Cyber Defense Strategies
Detecting Earlier and Responding Faster

ZERO HYPE
ZERO FALSE POSITIVES
ZERO EXCUSES

Hamlet Khodaverdian, VP Americas

LMNTRIX
BE THE HUNTER | NOT THE PREY

WHO WE ARE

- Founded Earthwave in 1999 – Gartner leading APAC MSSP
- Was the core security service for Telstra and Cisco MSS in Australia
- 2012 sold to NTT Japan - ~$100m exit – No VC Investors
- Helped globalise MSS for Dimension Data / NTT Japan – Managed 10 SOC's Globally for Dimension Data / NTT Japan
- Recognised the failure of legacy SOC approach to cyber defense when only relying on logs and SIEM
- We knew there was a better way. Started LMNTRIX in 2015 after considerable research and investment

LMNTRIX

BE THE HUNTER | NOT THE PREY

Issues we had identified

#1 – How are you using your current SOC?
Are you able to detect any new threats?
Most organizations use their SOC for incident response

#2 – Alert Fatigue – Even after adding ML/AI/SOAR/Threat Intelligence

#3 – Whenever a threat bypasses your existing security controls - In most cases it means there is no alert for it

LMNTRIX
BE THE HUNTER | NOT THE PREY

Detect threats that are consistently bypassing existing security controls and provide full IR lifecycle

To do this correctly requires an integrated, multi-vector platform which combines the tactical acquity of automated systems (ML/AI/Automation) with human analysts

LMNTRIX

BE THE HUNTER | NOT THE PREY


YOU ARE GOING TO BE
BREACHED
LMNTRIX
BE THE HUNTER | NOT THE PREY

THE SLIDING SCALE OF **CYBER SECURITY**

ARCHITECTURE

The planning establishing, and upkeep of systems with security in mind

PASSIVE DEFENSE

System added to the Architecture to provide reliable defense or insight against threats without consistent human interaction

ACTIVE DEFENSE

The process of analysts monitoring for, responding to, and learning from adversaries internal to the network

INTELLIGENCE

Collecting data, exploiting it into information, and producing intelligence

OFFENSE

Legal countermeasures and self-defense actions against an adversary

LMNTRIX

BE THE HUNTER | NOT THE PREY

BLOCK THE NOISE & FALSE POSITIVES
TERMINATE ALERT FATIGUE

- **At minimum use NGFW, Email & Web Security**
- **Build an outer shell**
- **Think of it like the layers of an onion**

LMNTRIX
BE THE HUNTER | NOT THE PREY

DEVELOP A POST BREACH STRATEGY **FOR DETECTING MALWARE**

- Automate detections across multiple threat vectors
  - Email(Example) links/attach, Web, IDS, Encrypted attacks, Retrospection
  - Instrumenting Constituent Systems in the Cloud
  - Monitoring Operational Technology
  - Monitoring Mobile
  - Bots, malware, ransomware, Sandboxes, Threat Intelligence
  - EDR, NDR, Adversary behaviours, ML, FIM, DLP
  - Monitoring in Zero Trust Environments

DEVELOP A POST BREACH STRATEGY **FOR DETECTING HUMAN ADVERSARIES**

- **Deceptions**
- **Moving target defense**
- **Lateral movement**
- **Insider threats**
- **Identity**

