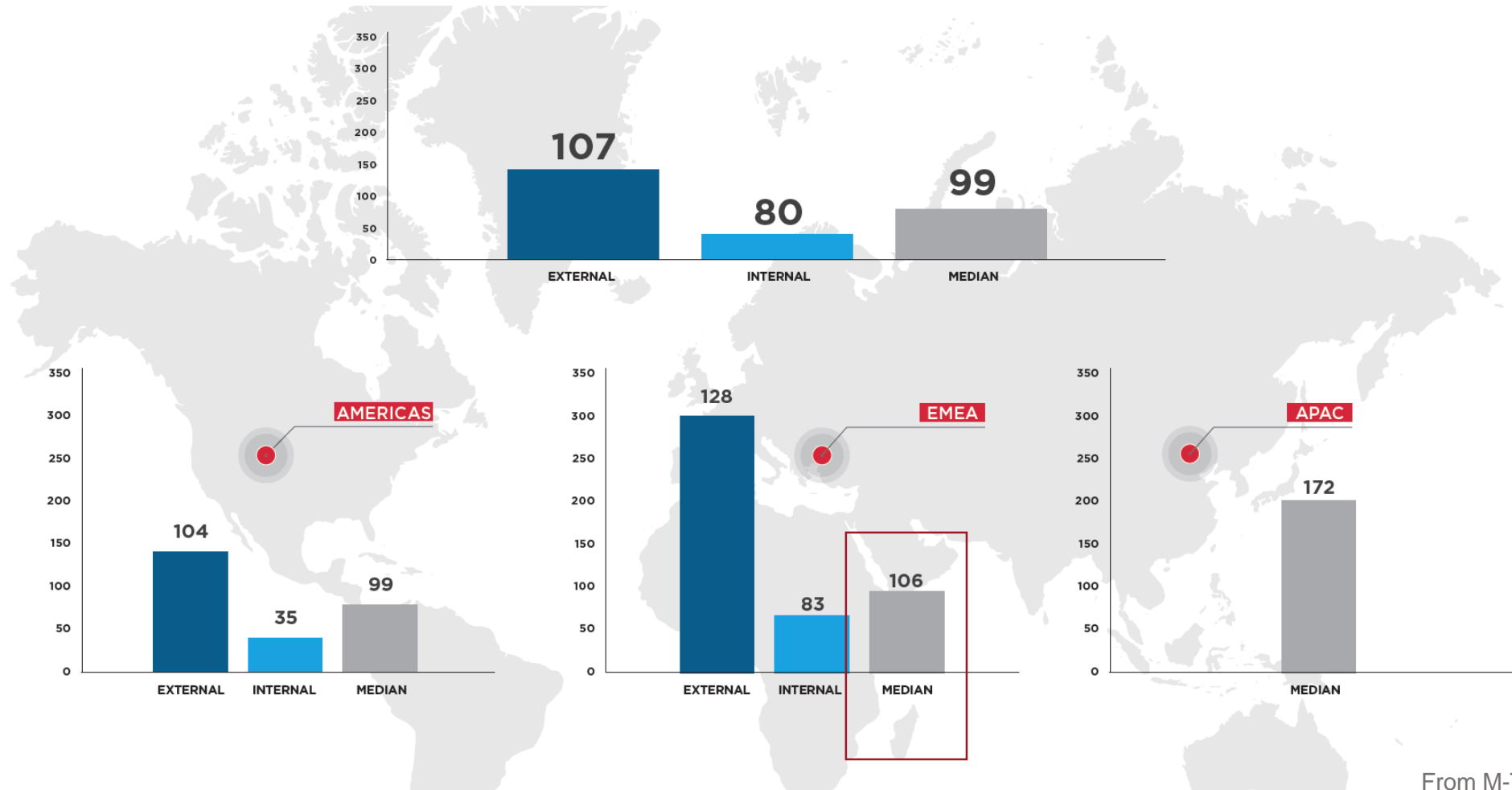
+

**Rapid threat evolution
creating complex and
diverse threats**



As a result

Dwell time is too long ...



OUR ANSWERS:

How to reduce DWELL time ?

Intelligence – to focus & prioritize

Endpoint – to validate & react

Orchestration - to speed up reaction

A photograph of American football players in a three-point stance on a grass field. The players are wearing blue jerseys with orange numbers and white helmets. The image is partially obscured by a dark, semi-transparent overlay on the right side. The text "GIVING THE ADVANTAGE BACK TO THE DEFENDERS - INTELLIGENCE" is written in white, uppercase letters on the left side of the image.

GIVING THE ADVANTAGE BACK
TO THE DEFENDERS - INTELLIGENCE

INTELLIGENCE

SOME NUMBERS

250 Analysts

19 countries, 29 languages

100 Millions invested

17 000 groups

Greek Hacktivist Group HellSec Starts New #OpIcarus Campaign; Poses Very Low Threat to Financial Entities

16-00011722 HK

July 29, 2016 03:05:00 PM ,Version:1

Indicators Analyst Access PDF Print

EXECUTIVE SUMMARY

On July 28, 2016, the Greek hacktivist group HellSec announced a new wave of the anti-financial #OpIcarus campaign. We judge that it poses a very low threat to financial entities and believe that it has no ties to the original #OpIcarus campaign.

