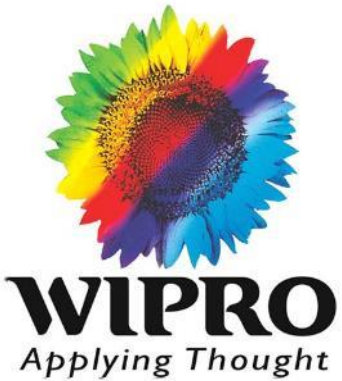


COGNITIVE CYBER DEFENSE

MACHINE LEARNING & APPLIED AI TO UNCOVER UNKNOWN THREATS

MURALI RAO

GLOBAL HEAD, CYBERSECURITY & RISK CONSULTING

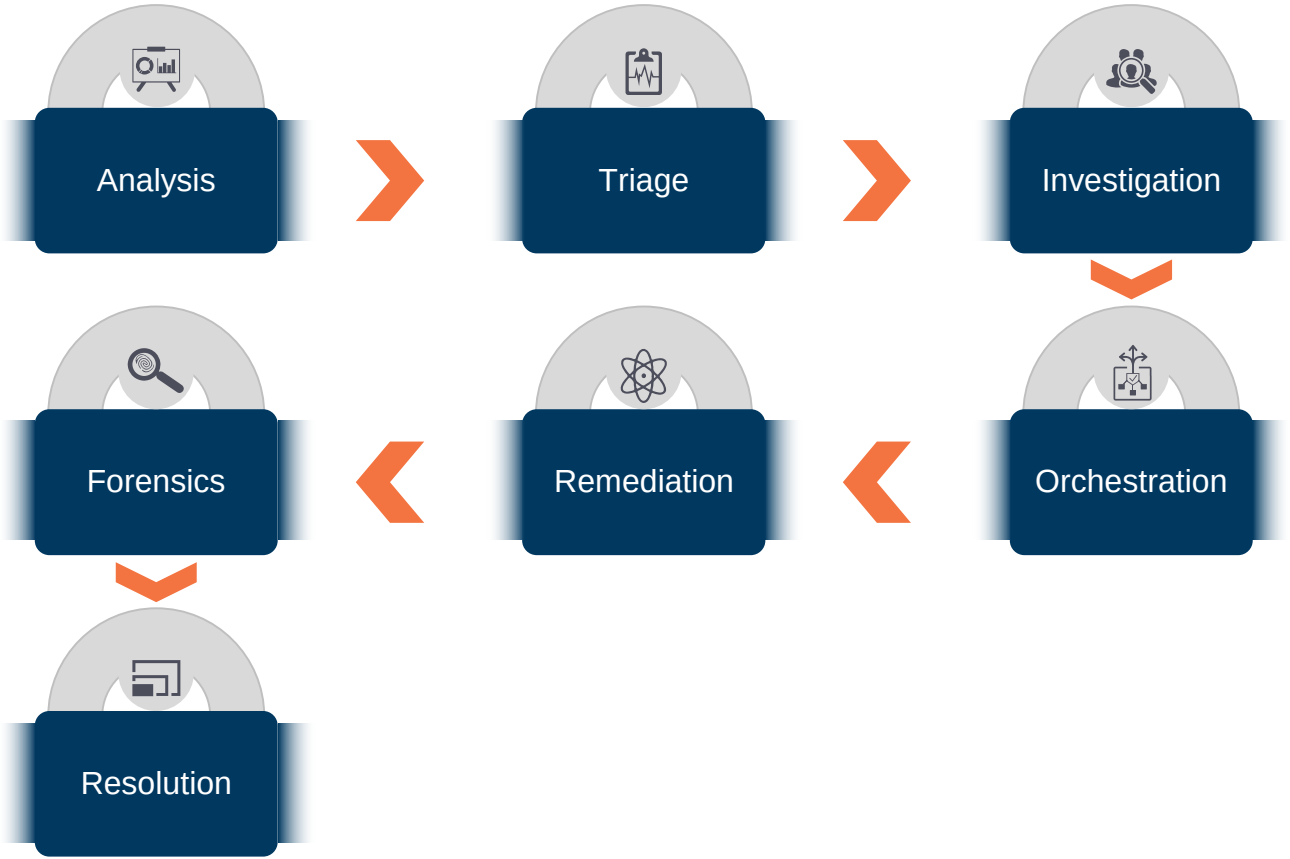
If the “IQ level” of a traditional signature-based antivirus can be compared to that of an insect, then the correlation engine of a modern security analytics solution is about as “smart” as a frog catching flies.