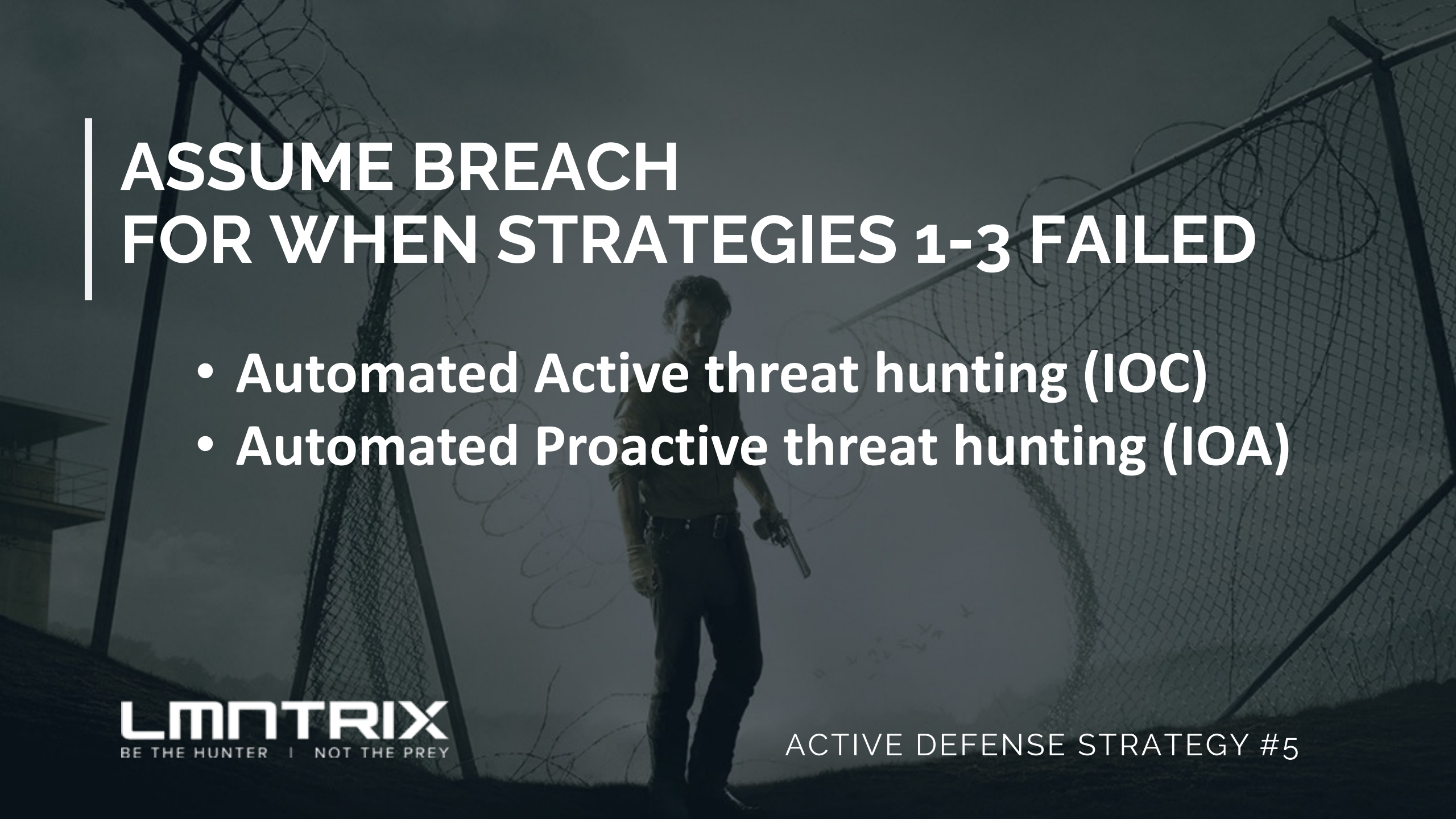
LMNTRIX
BE THE HUNTER | NOT THE PREY

ACTIVE DEFENSE STRATEGY #3

DEVELOP A POST BREACH FORENSICS CAPABILITY - EVIDENCE PRESERVATION & IR (Replay)

- Network Forensics – Meta Data
- EDR
- Logs
- Threat & underground intelligence

LMNTRIX
BE THE HUNTER | NOT THE PREY

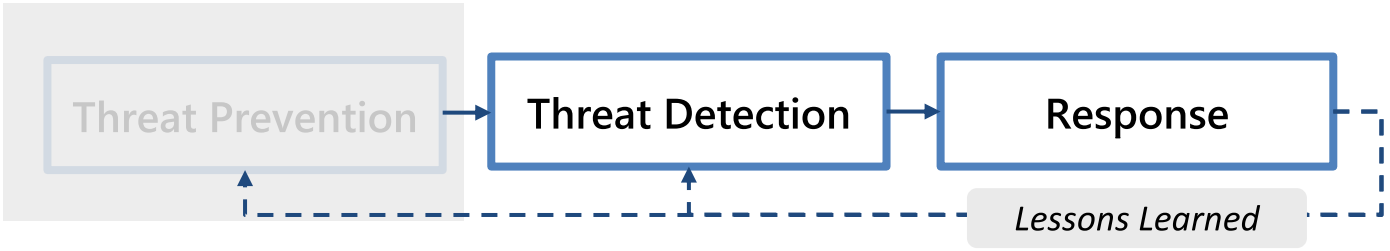


ASSUME BREACH
FOR WHEN STRATEGIES 1-3 FAILED

- **Automated Active threat hunting (IOC)**
- **Automated Proactive threat hunting (IOA)**

