

In Detection, the Only Thing
That Matters Is Results

In Detection, the Only Thing that Matters Is Results

Today's Breach Detection Gap

Threats: Malware, Risky Behavior, Insiders & Advanced Attacks

Detection Accuracy Metrics

Signature vs. Behavior-based Attack Detection

LightCyber Magna Behavioral Attack Detection

Breach Detection Gap

99%

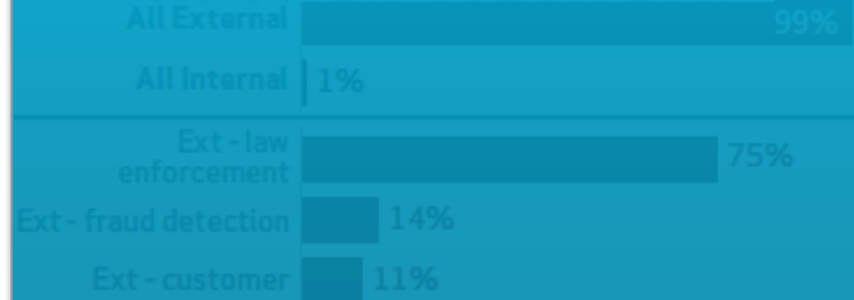
of post-intrusion attacks such as reconnaissance and lateral movement do not originate from malware.

Most Organizations Focus on Malware and External Attacks

146 days

Is the median length that attackers are present on a victim's network before detection

But Cannot Detect Attackers in Their Network



Malware Is Just the Tip of the Iceberg

A large, blue, multi-faceted iceberg floats in the ocean. The top of the iceberg is above the water line, while the much larger base is submerged. The word 'MALWARE' is written in large, semi-transparent blue letters across the top of the iceberg. Below the water line, the words 'HACKING TOOLS', 'NETWORKING TOOLS', 'ADMIN UTILITIES', and 'REMOTE DESKTOP APPS' are written in semi-transparent blue letters, arranged around the submerged part of the iceberg. Small black fish are visible swimming in the water around the submerged part of the iceberg. The background shows a blue sky with white clouds and a blue ocean.

MALWARE

HACKING TOOLS

NETWORKING TOOLS

ADMIN UTILITIES

REMOTE DESKTOP APPS

Plus, Attackers Can Hide in Encrypted Traffic



- **67%** of Internet traffic will be encrypted by the end of 2016



- **50%** of network attacks will use encryption to bypass controls by 2017

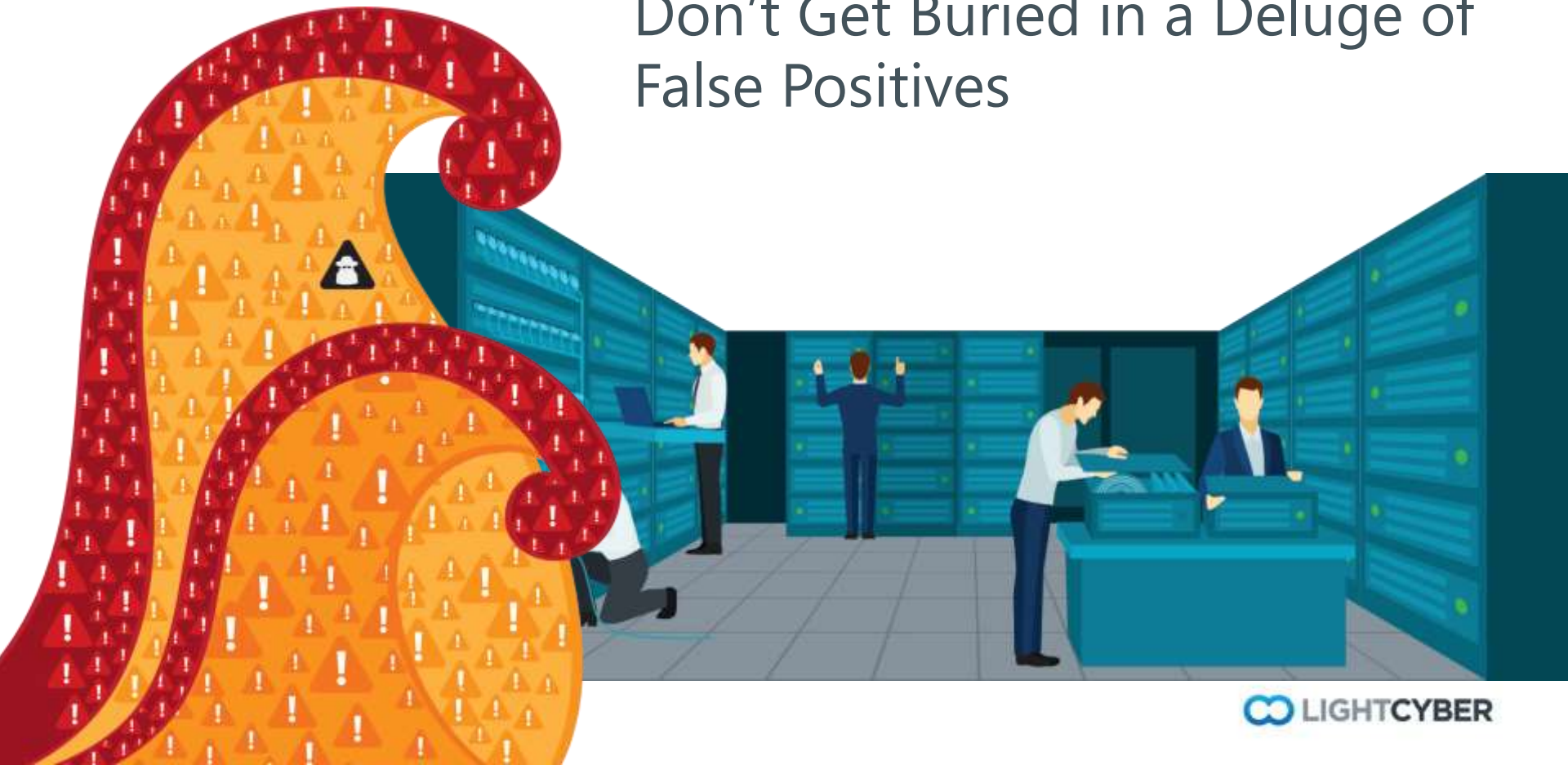


- **80%** performance degradation occurs when firewalls decrypt SSL traffic, on average

In addition, end-to-end encryption and privacy issues hinder SSL decryption plans

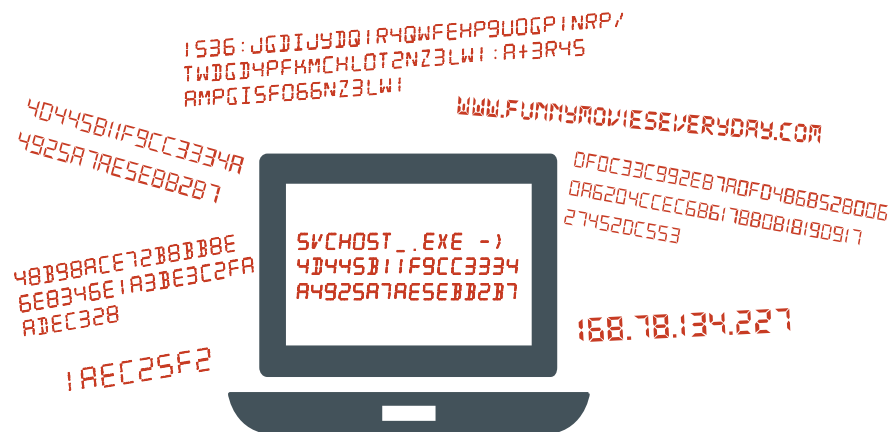
Detection Accuracy:

Don't Get Buried in a Deluge of False Positives



Current Limitations

Known Bad



Traditional Security

- Signatures, IoC's, Packet Signatures, Domains, Sandbox Activity
- Block, or Miss
- Necessary, Not Sufficient

Agents & Signatures

What's Needed?

