

RSA® Conference 2018

Singapore | 25–27 July | Marina Bay Sands

SESSION ID: SEM-W01E

BRINGING AI TO THE CYBERSECURITY BATTLE

Vikas Desai

Cybersecurity Advisor

<https://sg.linkedin.com/in/vikasdesai>

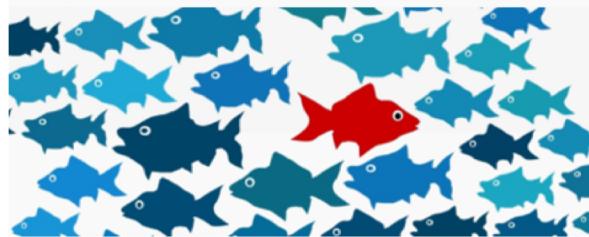


Uses of AI in Security



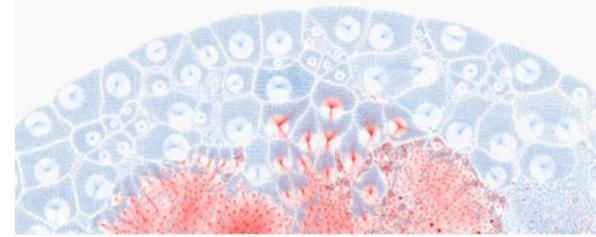
Predictive Analytics

- **Approach:** Model behaviors and identify emerging and past threats and risks
- **Applications:** Network, user, endpoint, app and data, cloud
- **Examples:** Beacons, DNS analytics, user behavior



Intelligence Consolidation

- **Approach:** Curation of intelligence and contextual reasoning
- **Applications:** Structured and unstructured (NLP) data sources
- **Examples:** Intelligence Feeds, Augmented Intelligence



Trusted Advisors & Response

- **Approach:** Reason about security events for triage and response
- **Applications:** Cognitive SOC analyst, orchestration, automation and digital guardian
- **Examples:** SoC Augmentation, SOAR applications



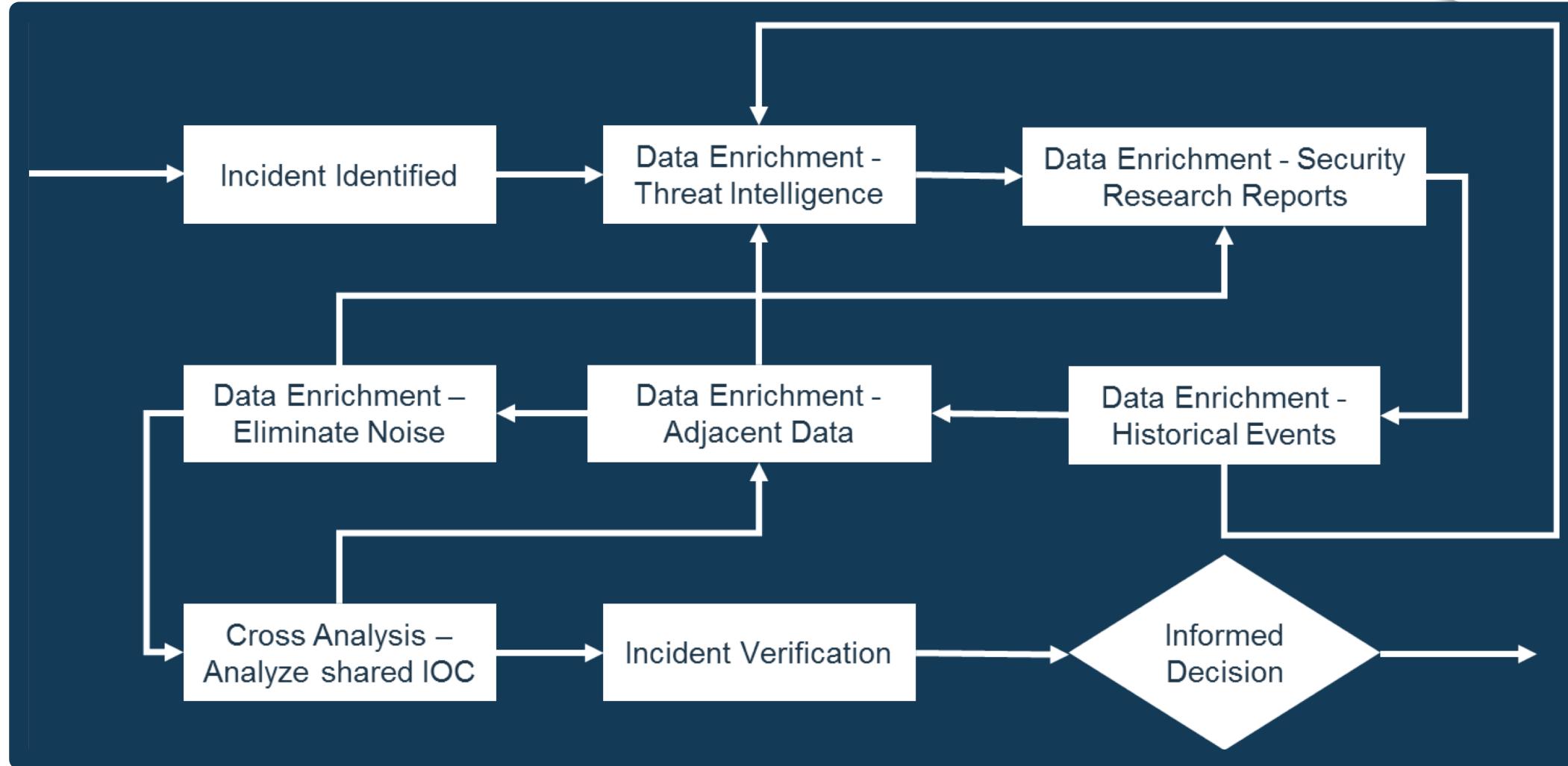
RSA® Conference 2018
Asia Pacific & Japan