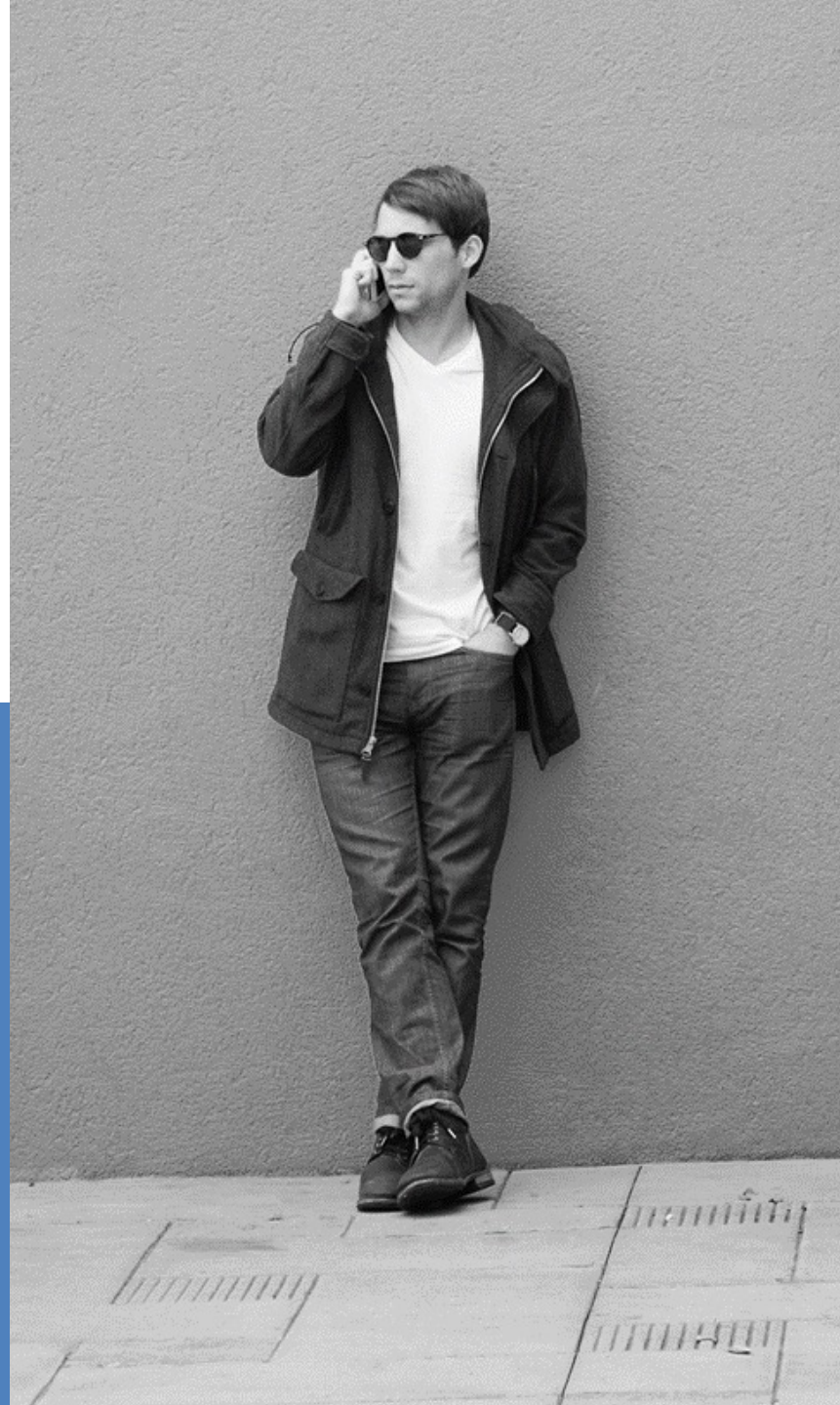
LMNTRIX
BE THE HUNTER | NOT THE PREY

ACTIVE DEFENSE STRATEGY #5



At some point the adversary has to do something anomalous (re-insert)

You have to be able to spot that and quickly take action on it



THREAT VALIDATION
AUTOMATE EVERYTHING

- Validating threats
- Incident creation
- Client communication
- Threat intelligence, Vulnerability management, Compliance, Automating Reporting:, Automating Manual Tasks
- SIEM, SOAR, UEBA

LMNTRIX
BE THE HUNTER | NOT THE PREY

THREAT VALIDATION
AUTOMATE EVERYTHING

- Use bots - Python or Java and security-specific libraries like OpenCV for computer vision, OpenSSL for encryption and libraries such as scikit-learn for machine learning. (ML Engineer vs Context-Business) – Risk Scoring system (Intelligence driven)
- Can your analyst move from endpoints to packets to threat intelligence to deceptions to cloud and create a story in a single click for that IOC? Very difficult with just logs.

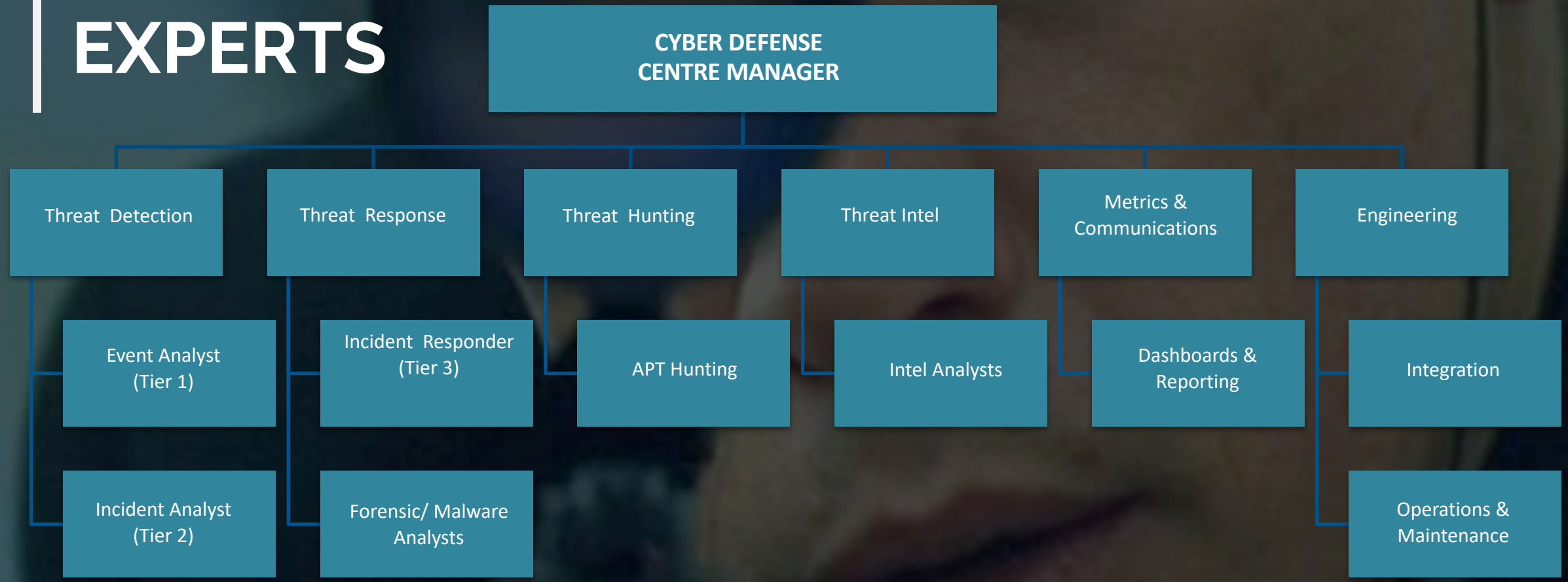
TO FIND A HUMAN - YOU NEED A HUMAN
HIRE AND GROW QUALITY STAFF

- Whom Should I Hire?
- Grow Your Own SOC Staff
- Create an Environment that Encourages Staff to Stay
- Pre-Plan for Staff Turn-Over
- How Many Analysts Do I Need?