Learned Good



What's Needed

- Learn What is Good [Baseline]
- Detect What Isn't [Anomaly]
- Catch What Slips Through the Cracks of Traditional Security

Agentless & Signature-less

The problem is the internal network!

16,937

**(average) # of SIEM
Alerts/Week**

80%

of networks are breached

Verizon, 2016

205

median detection gap (days)

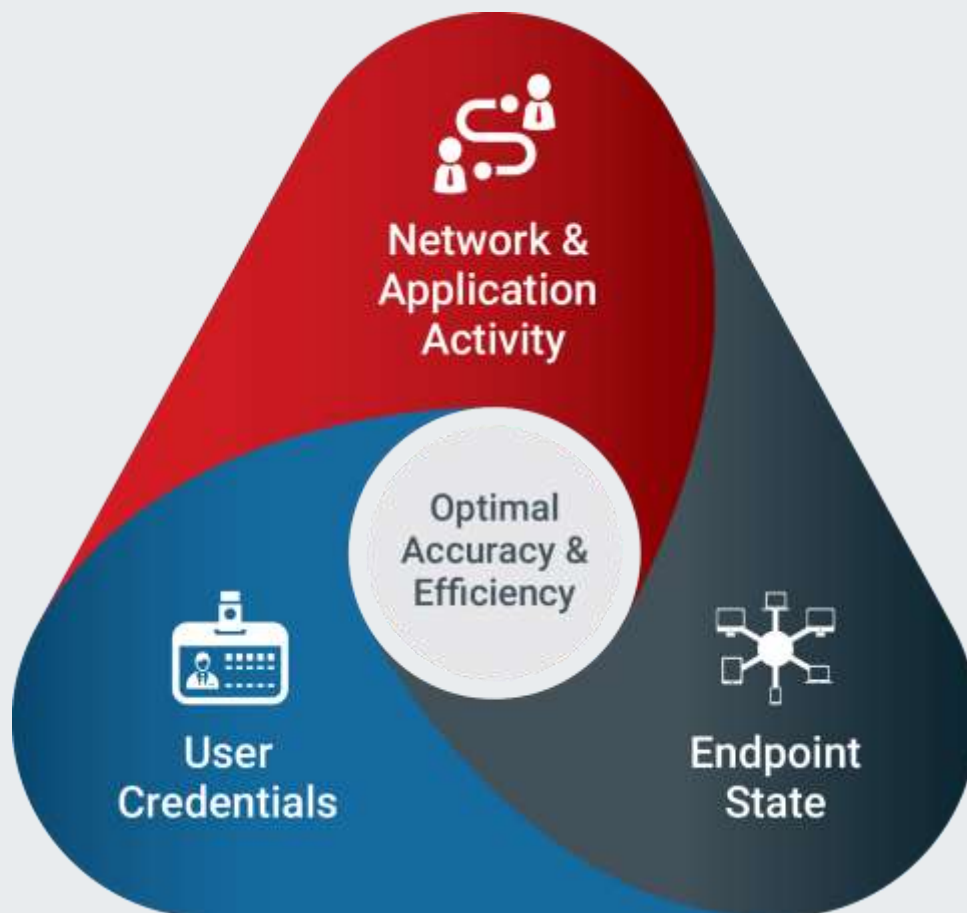
Mandiant, 2015

84%

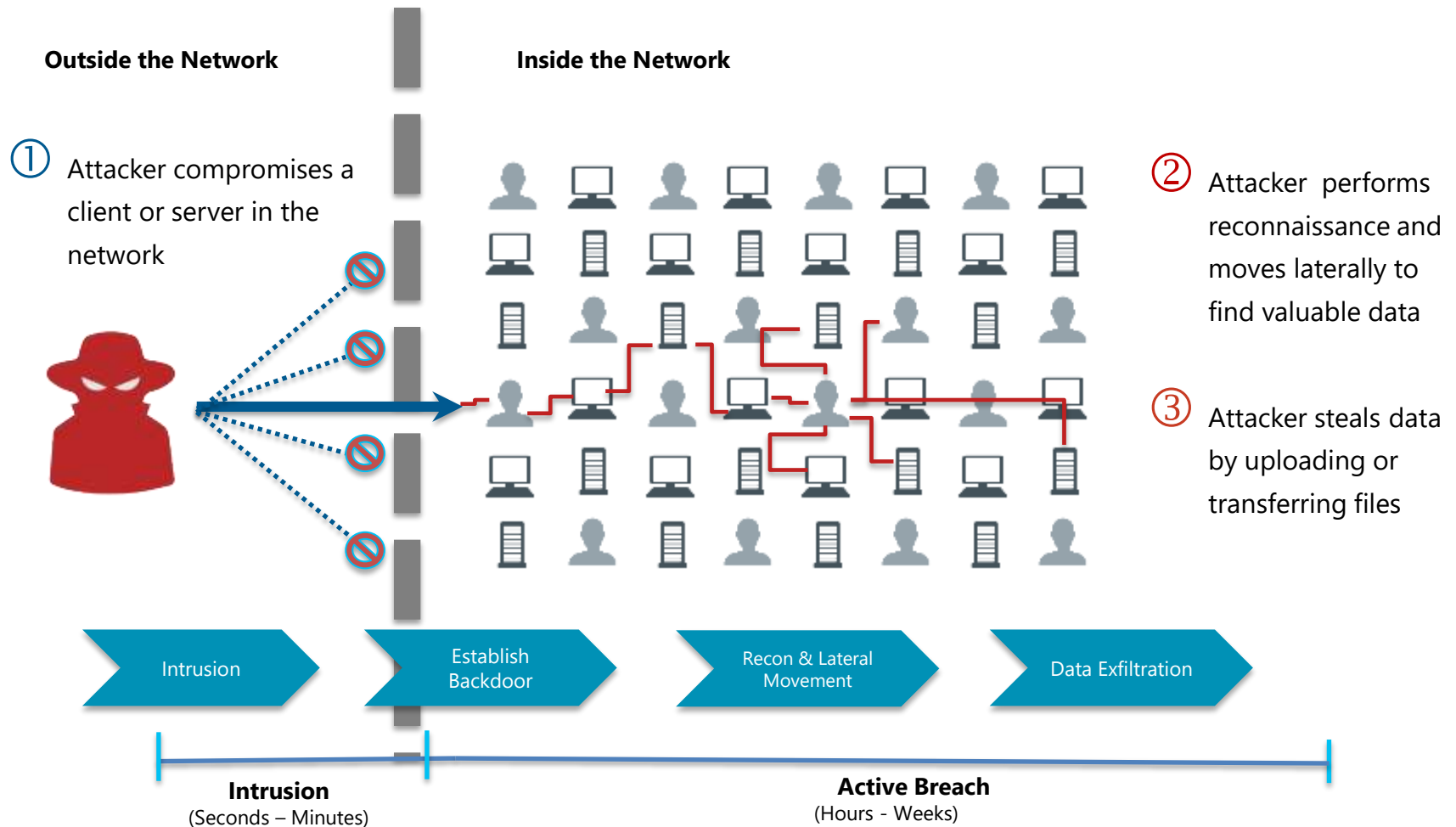
**of breaches discovered by an
external entity**