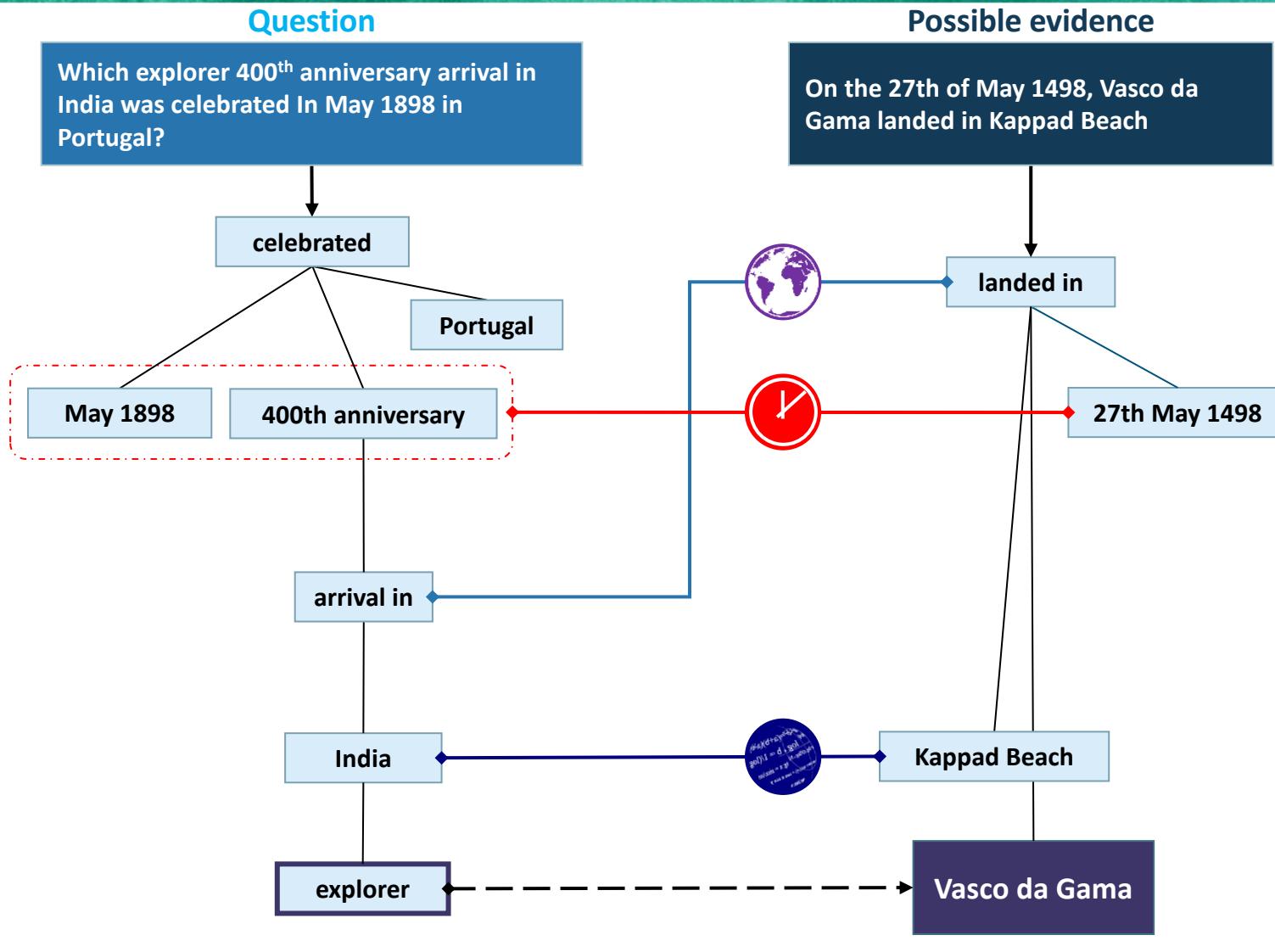
AUGMENTED INTELLIGENCE

Trusted Advisors & Response

Incident Investigation Today

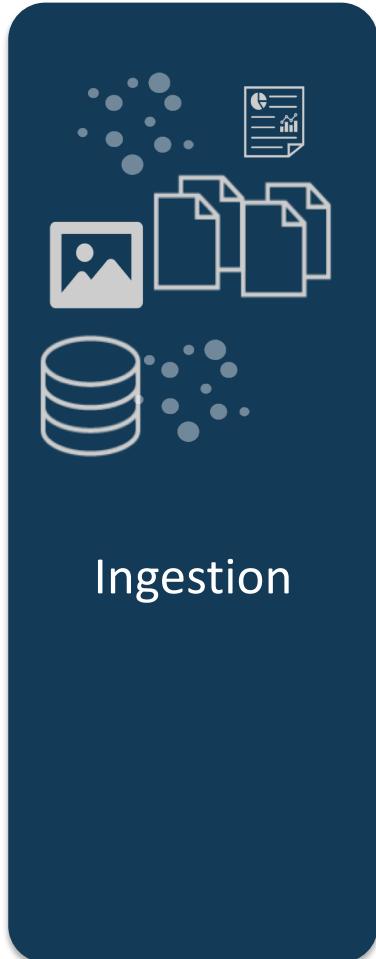