LMNTRIX
BE THE HUNTER | NOT THE PREY

ACTIVE DEFENSE STRATEGY #7

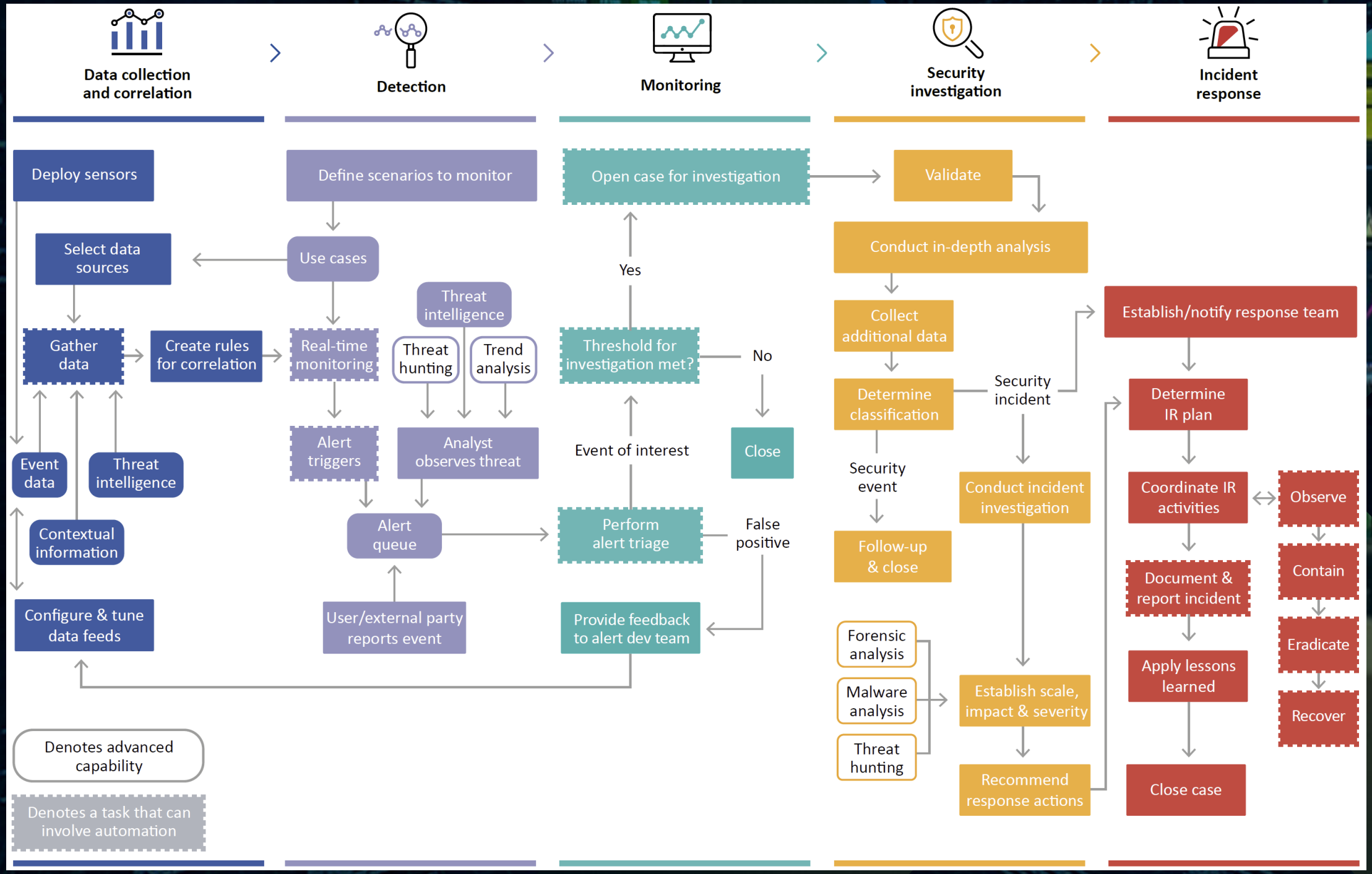
YOU NEED **EXPERTS**



LMNTRIX

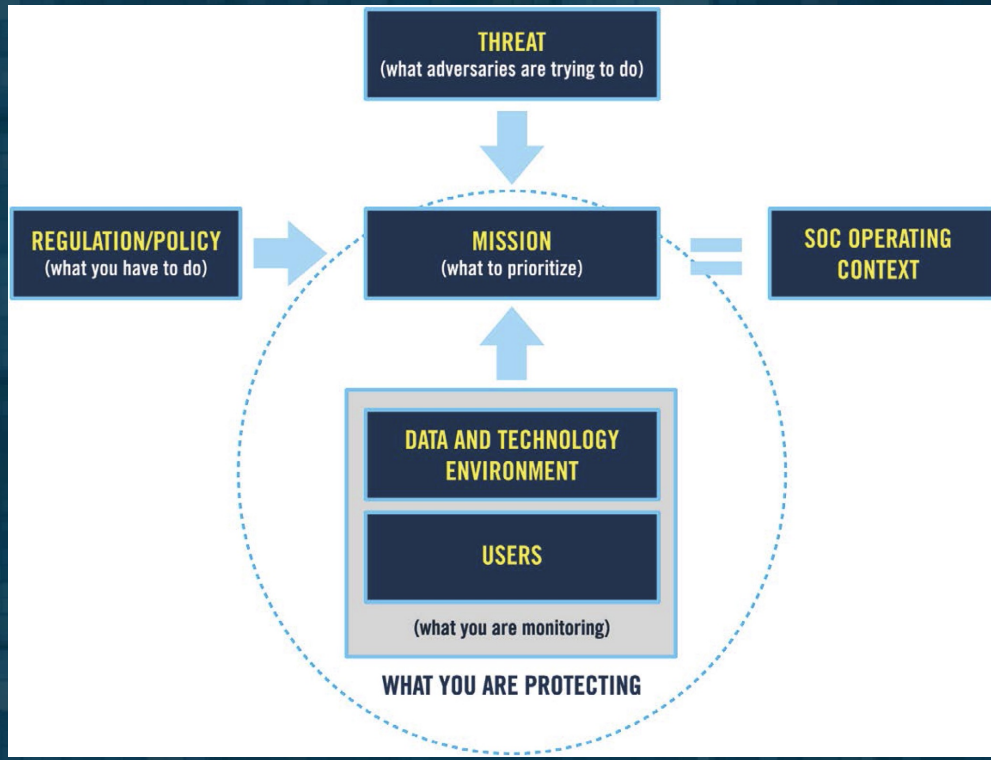
BE THE HUNTER | NOT THE PREY

RE CAPABILITIES OF A CDC



KNOW WHAT YOU ARE PROTECTING **AND WHY**

- Situational Awareness
- SOC Operating Context
- Understand the Organization's Mission
- Understand the Legal, Regulatory, and Compliance Environment
- Understand the Technical Environment, Especially Critical Systems and Data
- Understand the Users, User Behaviors, and Service Interactions
- Understand you Threat Model
- Building Awareness over Time

