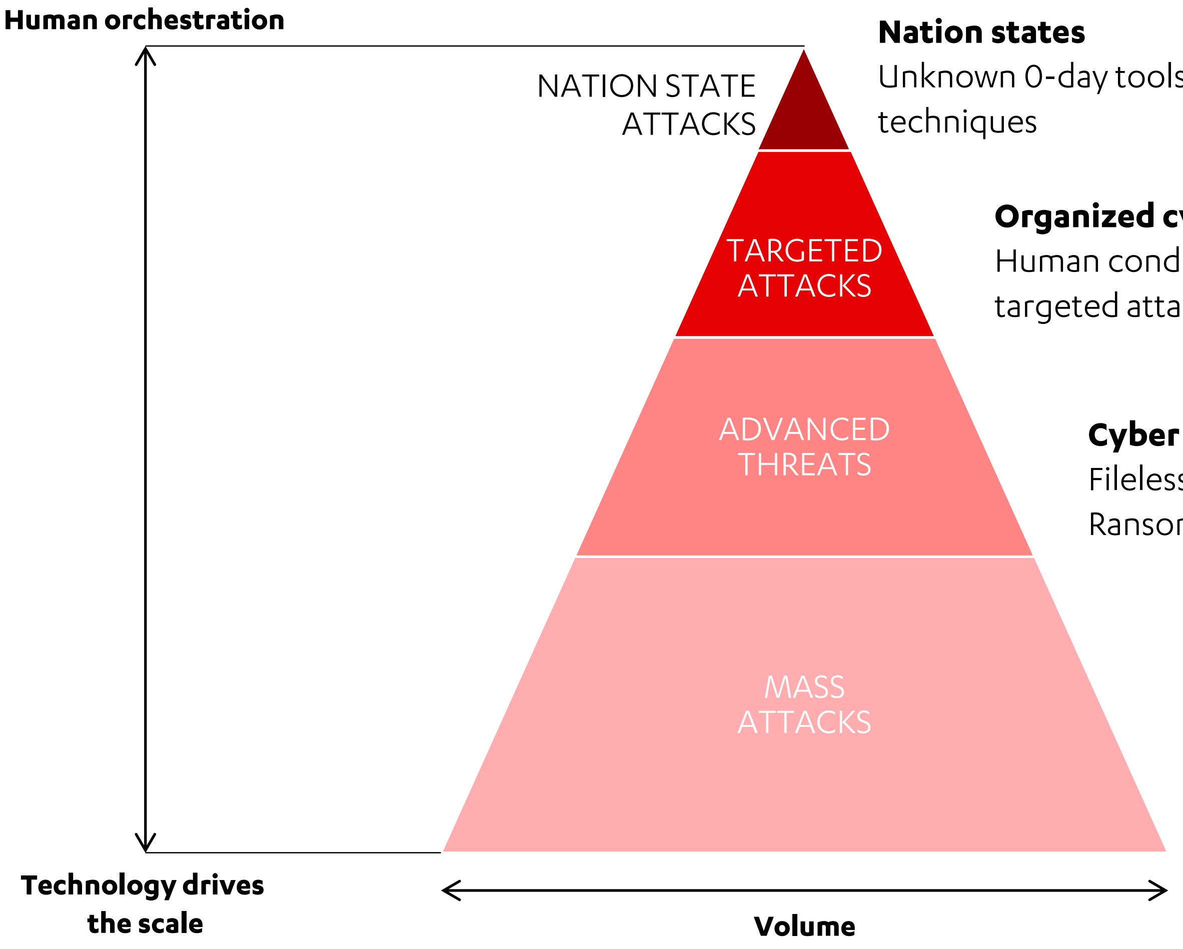
TECHNOLOGY

F-SECURE’S UNIQUE CAPABILITIES IN DETECTION & RESPONSE

Jyrki Tulokas, EVP, Cyber security products & services