Mandiant, 2016

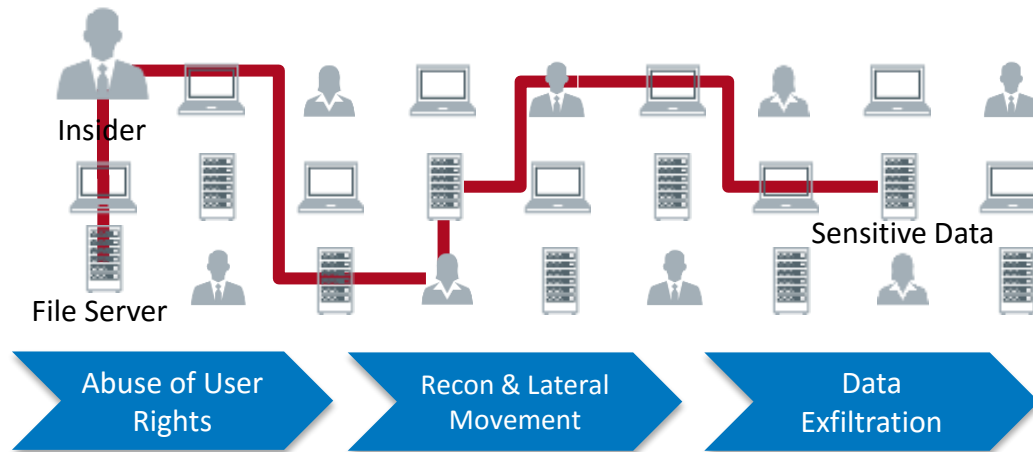
Behavioral Attack Detection: Optimal Data Context



Targeted Attacks



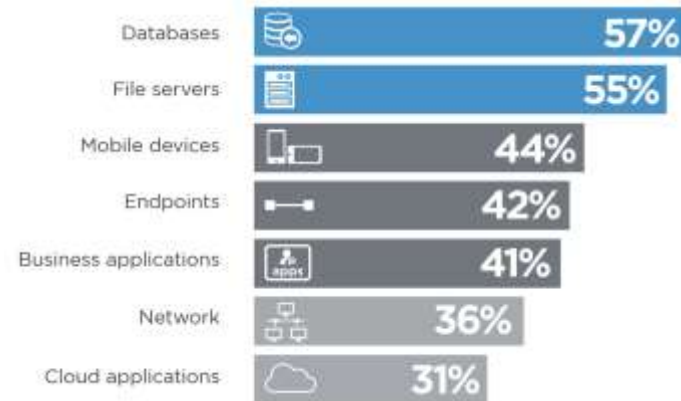
Insider Attacks



- ① Employee is upset by demotion; decides to steal data and quit job
- ② Employee accesses many file shares including rarely accessed file shares
- ③ Employee uses other users' credentials and exfiltrates a large volume of data

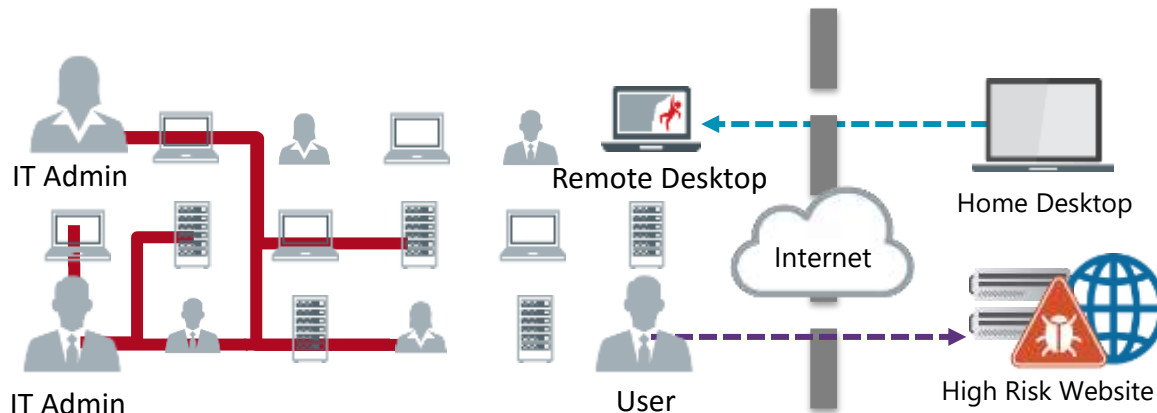
IT Assets at Risk

- Databases and file servers are considered the most vulnerable to insider attacks



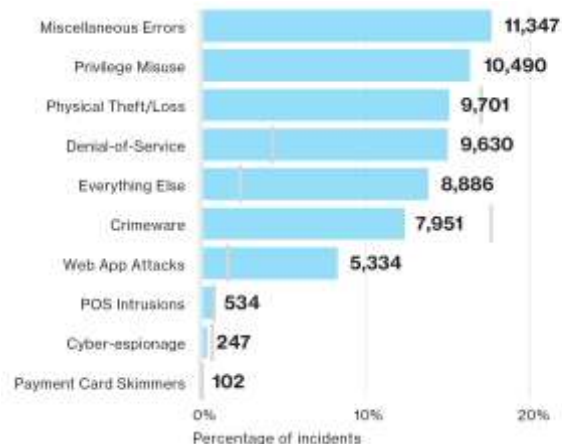
SOURCE: LinkedIn Group - Insider Threat Report sponsored by LightCyber

Risky Behavior



- ① Remote desktop access from home
- ② User credentials for service account shared by multiple admins
- ③ Access to high-risk websites