KEY POINTS

DETAILS

TECHNICAL

- On July 28, 2016, the hacktivist group HellSec claimed to start a new wave of the anti-financial campaign #OpIcarus. FireEye iSIGHT Intelligence judges that it poses a very low threat to financial institutions.
- We assess with moderate confidence that this version of the campaign is a copycat campaign that maintains no affiliation with the original #OpIcarus campaign.

Industry Brief: Finance

16-00013832 EN

September 13, 2016 08:29:00 PM ,Version:2

Indicators Analyst Access PDF Print

EXECUTIVE SUMMARY

- Cyber espionage is a significant threat to finance.** The finance industry has seen a much higher than average use of watering holes (i.e., compromised third-party websites trusted by members of the finance industry) that attackers use to deliver malware and profile targets while appearing to deliver legitimate traffic. Most activity targeting the sector is likely Chinese and motivated by supporting key industries for economic advantage. However, Iran also targets the West and Middle East to gain leverage in its geopolitical conflicts. Additionally, Russia targets the West for data theft, probably to support intelligence targeting or to prepare for attacks on the finance industry as part of political conflicts, rather than for financial gain, and North Korea routinely targets South Korea for strategic asset compromise.
- Cyber crime is the greatest threat to finance.** Victims include a wide range of organizations including banks, investment services, and insurance companies. Developing trends in cyber crime include increases in attempted and successful exploitations of banks' client-side Society for Worldwide Interbank Financial Telecommunication (SWIFT) connections; exploitation of the Europay, MasterCard, and Visa (EMV) chip protocol; use of mobile malware to bypass multi-factor authentication; and continuing actor interest in ATM