F-Secure

UNDERSTANDING THE THREAT LANDSCAPE



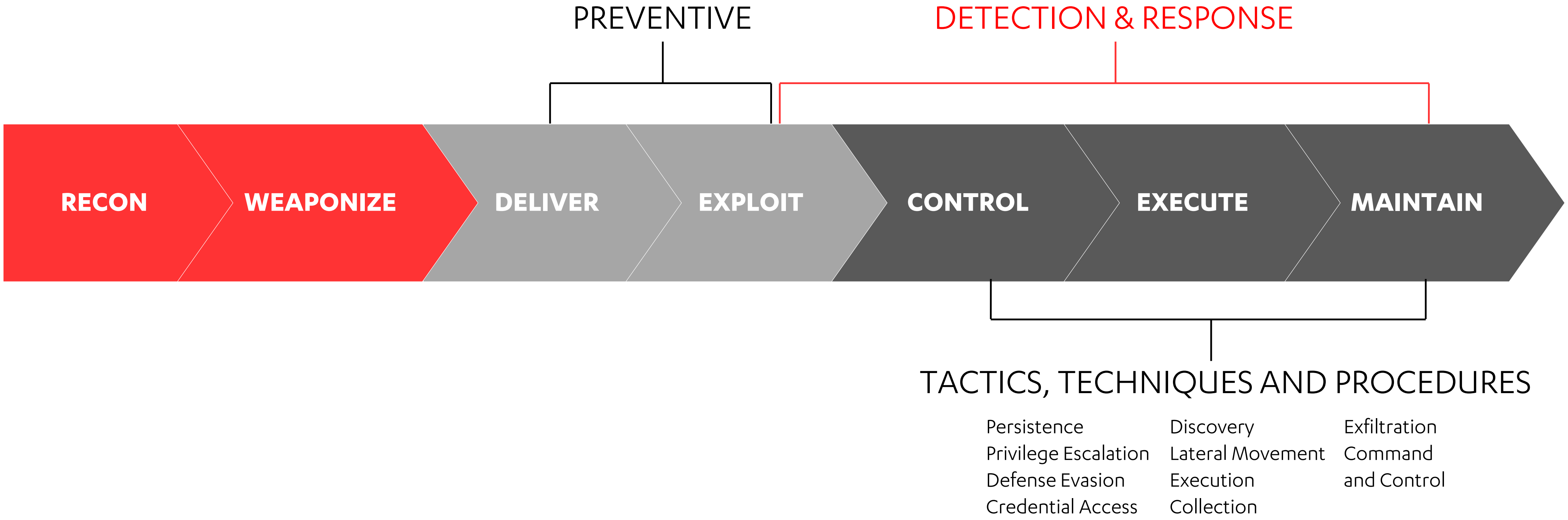
Nation states
Unknown 0-day tools and techniques