Data Breach Incidents



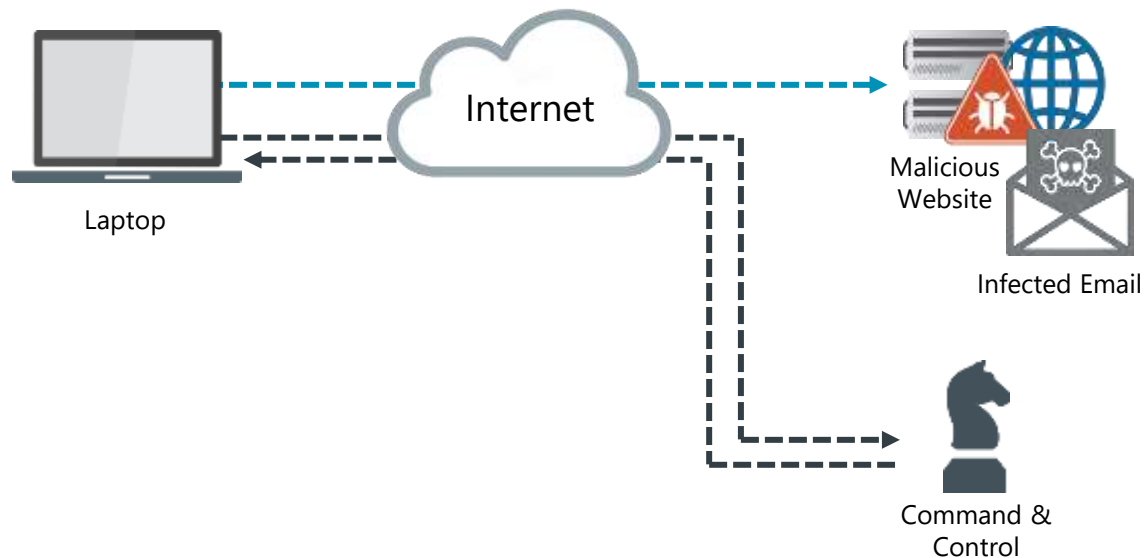
Miscellaneous errors, such as misconfiguration, misdelivery, and other errors, accounted for the highest number of data breaches in 2015

‘With all of the hubris and bravado in the InfoSec world, one proclamation we usually don’t hear is “Our employees NEVER make mistakes.”’

SOURCE: 2016 Verizon: Data Breach Investigations Report

Malware

Ransomware Attack



① User downloads ransomware from a website **or** opens a malicious email attachment

② Infected client contacts command and control server to receive remote instructions and exfiltrate data

Detect Malware “Phoning Home”

Monitor for access to known command and control servers

Detect failed DNS lookups and excessive DNS requests

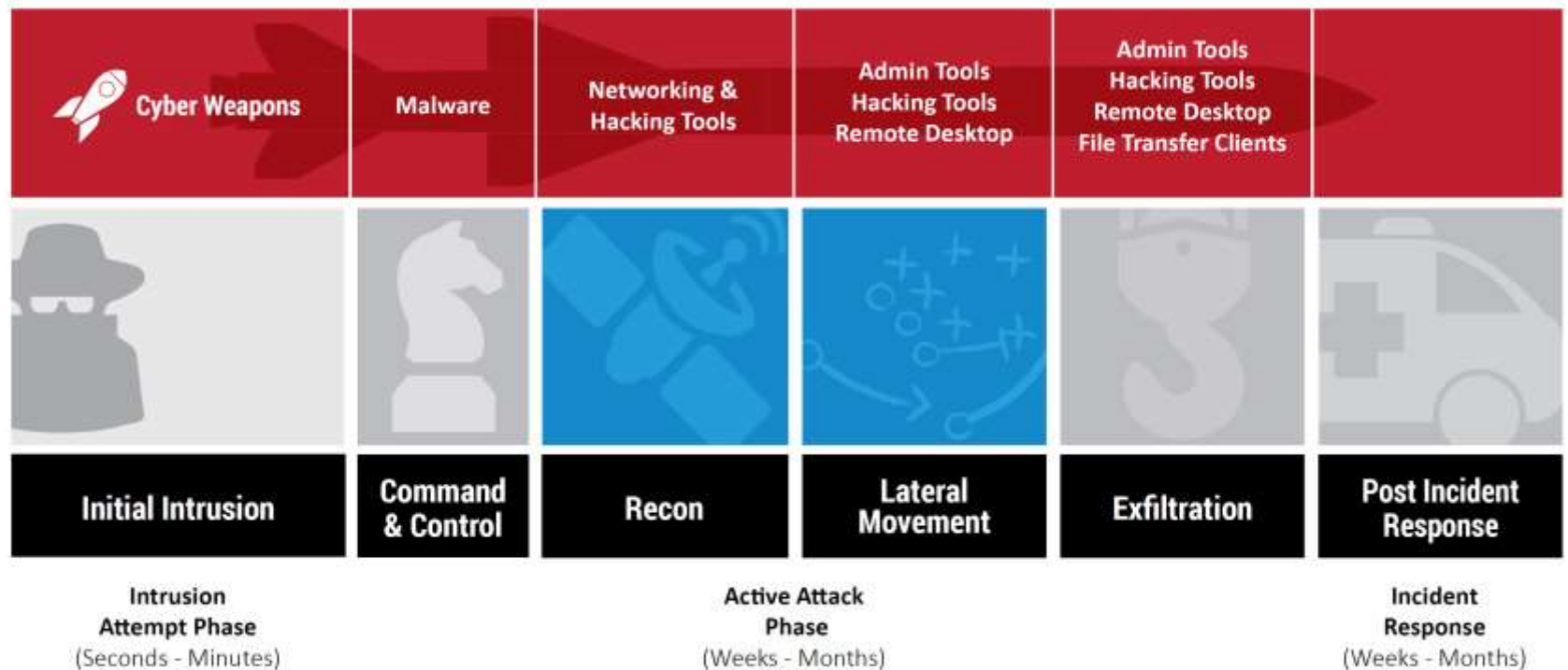
Look for repeated access to unusual destinations over time, and tunneled connections



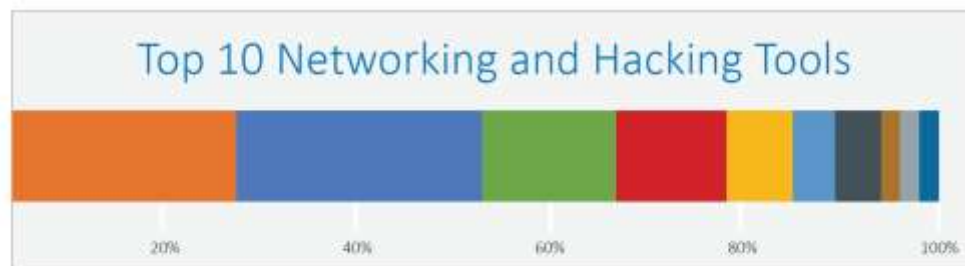
Cyber Weapons Research Findings

*Based on Anonymized Alert Data
and Network to Process Association
(N2PA) Technology*

Cyber Weapons Used in Phases of an Attack



Networking and Hacking Tools



Tool Name	Function	Percentage of Top 10
Angry IP Scanner	IP address and port scanner	27.08%
PingInfoView	Program that pings multiple hosts at once	25.00%
Nmap	Network discovery and security auditing tool	14.58%
Ping	Ping command program	12.50%
Mimikatz	A tool that extracts plain text passwords stored in Windows	6.25%
NCCrack	High-speed network authentication cracker	4.17%
Perl	Scripting tool that can be used to script hacking and reconnaissance tasks	4.17%
Windows Credential Editor	A tool that manages Windows logon sessions and credentials; can be used to perform "Pass-the-Hash" attacks	2.08%
SmartSniff	Network packet sniffer	2.08%
PDF Exploit Generator	An app that generates malicious PDF files that can infect vulnerable PDF applications	2.08%