So What Do we Need?

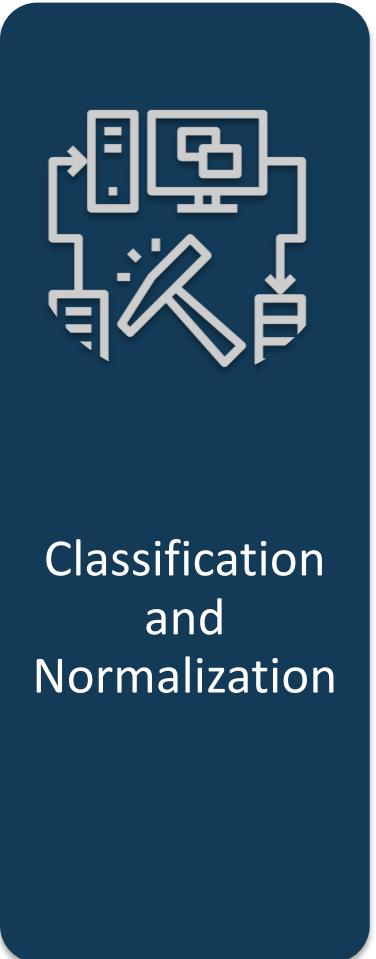


Legend	
➡➡	Temporal Reasoning
➡◆	GeoSpatial Reasoning
◆➡	Statistical Paraphrasing
■	Reference Text
■■	Answer