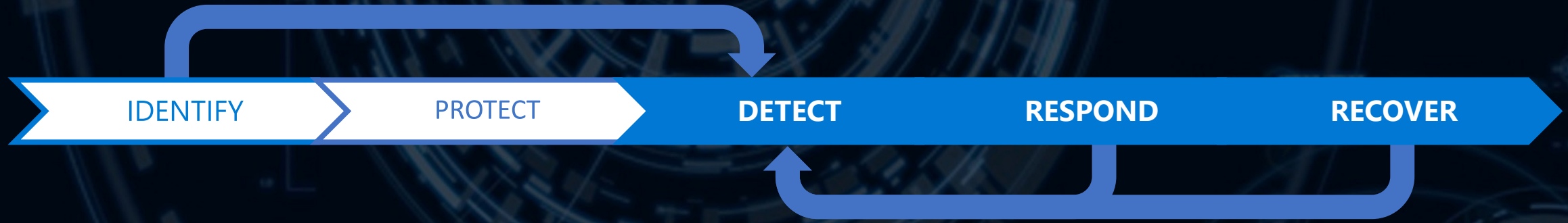


LMNTRIX
BE THE HUNTER | NOT THE PREY

FOCUS ON MEAN TIME TO REMEDIATION (MTTR)

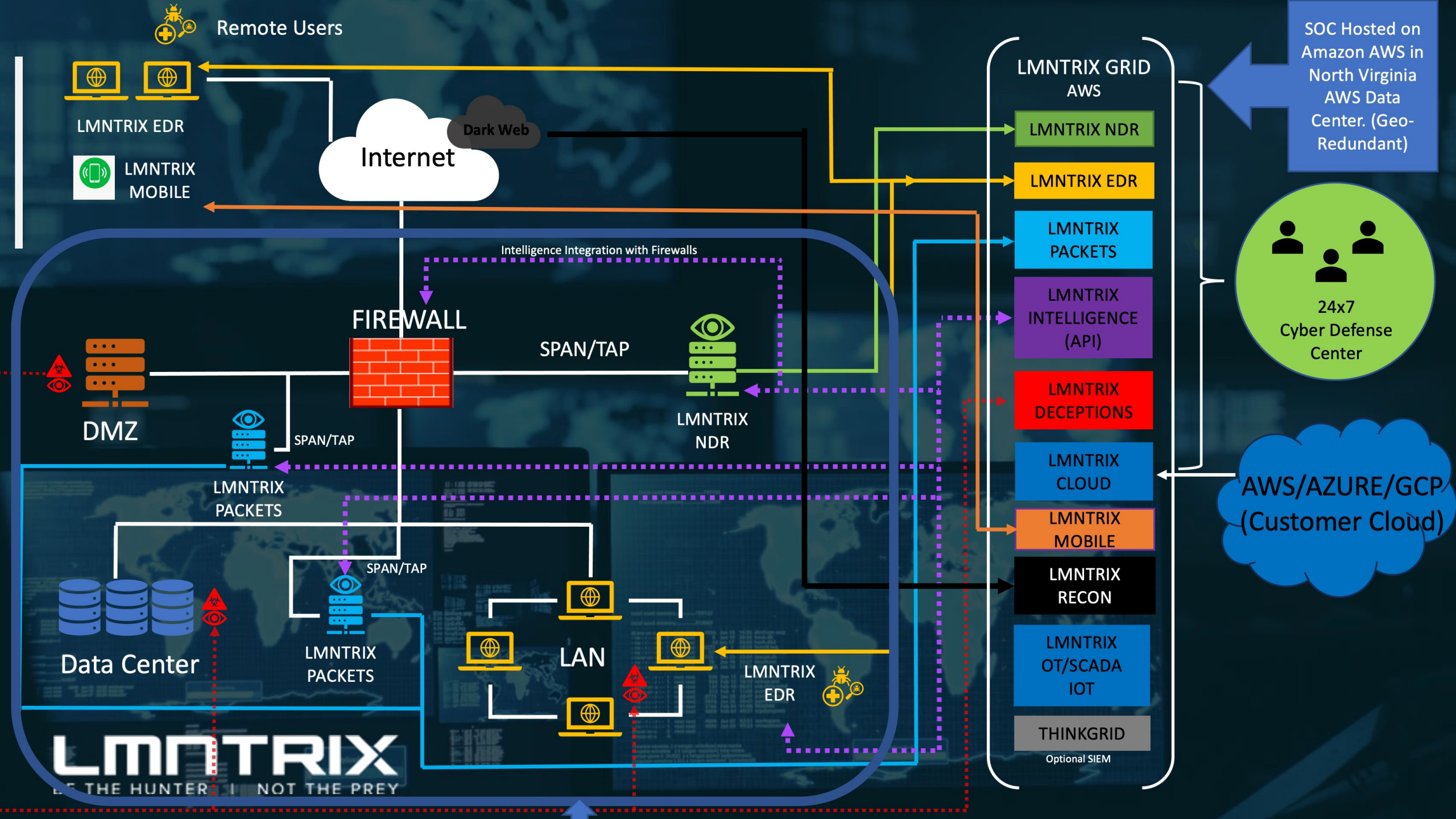
Drives up attacker cost by limiting dwell time
Time to Acknowledge (TTA), Time to remediate (TTR), manual vs automation, escalations