-

Alexei Balaganski, Kuppinger Cole

Security Incident Life Cycle

SECURITY ANALYST

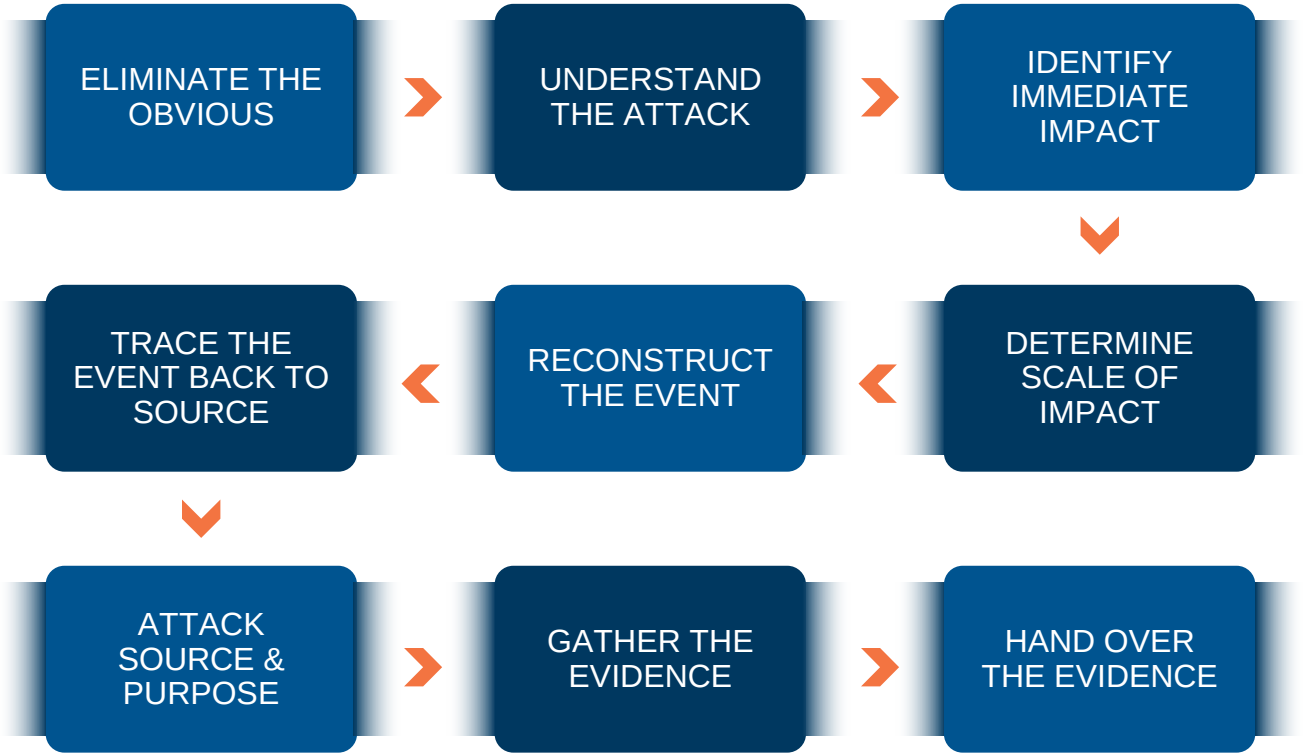


Security Incident Analysis

SECURITY ANALYST

FINDING ANSWERS LOCKED IN **DATA**

OBSERVE
INTERPRET
EVALUATE
DECIDE



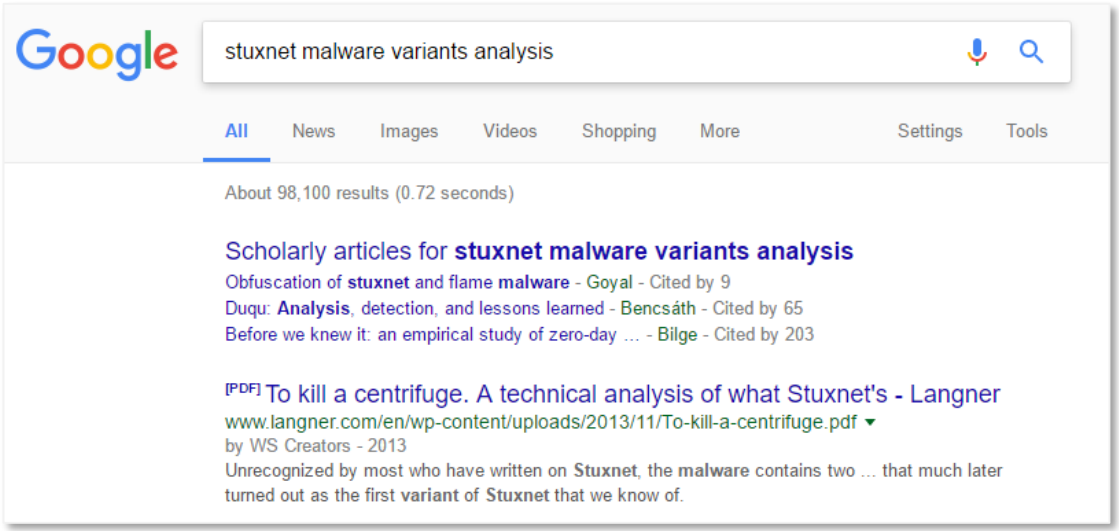
Security Incident Analysis

SECURITY ANALYST

FINDING ANSWERS
LOCKED IN **DATA**

OBSERVE
INTERPRET
EVALUATE
DECIDE

TO ANALYSE UNKNOWN THREATS
MOST SECURITY ANALYSTS START HERE…



Lack of data isn't the problem, there's TOO MUCH of it.

Visible Structured Data

Visible Unstructured Data

Hidden Unstructured Data

Logs, NetFlow, sFlow, PCAP, IPFIX, JDBC, SNMP, Structured Threat Intel, STIX, TAXII, etc.

Blogs, Documents, Articles, Research Papers, Tweets, Forums, News, Analyst Reports, etc.