Organized cyber crime
Human conducted, stealthy, targeted attacks

Cyber crime
Fileless scripts, System tools, Ransomware

Commodity threats
Opportunistic phishing
Malware
Spam

CUSTOMERS CONTINUE TO NEED BOTH PREVENTIVE AND REACTIVE CAPABILITIES



PREVENTIVE

DETECTION & RESPONSE

RECON

WEAPONIZE

DELIVER

EXPLOIT

CONTROL

EXECUTE

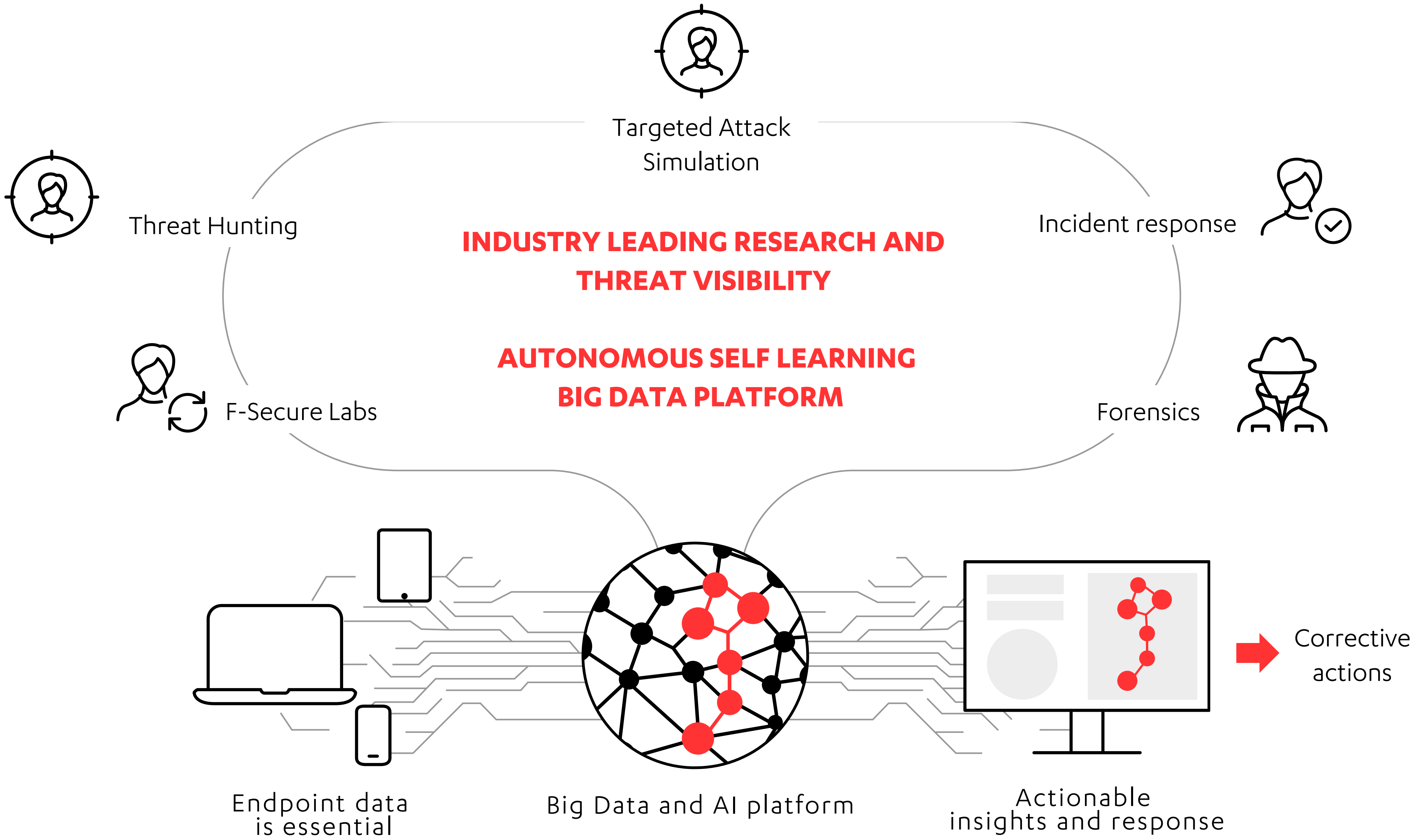
MAINTAIN

TACTICS, TECHNIQUES AND PROCEDURES

Persistence
Privilege Escalation
Defense Evasion
Credential Access

Discovery
Lateral Movement
Execution
Collection

Exfiltration
Command and Control



Targeted Attack Simulation

Threat Hunting

Incident response

INDUSTRY LEADING RESEARCH AND THREAT VISIBILITY

AUTONOMOUS SELF LEARNING BIG DATA PLATFORM

F-Secure Labs

Forensics

Corrective actions

Endpoint data is essential

Big Data and AI platform

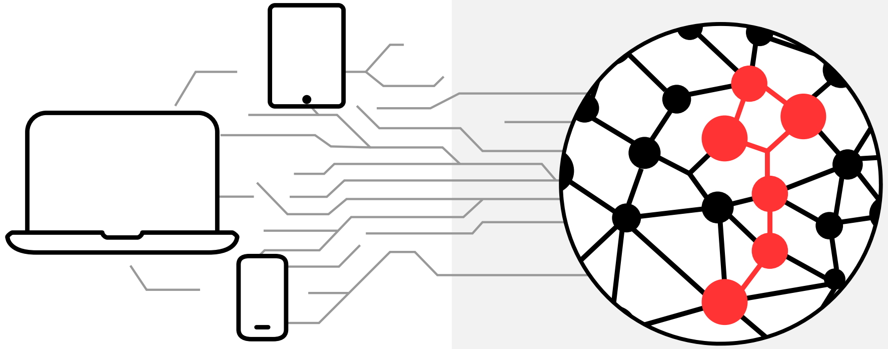
Actionable insights and response

AUTONOMOUS BIG DATA DETECTION & RESPONSE PLATFORM BUILT FOR MASSIVE SCALE

DATA COLLECTION SENSORS

The endpoint sensors collect :

- ✓ file accesses;
- ✓ process creations;
- ✓ network connections;
- ✓ registry writes;
- ✓ system log entries relevant to detecting security breaches;
- ✓ extracts of scripts derived from run-time execution;