1. **Monitor all assets**
   Emphasis on attack paths to critical assets



2. **Rapid investigation and remediation**
   Focused on resuming secure business operations

LMNTRIX
BE THE HUNTER | NOT THE PREY


Remote Users
LMNTRIX EDR
LMNTRIX MOBILE
Internet
Dark Web
Intelligence Integration with Firewalls
FIREWALL
SPAN/TAP
DMZ
LMNTRIX NDR
SPAN/TAP
LMNTRIX PACKETS
SPAN/TAP
Data Center
LMNTRIX PACKETS
LAN
LMNTRIX EDR
LMNTRIX
BE THE HUNTER | NOT THE PREY
LMNTRIX GRID
AWS
LMNTRIX NDR
LMNTRIX EDR
LMNTRIX PACKETS
LMNTRIX INTELLIGENCE (API)
LMNTRIX DECEPTIONS
LMNTRIX CLOUD
LMNTRIX MOBILE
LMNTRIX RECON
LMNTRIX OT/SCADA IOT
THINKGRID
Optional SIEM
SOC Hosted on Amazon AWS in North Virginia AWS Data Center. (Geo-Redundant)
24x7 Cyber Defense Center
AWS/AZURE/GCP (Customer Cloud)

CYBER SCAPE 2023

Network & Infrastructure Security

Advanced Threat Protection
Barracuda, BlueHexagon, Bluvector, Broadcom, Check Point, Cisco, Corsa, FireEye, Fortinet, Hornetsecurity, Huawei, Hysolate, JoeSecurity, Juniper, lastline, mimecast, OPSWAT, paloalto, RESEC, Sasa Software, SonicWall, Sophos, Trellix, VMRay, Votiro, WatchGuard

NAC
aruba, Auconet, Axonius, Cisco, Extreme, ForeScout, Fortinet, Genians, NetShield, portnox, Pulse Secure, Trustwave

SDN
BlackRidge, Certes, Cisco, Cybera, Cyxtera, Tempered, Transient, Versa, zentera, Zero, zscaler

DDoS Protection
Akamai, Check Point, Cloudflare, Corero, F5, Fortinet, imperva, neustar, Nexusguard, Nsfocus, Oracle, Quad9, Radware, Secure64

DNS Security
BlueCat, Cisco, Cyren, efficient iP, Infoblox, neustar, Secure64, Quad9, ThreatSTOP, Stackpath, Verisign

Network Firewall
algosec, CATO, Check Point, Cisco, Clavister, endian, Firemon, Forcepoint, Fortinet, Hillstone, Huawei, paloalto, Sangfor, Secucloud, SonicWall, Sophos, Stormshield, tufin, untangle

SASE
CATO, Check Point, Forcepoint, Fortinet, iboss, netskope, Opensystems, paloalto, perimeter 81, Skyhigh, Versa, zscaler

Deception
Acalvio, Attivo, CounterCraft, CyberTrap, fidelis, Illusive, Smokescreen, Thinkst Canary, TrapX, Viper

ICS + OT
Aperio, Bayshore, Belden, Cisco, Claroty, CritiFence, Cyberx, Dragos, endian, Forescout, Halo Digital, dimension, Nextnine, Nozomi Networks, OWL, PAS, PFP, Radiflow, Rhebo, SCADAfence, tenable, Verve

Network Analysis & Forensics
Awake, Bricata, CGS, Cisco, Cloudshark, corelight, Darktrace, ExtraHop, Fidelis, Firemon, Fortra, Gigamon, Grey Cortex, LogPoint, LogRhythm, MixMode, Netscout, paloalto, Perch, PICO, Plixer, SS8, utimaco, Vectra, Verint

Web Security
Akamai, aurionpro, Authentic8, Barracuda, Broadcom, capy, Cequence, Check Point, Cisco, ContentKeeper, Cyren, Defiant, digicert, Ericom, F5, Forcepoint, Fortinet, GoSecure, Hornetsecurity, Human, iboss, imperva, Menlo Security, Micro Focus, Namogoo, perimeter 81, proofpoint, randed, Reblaze, reflectiz, SecuredTouch, SHAPE, Shieldsquare, Skyhigh, smoothwall, Sophos, source defense, Trend Micro, Trustwave, unbotify, zscaler

Endpoint Security

Endpoint Prevention
AhnLab, avast, Avira, BeyondTrust, Binary Defense, Bitdefender, BlackBerry, Blueridge, Broadcom, Bufferzone, Check Point, Comodo, cybereason, CyberArk, deepinstinct, elastic, Ericom, eset, F-Secure, Faronics, Fortinet, Fortra, HP, Hysolate, intego, ivanti, kaspersky, Microsoft, Morphisec, Nyotron, OPSWAT, paloalto, panda, Perception Point, SentinelOne, Sophos, sparkcognition, Stormshield, Tehtris, Trellix, Trend Micro, VMware Carbon Black, Webroot, Zero Networks

Endpoint Detection & Response
Belden, Binary Defense, Bitdefender, BlackBerry, Broadcom, Cisco, Comodo, cybereason, Cybonet, Cycraft, Cynet, dtex, elastic, Fenror7, fidelis, FireEye, Forcepoint, Fortinet, Fortra, GoSecure, Huntress, kaspersky, Microsoft, Nehemiah, Nyotron, paloalto, panda, Promisec, RSA, secpod, SentinelOne, Sophos, Tanium, Tehtris, VMware Carbon Black, WatchGuard, ziften