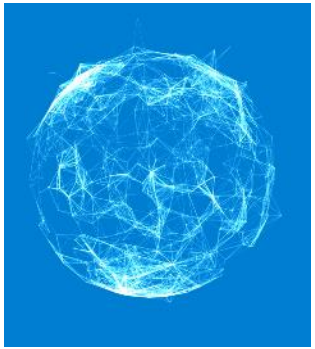
Unstructured Threat Intel

Exploit Kits, Custom Malware, Zero-Day vulnerabilities, User Credentials, Target Lists, Chats, Cyber Criminal Marketplace, Clandestine networks, Hacking groups, Pedophiles, etc.

Baseline our understanding of COGNITIVE SECURITY

COGNITIVE SECURITY

UTILIZES NATURAL LANGUAGE PROCESSING AND MACHINE LEARNING METHODS TO ANALYZE BOTH STRUCTURED AND UNSTRUCTURED SECURITY INFORMATION THE WAY HUMANS DO.



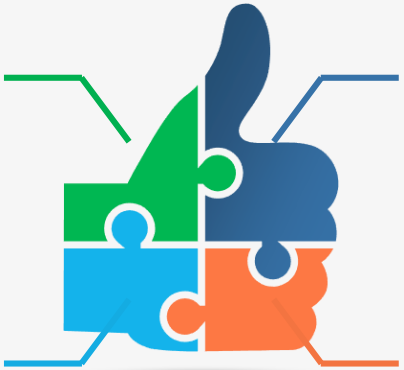
TRAITS OF CANDIDATE FOR COGNITIVE

VOLUME

Huge data size that transforms user experience with contextual relevance and active dialogue

VELOCITY

High-speed acquisition of data and near real-time availability of response.