66 BN

EVENTS/MONTH

REAL-TIME ANALYTICS IN THE CLOUD

Cloud used for analytics:

- ✓ Machine learning
- ✓ Broad Context Detection ™
- ✓ Automatic analysis, categorization and detection creation
- ✓ Telemetry of the attacks shared in real-time with our security cloud
- ✓ Long-term view to threat propagation

A SELF-LEARNING AI PLATFORM ALREADY PROVEN ON THE MARKET

SUPERVISED ML MODULES

- Detecting threats based on training data
- Learning from expert feedback

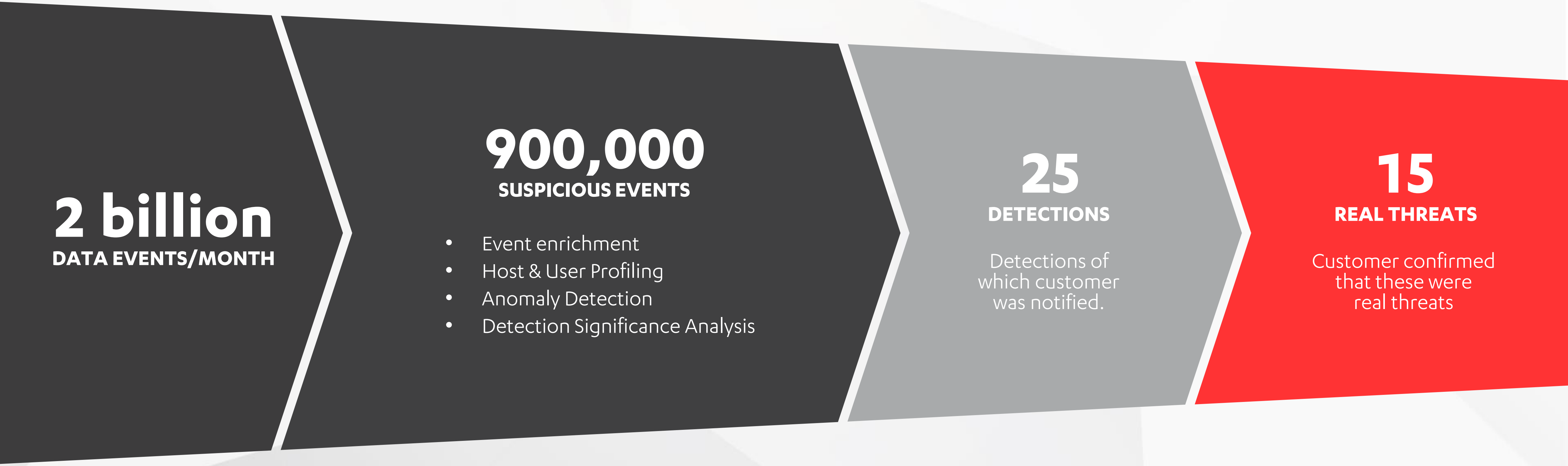
UNSUPERVISED ML MODULES

- User/host profiling
- Anomaly detection

DATA TRANSFORMATION

- Advanced visualization
- Intelligently clusters anomalies

RESULT: INDUSTRY’S FASTEST AND MOST ACCURATE DETECTIONS



2 billion
DATA EVENTS/MONTH

900,000
SUSPICIOUS EVENTS

- Event enrichment
- Host & User Profiling
- Anomaly Detection
- Detection Significance Analysis