Application Security

WAF & Application Security
A10, Akamai, Arxan, Barracuda, Cequence, Citrix, Cloudflare, Contrast Security, DBAPP Security, ergon, F5, fastly, Fortinet, Fortra, imperva, Kona, netsparker, NetSPI, onapsis, Oracle, paloalto, Penta Security, perimeter x, portshift, Promon, Protego, Qualys, radware, RAPID7, Reblaze, riverbed, rohde & schwarz, safe-t, SEWORKS, SHAPE, sqreen, Stackpath, Sucuri, Templarbit, ThreatX, Trend Micro, Trustwave, Veracode, Vicarius, VIRSEC, wallarm, waratek, WhiteHat

Application Security Testing
acunetix, Assert Security, Checkmarx, Digivante, ERPScan, Fasoo, Fortra, hackerone, HCL Software, IBM, kryptowire, Micro Focus, N-Stalker, NowSecure, onapsis, OX, Parasoft, Perforce, PortSwigger, Qualys, RAPID7, rezilion, Secure Code Warrior, SecurityCompass, ShiftLeft, SiteLock, snyk, sonarsource, Synack, synopsys, tenable, Trustwave, Veracode, WhiteHat, WhiteSource

MSSP

Traditional MSSP
accenture, AT&T, Atos, BAE Systems, BT, CenturyLink, Clone Systems, Cybereason, Foresite, IBM, MegaPath, NTT, nuspire, Optiv, SK shieldus, Trustwave, verizon, wipro

Advanced MSS & MDR
Anitian, Arctic Wolf, Atos, Booz Allen Hamilton, Cybriant, Cyderes, deepwatch, eSentire, expel, Fortra, Kivu, Rapid7, Raytheon, Secureworks, unisys

Data Security

Encryption
anjuna, baffle, Cypherix, cyphre, eshare, ENVEIL, Fortanix, HP, Keyfactor, nucypher, PKWARE, Protegrity, Sharp Secure, StorMagic, Thales, Titanium, Trend Micro, virtru

DLP
Broadcom, Code42, Cososys, Dasera, fidelis, Forcepoint, Fortra, GTB Technologies, Infowatch, SearchInform, Skyhigh, Somansa, Zecurion

Data Privacy
Actifile, BigID, Ground Labs, Integris, mineye, NetApp, nuix, OneTrust, Privacera, SecuPi, Spirion, Sytorus, TrustArc, trust-hub, Very Good Security, Wirewheel, Fortra

Data Centric Security
Code42, Cyberhaven, Datex, dataphy, druva, egress, Fortra, Ionic, Microsoft, opentext, Privitar, Protegrity, Seclore, Spirion, StorageCraft, Varonis

Mobile Security
appdome, Better, BlackBerry, BlueCedar, cellrox, Check Point, CommunicAte, Cyber adAPT, deepinstinct, eMune, Fyde, helixos, INPEDIO, Kaymera, Koolspan, kryptowire, Lookout, mobileiron, NortonLifeLock, NowSecure, pradeo, PSafe, SaltDNA, silent circle, SOTI, TeleSign, Teskalabs, tigerconnect, Trustlook, Vaulto, vmware, wandera, wickr, Zimperium

Risk & Compliance

Risk Assessment & Visibility
AnNimbus, Axonius, Balbix, cavirin, Coalfire, Coalition, Cyber Observer, CyberCube, CyberSaint, Cyence, Firemon, Innosec, JupiterOne, Kenna, Keycaliber, mastercard, Nehemiah, noetic, Nopsec, Outpost24, panaseer, Prevalent, RedSeal, Red Vector, rezilion, riskrecon, RiskSense, Secureworks, Simspace, Skybox, tenable, UpGuard, Venafi, venminder, zeguro, ZeroNorth

Risk Quantification
Arceo.ai, Arx Nimbus, BitSight, corax, Cowbell Cyber, FICO, Guidewire, Panorays, Prevalent, RiskLens, riskrecon, SecurityScorecard

Pen Testing & Breach Simulation
AttackIQ, bugcrowd, Cobalt, Cronus, Cyberrat, Cycognito, Cymulate, Depth, FireEye, Mazebolt, Nopsec, Picus, PCysys, RAPID7, SafeBreach, XM Cyber

GRC
algosec, Apptega, Caveonix, Diligent, Firemon, MetricStream, Navex, netwrix, Onspring, Resolver, reliance, RSA, SAI Global, TrustMAPP, tufin

Security Awareness & Training
Barracuda, CyberVista, Fortra, Hook Security, Immersive Labs, Ironscales, KnowBe4, proofpoint, Rangeforce, SANS, SimSpace

Identity & Access Management

Authentication
Acceptto, Auth0, averon, BehavioSec, BioCatch, BlackBerry, callsign, Centrify, CORE Security, Duo, Exostar, ForgeRock, FUDO Security, Google, HYPR, IDEE, imprivata, Intrinsic ID, jumio, LexisNexis, nok nok, pindrop, Ping, plainID, SaaSPass, SaferPass, Secret Double Octopus, Secure Key, SecurePush, Silverfort, tascent, transmit, TransUnion, Trusona, UnboundID, Unifyid, Uniken, V-Key, Virgil Security, xage

IDaaS
Avatier, Centrify, IBM, idaptive, ilantus, Microsoft, okta, onelogin, Oracle, Ping, RSA, Thales, welcome

Privileged Management
BeyondTrust, Centrify, CyberArk, FUDO Security, Hitachi, IBM, ManageEngine, Micro Focus, One Identity, Remediant, SecureLink, thycotic, Xton

Identity Governance
Axiomatics, Deep Identity, fálaina, Fortra, SailPoint, Saviynt, simeio

Consumer Identity
Akamai, Auth0, ForgeRock, IDExperts, ID.me, jumio, loginradius, Microsoft, Ping, Pirean, Salesforce, SAP, Secure Key, Trulioo, verato, Verify, Zamna