VERACITY

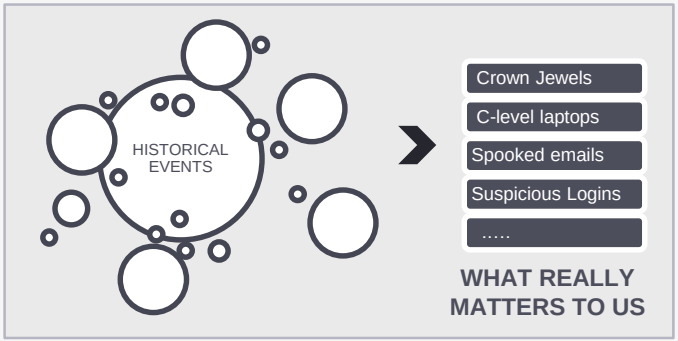
Need for data assurance that leverages evidence-based insights with weighted confidence

VARIETY

Great diversity of data formats & sources that require deep natural language processing

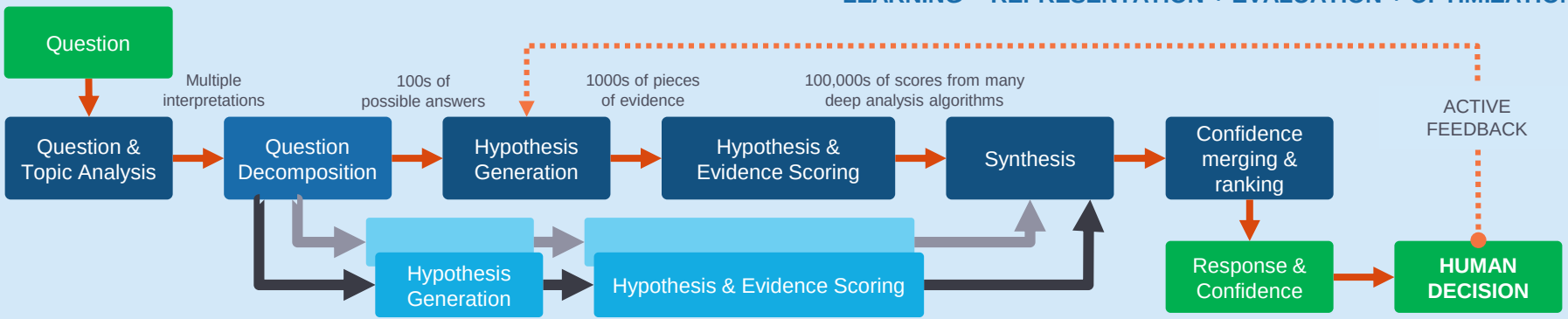
Baseline our understanding of COGNITIVE SECURITY