- Attackers use well-known tools to map the network, probe clients, and monitor activity
- NCrack, Mimikatz, and Windows Credential Editor can be used to steal user credentials
- Some tools are native OS utilities

Admin Tools

- Attackers use a variety of command line shells, including native OS utilities
- Admin tools are used for lateral movement as well as recon and exfiltration



Remote Desktop Tools



- Remote desktop tools are:
 - Used for C&C and lateral movement
 - Also indicative of risky user behavior

Tool Name	Function	Percentage of Top 10
 TeamViewer	Cloud-based or locally hosted remote desktop and web conferencing software; can be used for command and control and lateral movement	37.22%
 WinVNC	Remote desktop software using Virtual Network Computing (VNC) for remote access	27.44%
 Radmin	Remote desktop and technical support software	9.09%
 AnyDesk	Remote desktop software	6.86%
 LogMeIn	Cloud-based remote access and remote desktop service	4.12%
 NetOp Remote Control	Cloud-based or locally hosted secure remote access	2.92%
 Ammyy Adminn	Free remote desktop and remote control software	1.72%
 Citrix Client	Application used to access Citrix XenDesktop and XenApp programs	0.86%
 Remote Desktop Connection	Microsoft's native remote desktop solution	0.69%
 UltraVNC	Remote desktop software that also includes file transfer and chat messaging	0.34%

Major Findings

Attackers often use “benign” apps, native OS tools and web browsers to conduct attacks



70%+ of malware was only detected on a single site, revealing targeted & polymorphic variants

Companies that only look for malware will miss attackers that are already in the network



LightCyber Magna Platform

*Using Behavioral Analytics to Find
Attacks & Malware on Your Network*

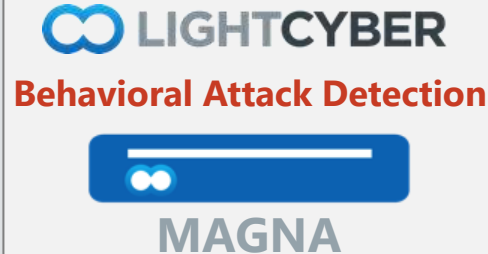
About LightCyber

Magna Platform Overview

- Network-Centric Detection
- Agentless & Signature-less
- Post-Intrusion: NTA/UEBA

Differentiation

- Most Accurate & Efficient:
Proven & Measured Success
- Broadest Context: Network + Endpoint + User
- Broadest Attack Coverage with Integrated Remediation



Operations Overview

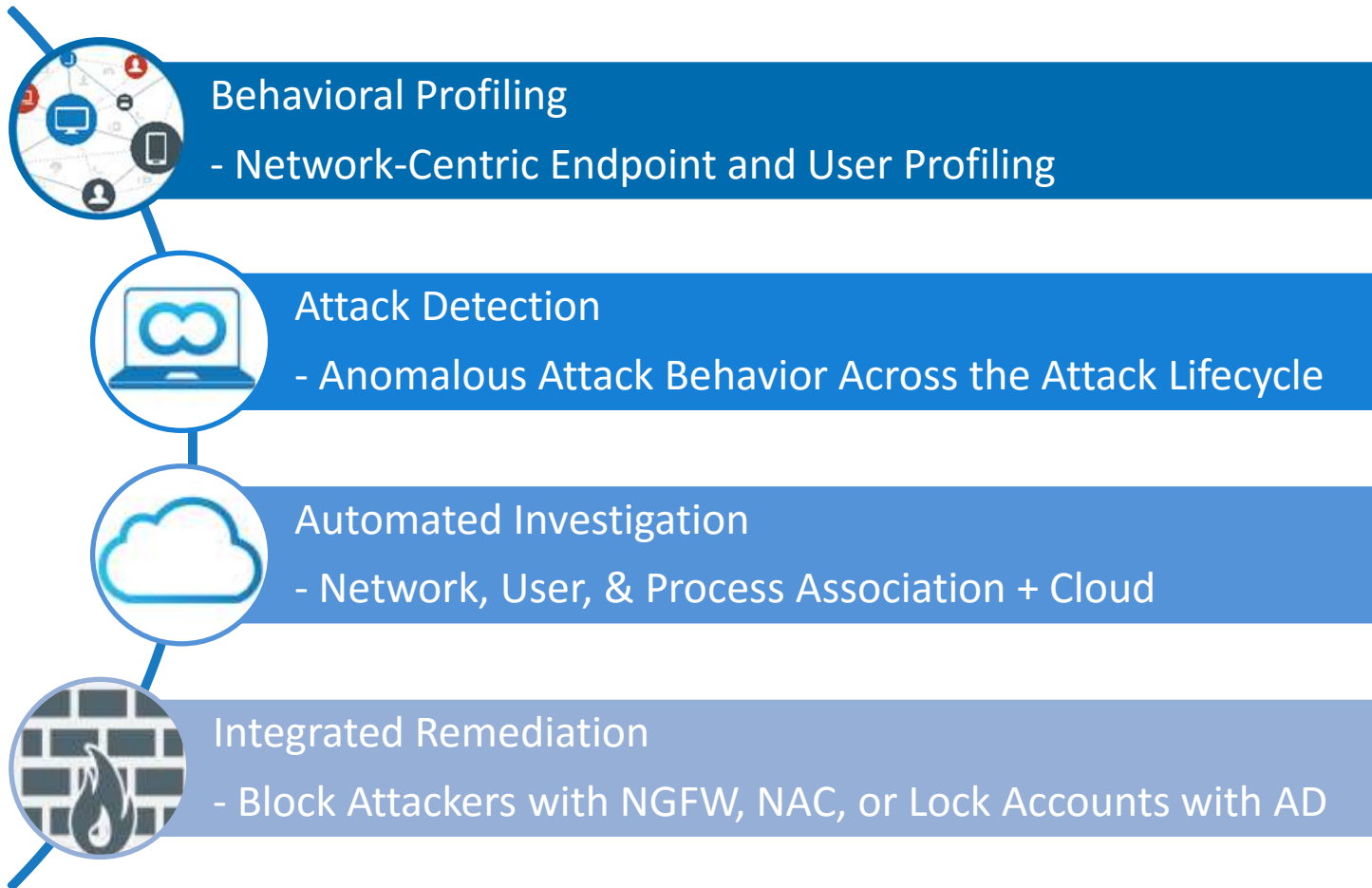
- US HQ - CA
- EMEA HQ - Amsterdam
- IL HQ - Ramat Gan
- Customers World-Wide

Verticals Served

- Finance & Insurance
- Public Sector
- Retail, Healthcare, Legal
- Service Providers
- Media, Technology, & More