Security Ops & Incident Response

SIEM
AT&T Cybersecurity, Blackstratus, bmc, Cygilant, Devo, DNIF, exabeam, Fortinet, HanSight, Huntsman, IBM, Igloo Security, logentries, LogPoint, LogRhythm, logz.io, Micro Focus, Netsurion, EventTracker, Palantir, RAPID7, RSA, Sawmill, Securonix, solarwinds, splunk, sumo logic, TIBCO, Trellix, Trustwave

Security Incident Response
arctos networks, atarlabs, ayehu, BreachQuest, Cybersponse, Cyber Triage, D3 Security, Darklight, Demisto, DFLabs, N-able, encode, IBM, Kivu, LogPoint, Mandiant, Microsoft, netskope, paloalto, Polarity, Query.ai, Radar, RAPID7, Raytheon, Secureworks, servicenow, Siemplify, splunk, Swimlane, Syncurity, ThreatConnect, Trellix, Verint, witfoo

Security Analytics
Awake, Broadcom, Cycraft, Darktrace, dtex, empow, exabeam, Fluency, Fortinet, HanSight, haystax, Imvision Technologies, IronNet, LogPoint, LogRhythm, Micro Focus, observeIT, paloalto, patternex, Reservoir Labs, Rvidium, RSA, Securonix, sumo logic, Teramind, ThetaRay, Vectra, Veriato, vmware

Momentum Cyber

Threat Intelligence
4iQ, Anomali, Blueliv, BlueVoyant, Centripetal, Cisco, Cyberint, digital shadows, DomainTools, EclecticIQ, Flashpoint, Foresight, Group-IB, HanSight, HYAS, Intel471, IntSights, KELA, King, LexisNexis, LookingGlass, Malware Patrol, Nucleon, Recorded Future, ReversingLabs, RiskBased Security, RiskIQ, SenseCy, Sixgill, Skurio, SpyCloud, Surfwatch, ThreatConnect, ThreatQuotient, ThreatSTOP, TRU*STAR, Webroot

IoT

IoT Devices
Agilepq, Apolloshield, Armis, Bastille, BlackBerry, Centri, Cyberx, Cylus, dellfer, Forescout, Icon Labs, Imubit, Keyfactor, Level, MagicCube, Medigate, Mocana, MDX, Ordr, Regulus, riscure, Rubicon, Securithings, Senrio, Sepio, Zingbox, Ceq Group

Automotive
BlackBerry, Blue, C2A, Continental, Cymotive, Enigmatos, foretellix, GuardKnox, Harman, Karamba Security, NNG, otonomo, SafeRide, Trillium, Upstream

Connected Home
Bitdefender, Cujo AI, F-Secure, Fortress, NortonLifeLock, RUBICA, sam

Messaging Security
Area 1, BAE Systems, Barracuda, BlackBerry, Cisco, Cybonet, Cyren, FireEye, Forcepoint, Fortinet, Fortra, GoSecure, GreatHorn, Inky, Ironscales, malguard, Material, Micro Focus, Microsoft, mimecast, NortonLifeLock, proofpoint, Sasa Software, SonicWall, Sophos, Trellix, Trend Micro, Trustwave, Vade Secure, Validmail, Votiro, Webroot, wickr, zerospam, ZIX

Digital Risk Management
Axur, CRISP, Cyberint, digital shadows, DigitalStakeout, Echosec, Fortra, LookingGlass, Namogoo, reflectiz, RiskIQ, Safeguard Cyber, source defense, ZeroFox

Security Consulting & Services
accenture, Adapture, Align, AON, appsec, Bishop Fox, Booz Allen Hamilton, BT, Coalfire, Corvid, Deloitte, EY, FireEye, Fishtech, GreyCastle, GuidePoint Security, IBM, IOActive, Kivu, Kroll, KPMG, Kudelski Security, leidos, MindPoint Group, nccgroup, NEC, Nisos, NTT, Optiv, praetorian, pwc, Reveal Risk, Revolutionary Security, SecurityCompass, SERA-Brynn, SK shieldus, Spectorops, Sygnia, Versprite, wipro

Blockchain
Anchain.ai, Block Armour, Certik, Chainalysis, coinfirm, CYB, edge, elementus, Elliptic, Fireblocks, Forta, guardtime, Halborn, IDEE, Inter/stellar, NuID, Remme, Solidus Labs, TRM, valid.network, Zamna

Fraud & Transaction Security
Auth Tic, BioCatch, Block Fraud, Brighterion, Cardinal, Datavisor, Deduce, Early Warning, emailage, ethoca, EverCompliant, feedzai, FICO, fiserv, Forter, Group-IB, Guardian Analytics, Human, IdentityMind, IdenTrust, Kount, LexisNexis, MagicCube, Maxmind, NetGuardians, NICE, NuData Security, Outseer, riskified, SecuredTouch, Shift Technology, sift, Signifyd, Socure, SpyCloud, TokenEx, TransUnion, Uniken, Threatmetrix

Cloud Security

Container
anchore, aqua, Caveonix, Cisco, deepfence, Polyverse, paloalto, Qualys, RAPID7, Red Hat, Sophos, SUSE, sysdig

Infrastructure
Akamai, Armor, BetterCloud, Caveonix, cavirin, Chaosearch, Check Point, Cisco, ClearDATA, Cloudflare, Cloudways, Entrust, F5, fidelis, Fortinet, iboss, illumio, Lacework, orca security, paloalto, sonrai, Stacklet, Trend Micro, Varmour, vmware, WIZ, zscaler

CASB
Avanan, bitglass, Broadcom, Cisco, Coronet, Lookout, Managed Methods, Microsoft, netskope, Oracle, proofpoint, SecurIGO, Skyformation, Skyhigh, StratoKey

2023


LMNTRIX
BE THE HUNTER | NOT THE PREY
Thank You
shift