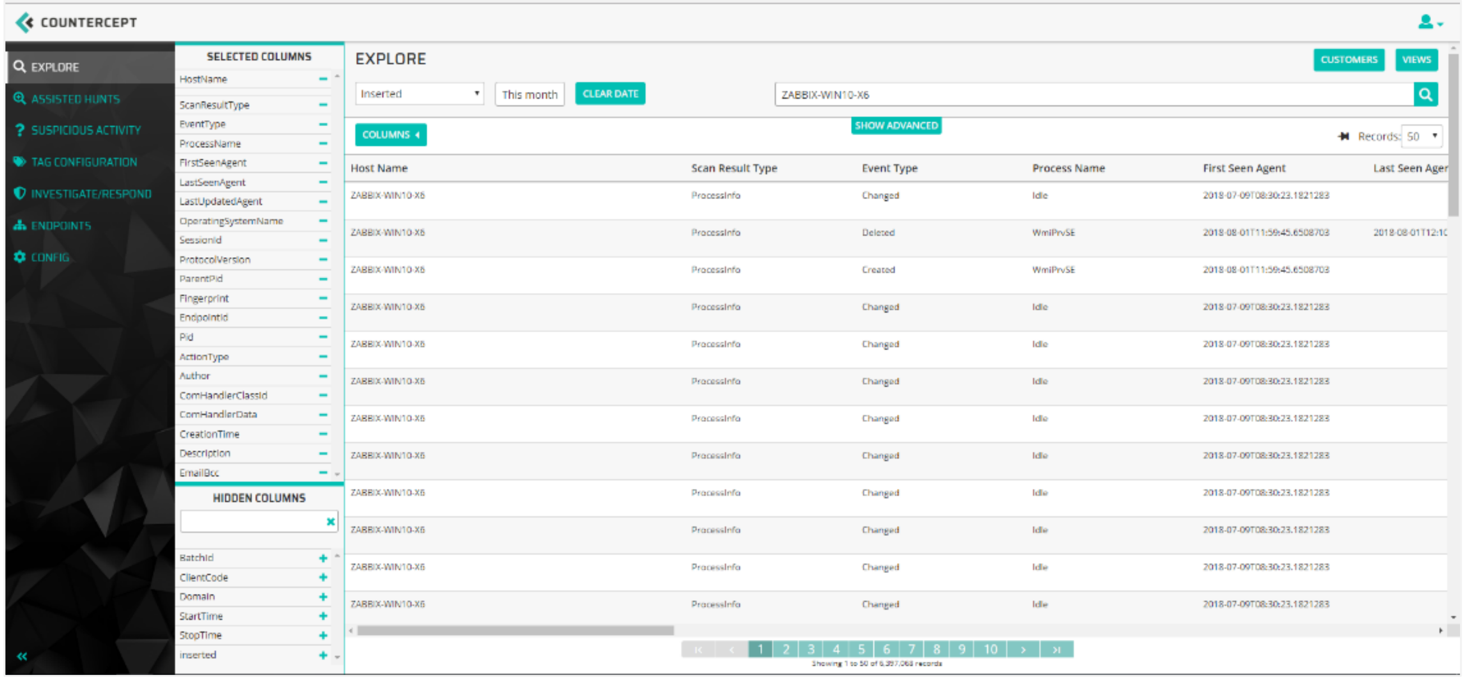
25
DETECTIONS

Detections of which customer was notified.

15
REAL THREATS

Customer confirmed that these were real threats

F-SECURE COUNTERCEPT: HUMAN AUGMENTED TECHNOLOGY, DEEP INSIGHT TO TARGETED ATTACKS



EXPLORE

Inserted | This month | ZABBIX-WIN10-X6

Records: 50

SELECTED COLUMNS: HostName, ScanResultType, EventType, ProcessName, FirstSeenAgent, LastSeenAgent, LastUpdatedAgent, OperatingSystemName, SessionId, ProtocolVersion, ParentPid, Fingerprint, EndpointId, Pid, ActionType, Author, ComHandlerClassId, ComHandlerData, CreationTime, Description, EmailBcc

HIDDEN COLUMNS: BatchId, ClientCode, Domain, StartTime, StopTime, inserted

Host Name	Scan Result Type	Event Type	Process Name	First Seen Agent	Last Seen Ager
ZABBIX-WIN10-X6	ProcessInfo	Changed	Idle	2018-07-09T08:30:23.1821283	
ZABBIX-WIN10-X6	ProcessInfo	Deleted	WmiPrvSE	2018-08-01T11:59:45.6508703	2018-08-01T12:1(
ZABBIX-WIN10-X6	ProcessInfo	Created	WmiPrvSE	2018-08-01T11:59:45.6508703	
ZABBIX-WIN10-X6	ProcessInfo	Changed	Idle	2018-07-09T08:30:23.1821283	
ZABBIX-WIN10-X6	ProcessInfo	Changed	Idle	2018-07-09T08:30:23.1821283	
ZABBIX-WIN10-X6	ProcessInfo	Changed	Idle	2018-07-09T08:30:23.1821283	
ZABBIX-WIN10-X6	ProcessInfo	Changed	Idle	2018-07-09T08:30:23.1821283	
ZABBIX-WIN10-X6	ProcessInfo	Changed	Idle	2018-07-09T08:30:23.1821283	
ZABBIX-WIN10-X6	ProcessInfo	Changed	Idle	2018-07-09T08:30:23.1821283	
ZABBIX-WIN10-X6	ProcessInfo	Changed	Idle	2018-07-09T08:30:23.1821283	
ZABBIX-WIN10-X6	ProcessInfo	Changed	Idle	2018-07-09T08:30:23.1821283	
ZABBIX-WIN10-X6	ProcessInfo	Changed	Idle	2018-07-09T08:30:23.1821283	