MAKING COGNITIVE WORK



HOW COGNITIVE WORKS

LEARNING = REPRESENTATION + EVALUATION + OPTIMIZATION

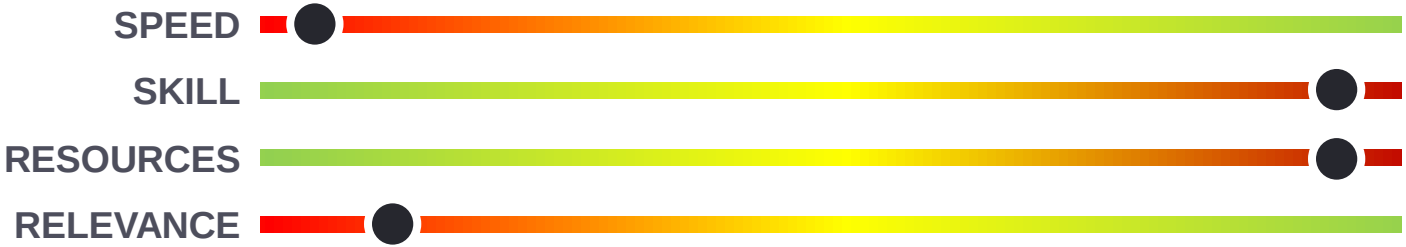


Putting Cognitive Cyber Defense to work… some examples

APPLIES TO MAJORITY OF THE SECURITY INCIDENT ANALYSIS PROCESS

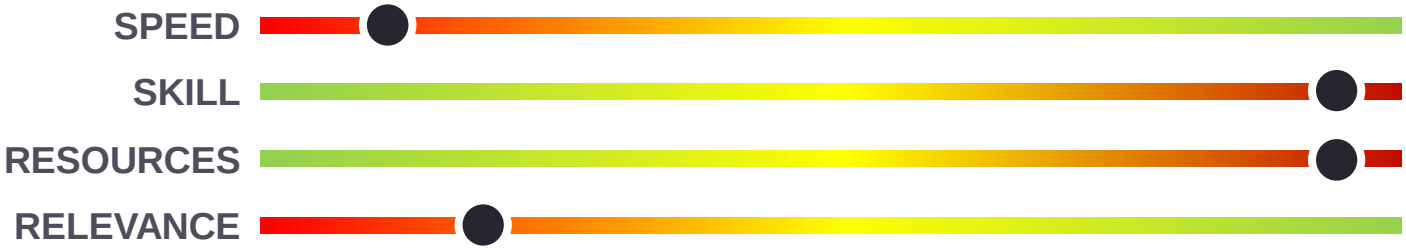
- REDUCE TIME TO BUILD THREAT CONTEXT
- UNCOVER PREVIOUSLY UNKNOWN CONNECTIONS
- REDUCE THE ATTACK SURFACE WITH NEW INSIGHTS
- DISCOVER ATTACKER TOOLS, TACTICS, TECHNIQUES, & PROCEDURES