ThreatScope®



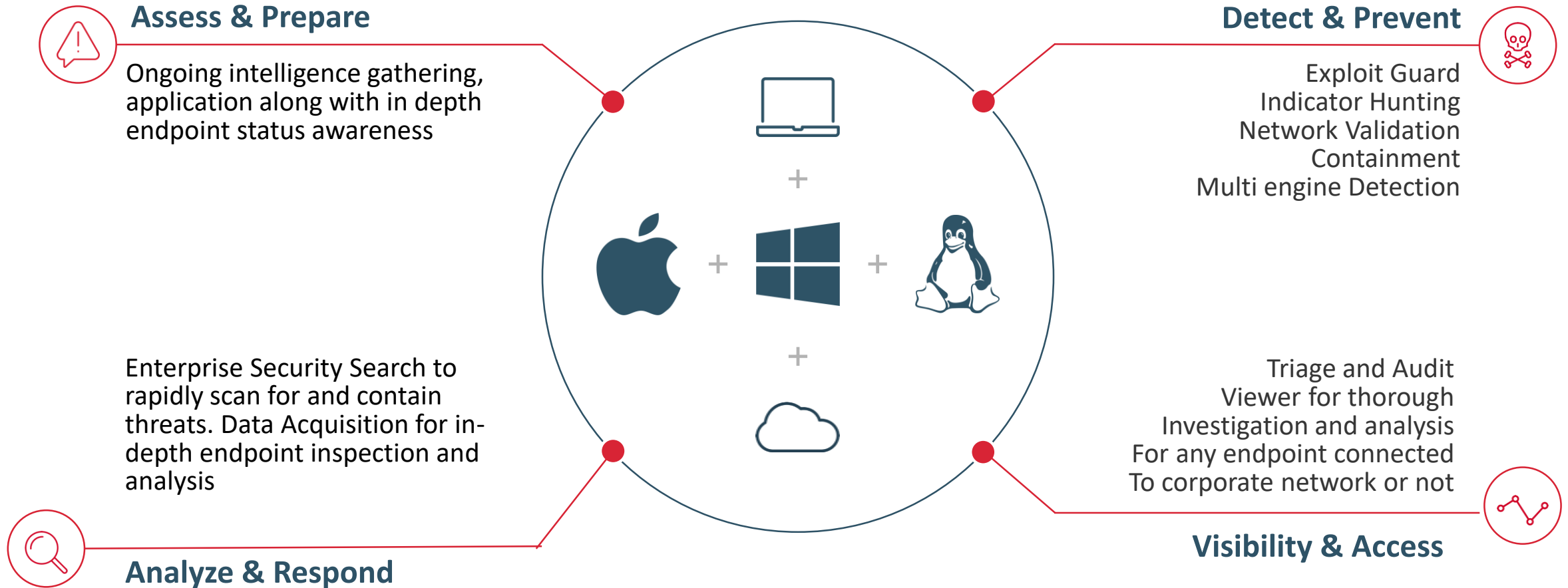
API

FORENSICS AS A BEHAVIOR

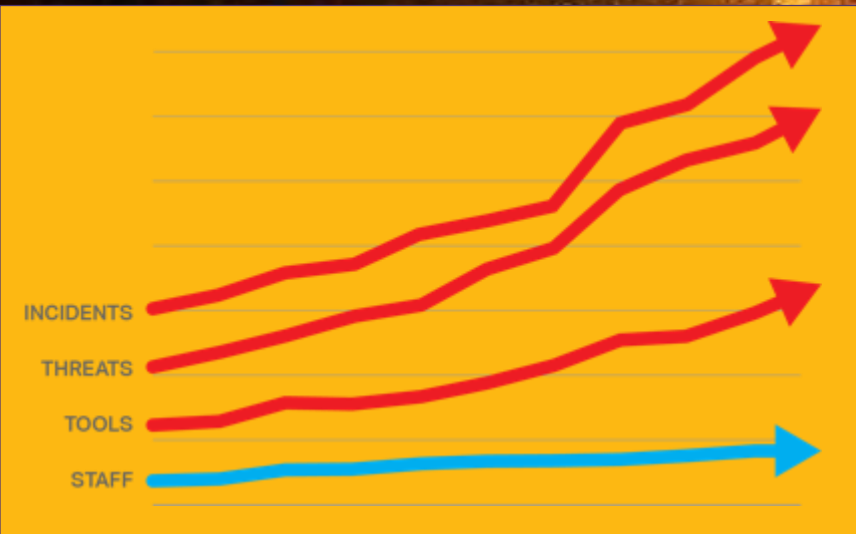


ENDPOINT

Endpoint Security Overview

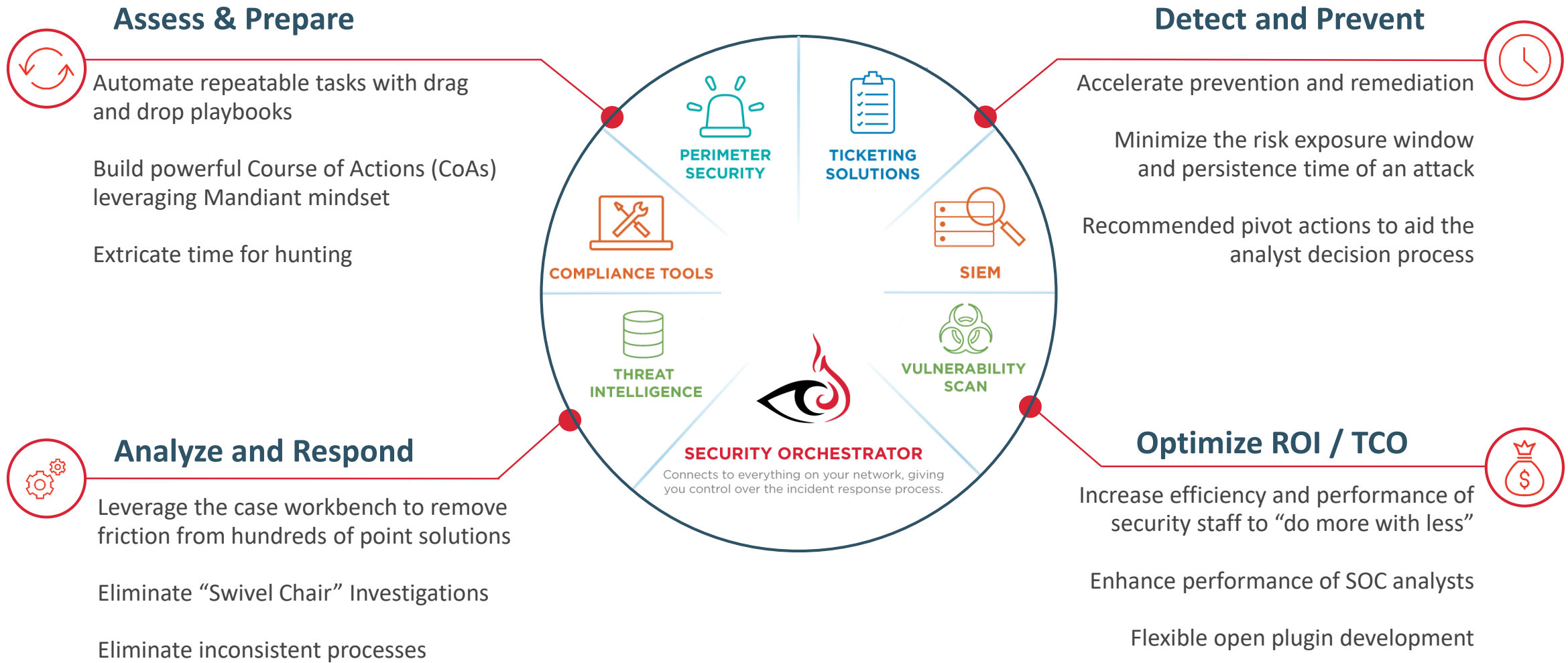


AUTOMATION -- OPTIMIZATION



ORCHESTRATION

FireEye Security Orchestrator



OUR MISSION:

To relentlessly protect our customers with
innovative technology
and expertise
learned on the front lines

UNIQUE TRIPLE THREAT ECOSYSTEM



HELIX- THE ANSWER

Increase expertise

Drive transformation

Protect our customers