Profiling, Detection, Investigation, & Remediation



LightCyber Magna Platform

Behavioral Attack Detection

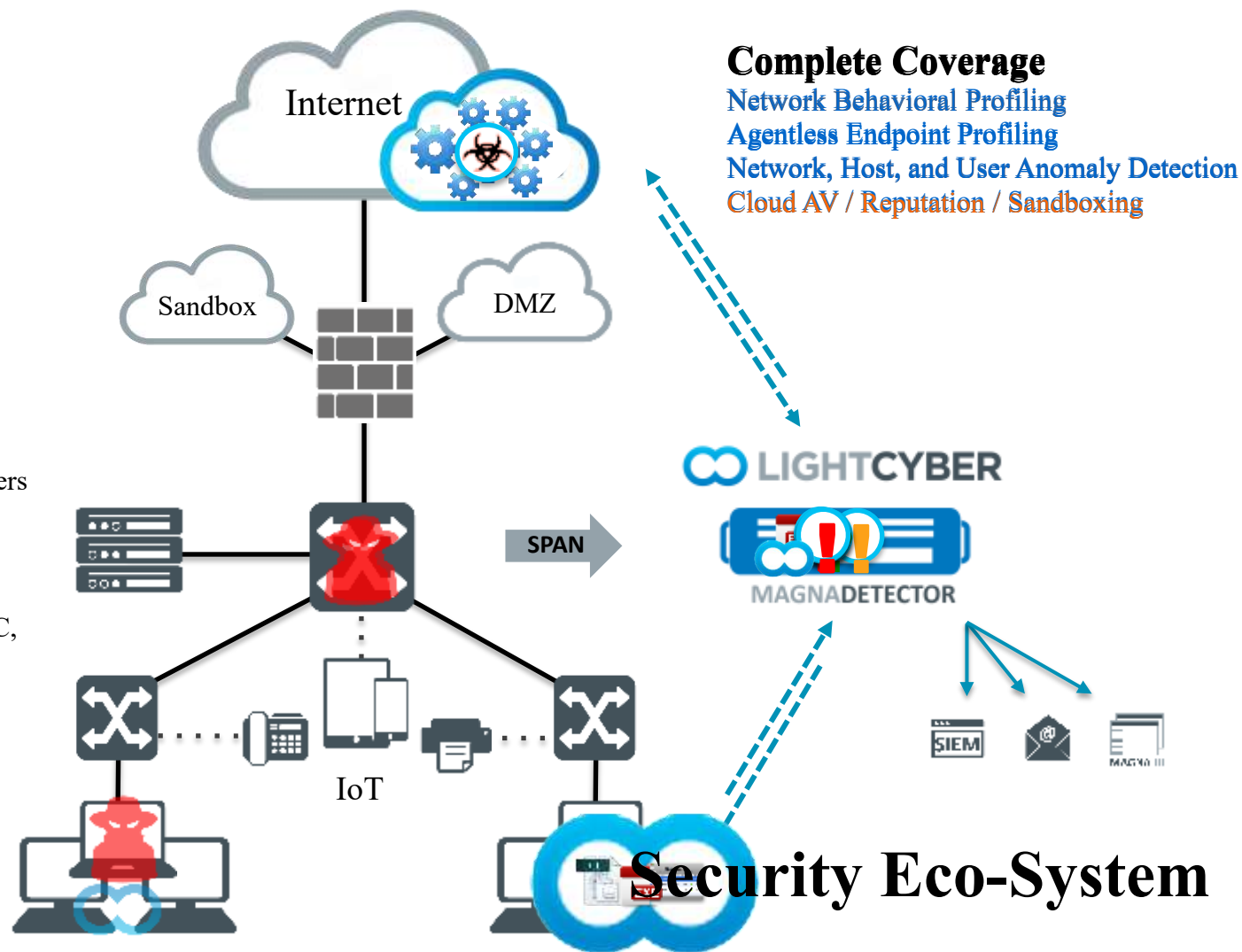
Malware
Risky Behaviors
Insider Attacks
Targeted Attacks

Servers:

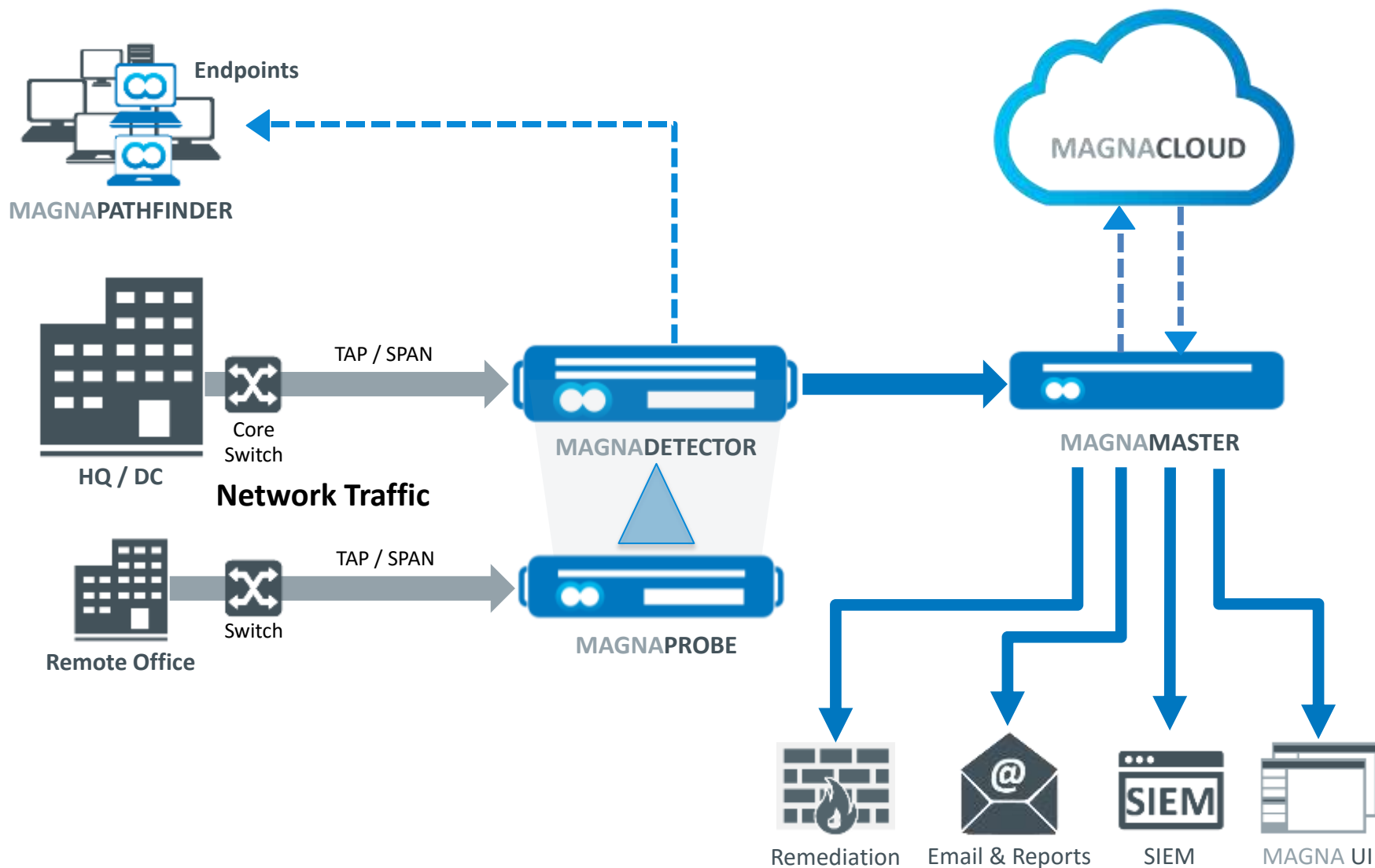
DHCP, DNS, AD, File Servers
etc

Protocols:

DHCP, DNS, Kerberos, RPC,
SMB, HTTP, HTTPS, etc



LightCyber Magna Platform



LightCyber Delivers Unbeatably Accurate Results

LIGHTCYBER ACCURACY



62%
ACROSS
ALL ALERTS

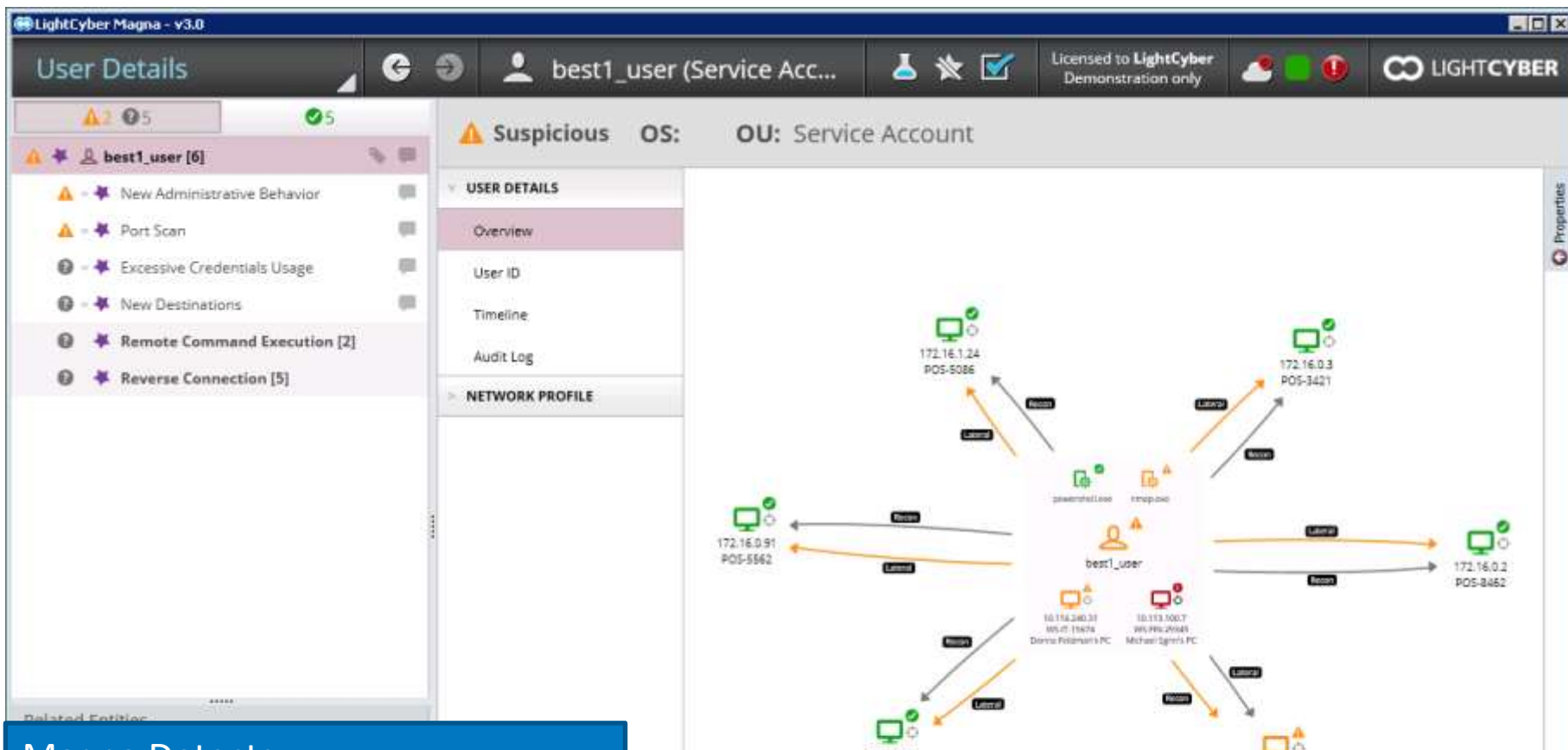


99%
ACROSS MAGNA'S
AUTOMATED "CONFIRMED
ATTACK" CATEGORY

EFFICIENCY

1.1 alerts / 1K Hosts / day

User, Entity; Network + Endpoint



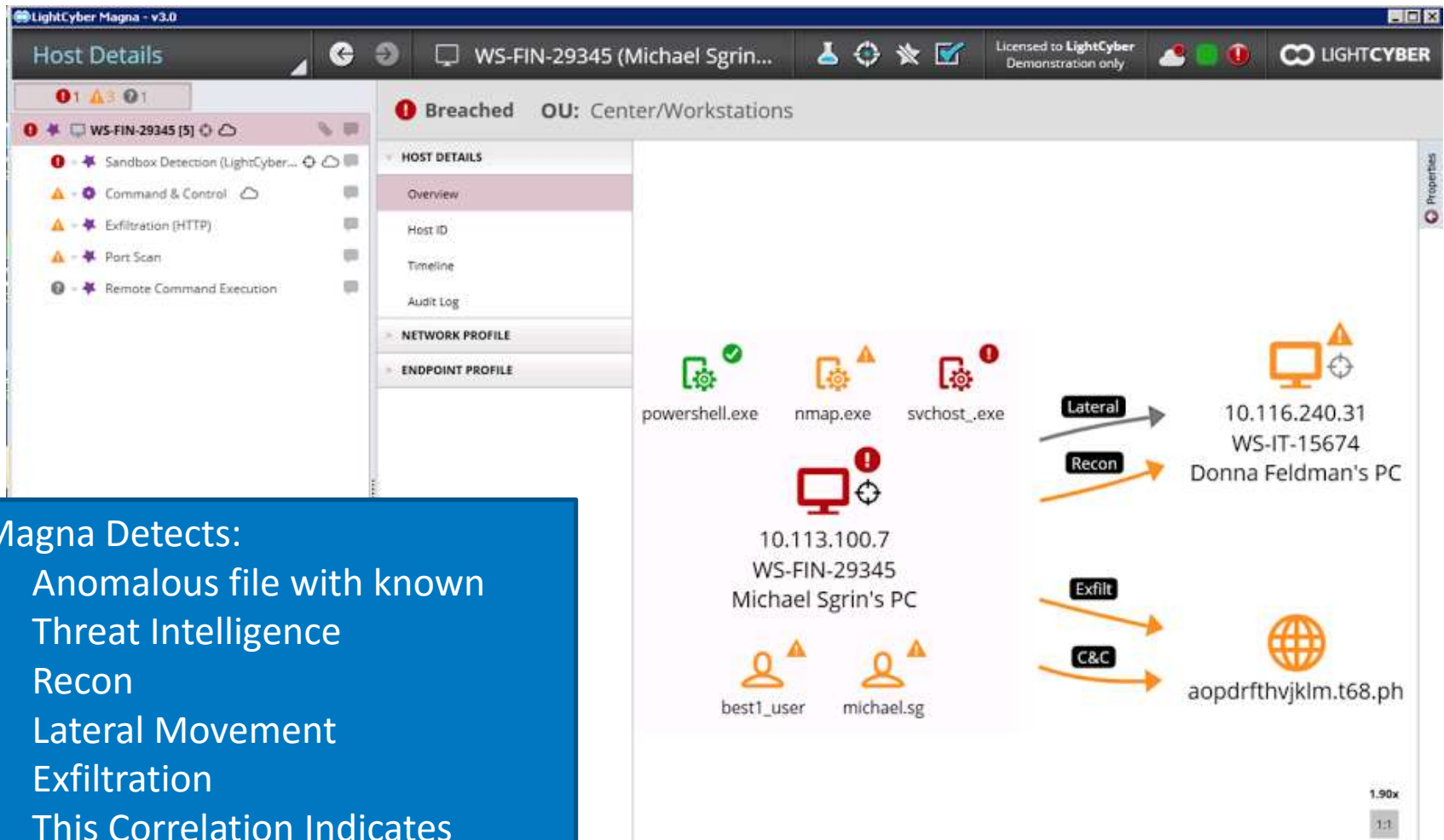
Magna Detects:

- Anomalous Network Activity
- Anomalous and Malicious Processes on the Endpoint
- Anomalous User Activity

Magna Correlates:

- User
- Entity
- Network
- Process
- Endpoint

Targeted Attack Example



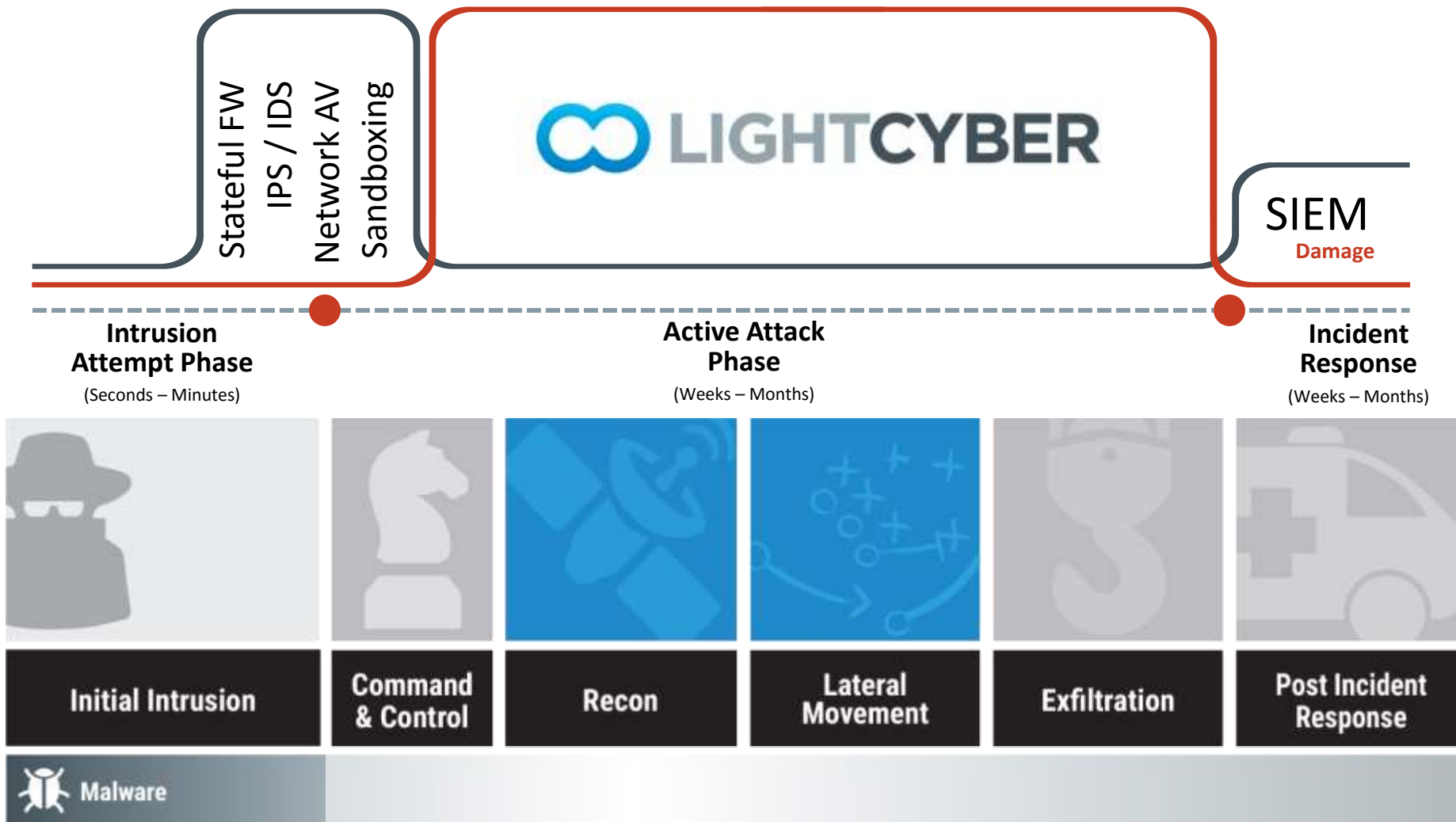
Magna Detects:

- Anomalous file with known Threat Intelligence
- Recon
- Lateral Movement
- Exfiltration
- This Correlation Indicates Targeted Attack

Detection Pattern:

- Multiple Correlated Findings
- North-South + East-West

Evolving IT Security Investment Needs



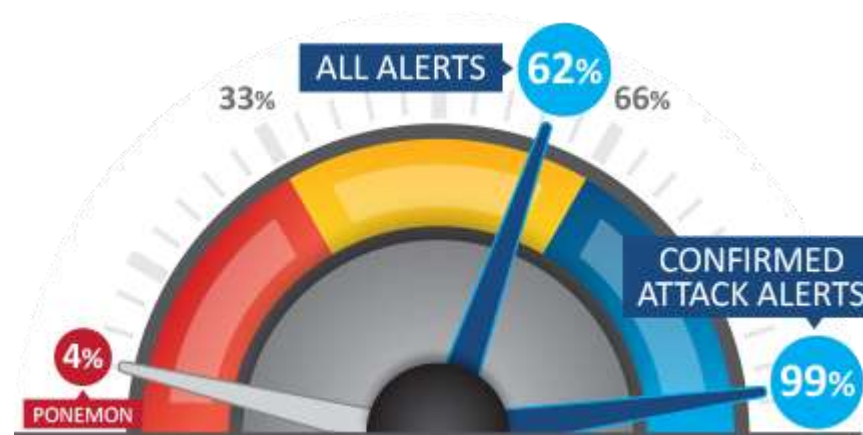
Detecting Attacks Requires Efficiency and Accuracy

Efficiency



Alerts/1k Hosts/Day:
Lower # is Better

Accuracy



% Actionable Alerts:
Higher % is Better

LightCyber Delivers Both Efficiency and Accuracy

Thank You