COGNITIVE CYBER DEFENSE MATURITY



SIEM

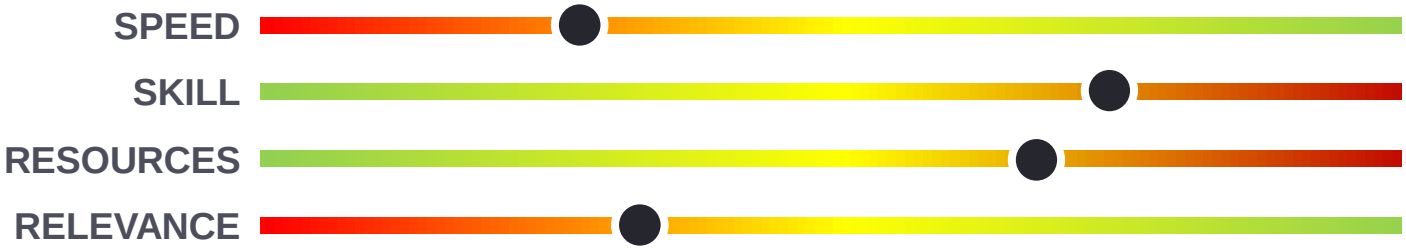
COGNITIVE CYBER DEFENSE MATURITY



STRUCTURED THREAT INTEL

SIEM

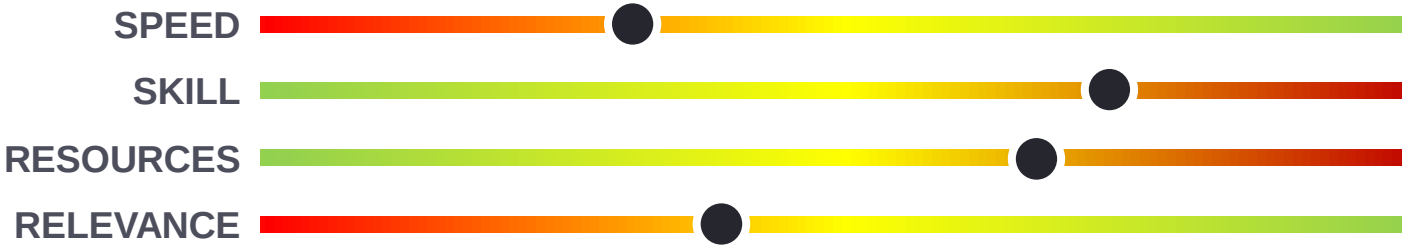
COGNITIVE CYBER DEFENSE MATURITY



STRUCTURED THREAT INTEL

SIEM | **EDR** | **NBAD** | **UEBA**

COGNITIVE CYBER DEFENSE MATURITY



STRUCTURED THREAT INTEL

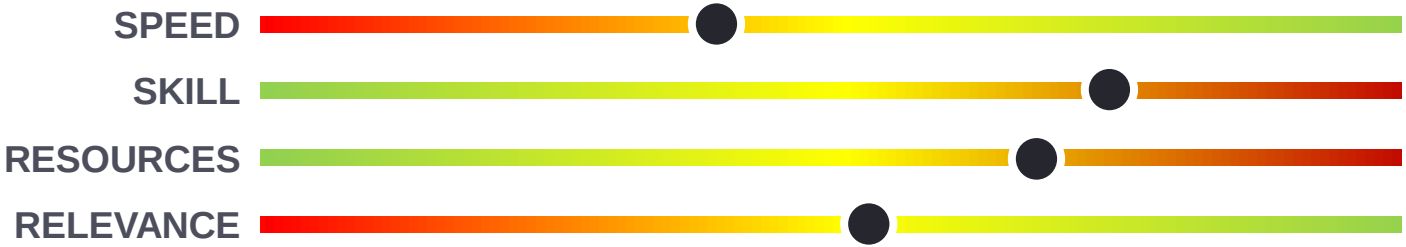
SECURITY DATA LAKE

SIEM

THREAT HUNTING

EDR | NBAD | UEBA

COGNITIVE CYBER DEFENSE MATURITY



UNSTRUCTURED THREAT INTEL

STRUCTURED THREAT INTEL

SECURITY DATA LAKE

BUSINESS CONTEXT

SIEM

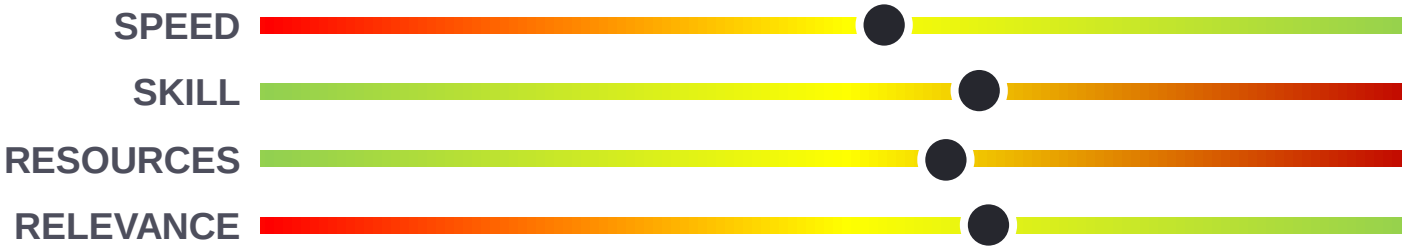
THREAT HUNTING

EDR

NBAD

UEBA

COGNITIVE CYBER DEFENSE MATURITY



UNSTRUCTURED THREAT INTEL

ANALYTICS, INVESTIGATION & FORENSICS

STRUCTURED THREAT INTEL

SECURITY DATA LAKE

BUSINESS CONTEXT

SIEM

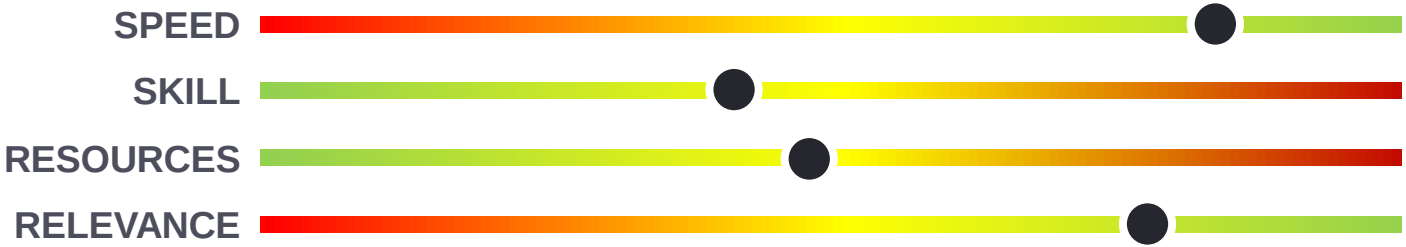
THREAT HUNTING

EDR

NBAD

UEBA

COGNITIVE CYBER DEFENSE MATURITY



UNSTRUCTURED THREAT INTEL

STRUCTURED THREAT INTEL

SIEM

ANALYTICS, INVESTIGATION & FORENSICS

SECURITY DATA LAKE

BUSINESS CONTEXT

THREAT HUNTING