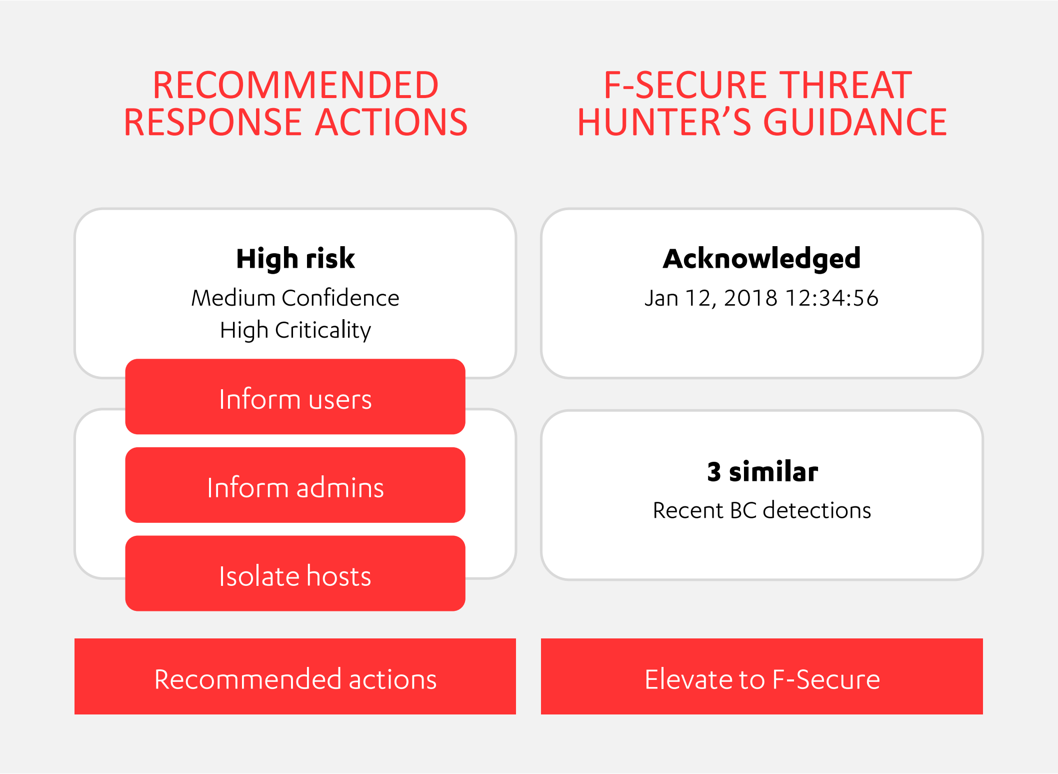
Showing 1 to 50 of 6,397,068 records

The **hunt team** use ‘Explore’ and ‘Investigate/Respond’. They create new ‘assisted hunts’ and tags which propagate to all other instances of THP including those used by our clients and our own 24/7 detection and response team.

AVAILABLE IN THREE MODELS:

- As a service
- Assisted
- Customer specific

TOWARD SELF-HEALING SYSTEMS AND GUIDED RESPONSE



RECOMMENDED RESPONSE ACTIONS

High risk
Medium Confidence
High Criticality

Inform users

Inform admins

Isolate hosts

Recommended actions

F-SECURE THREAT HUNTER'S GUIDANCE

Acknowledged
Jan 12, 2018 12:34:56

3 similar
Recent BC detections

Elevate to F-Secure

- Recommends response actions of informing users, or isolating hosts
- Get help on tough investigations from F-Secure experts with Elevate to F-Secure
- Constantly improves recommendations and detections with machine learning

SUMMARY

- Aiming to be a key player in detection and response technology and services
- Best-in-class integrated cyber security suite
- Scalability through managed services partners
- Security for the cloudified world