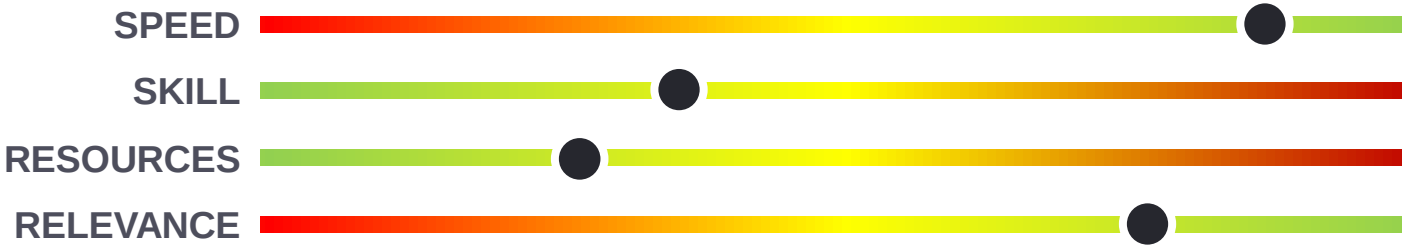
EDR

NBAD

UEBA

COGNITIVE SECURITY PLATFORM

COGNITIVE CYBER DEFENSE MATURITY



UNSTRUCTURED THREAT INTEL

STRUCTURED THREAT INTEL

SIEM

ANALYTICS, INVESTIGATION & FORENSICS

SECURITY DATA LAKE

BUSINESS CONTEXT

THREAT HUNTING

EDR

NBAD

UEBA

COGNITIVE SECURITY PLATFORM

SECURITY ORCHESTRATION & AUTOMATION

Things to ponder on

Security of Cognitive Security

Re-engineering Skills (Hunt, Data Science, etc.)

What happens in a Cloud scenario?

Will Data Lake truly deliver?

WIPRO'S COGNITIVE CYBER DEFENSE ECOSYSTEM

WIPRO HOLMES™
ARTIFICIAL INTELLIGENCE PLATFORM

sqrrl

IBM

DEMISTO

RSA

SecureEye

VECTRA™

hadoop

Intsights

splunk>

cybereason

SECURONIX
Security Analytics. Delivered.

CARBON BLACK

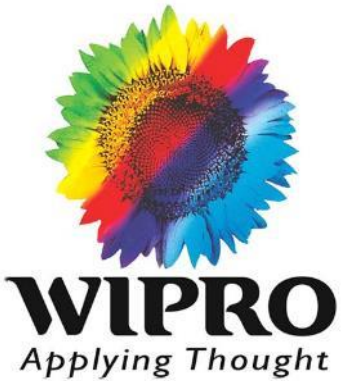
WIPRO CYBERSECURITY & RISK SERVICES

586+ CUSTOMERS
FORTUNE 1000 ENTERPRISES

10 PLATFORMS
FOR CYBER DEFENCE

7500+ PRACTITIONERS
CYBER SEC. & RISK EXPERTISE

VENTURE INVESTMENTS
AND STRATEGIC PARTNERSHIPS



Thank You

MURALI RAO

Global Head, Cybersecurity & Risk Consulting

murali.nagaraja@wipro.com | +1 (650) 224-4571