AI for Cybersecurity



Ingestion



Classification
and
Normalization



Natural
Language
Processing

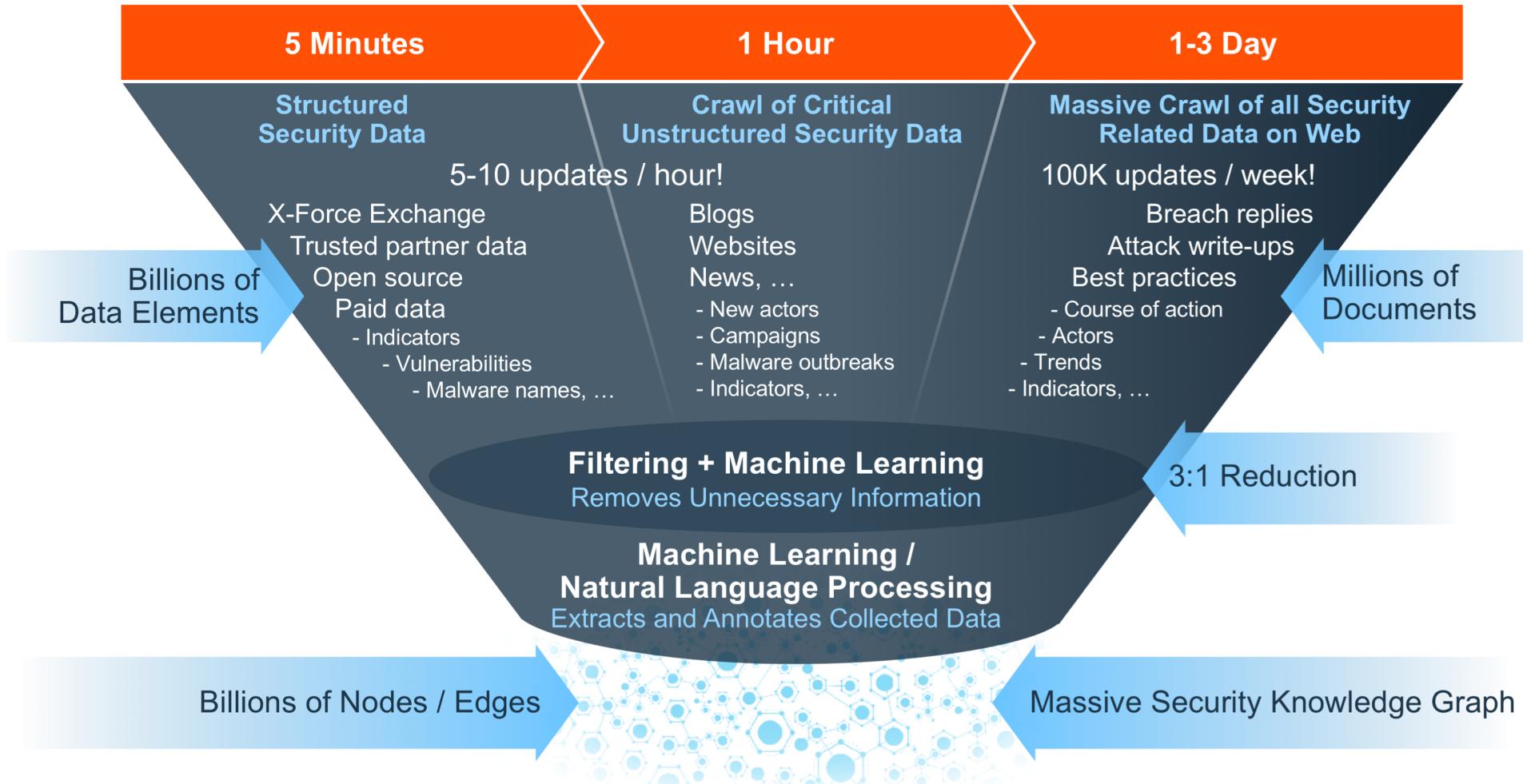


Training and
Learning



Knowledge
Graphs

Ingestion – Building the knowledge



Natural Language Processing / Understanding



User Generated Content: "What's interesting about TSPY_BANKER.YYSI is that it uses the social media network Pinterest in its command and control (C&C) routines. The comments, which look something like "104A149B245C120D," are decoded (by replacing letters with a dot) and the result is an IP address for the server hosting the phishing page. This tactic allows cybercriminals to quickly change the location of their servers in order to avoid detection, Trend Micro said in a blog post...the attackers leveraged exploits for two patched Internet Explorer vulnerabilities, CVE-2013-2551 and CVW-2014-0322"

Watson understands: TSPY_BANKER.YYSI [MALWARE] it [MALWARE REFERENCE] its [MALWARE REFERENCE] command and control (C&C) routines. Instead of contacting a C & C server, the Trojan [MALWARE] accesses comments ...which look something like "104A149B245C120D" [INDICATOR].

Site : <https://www.securityweek.com/banking-trojan-abuses-pinterest-cc-routines>

Training and Learning



IBM Watson Knowledge Studio

Completed Close

Alpha... 14pt

Mention Relation Coreference

The malware targets the websites of Hana Bank, Nonghyup Bank, the Industrial Bank of Korea (IBK), Shinhan Bank, Woori Bank, Kookmin Bank, and the Consumer Finance Service Center, Trend Micro said. When users visit one of these websites, the malware injects an iframe that loads a corresponding phishing page. These phishing sites are designed to look just like the bank's legitimate website, and the threat is capable of spoofing the URL in the Web browser's address bar to avoid raising any suspicion. In addition to the bank websites, TSPY_BANKER.YYSI also targets a popular South Korean search engine. When victims visit this site, they are presented with a pop-up window containing links to the websites of banks monitored by the malware. The redirection to the phishing pages only occurs when users visit the banking websites with Internet Explorer. However, this isn't a problem since an outdated South Korean law requires citizens to bank and make online purchases with Internet Explorer. Statistics show that 75% of the country's Web usage involves this browser. What's interesting about TSPY_BANKER.YYSI is that it uses the social media network Pinterest in its command and control (C&C) routines. Instead of contacting a C&C server, the Trojan accesses comments posted on Pinterest. The comments, which look something like "104A149B245C120D," are decoded (by replacing letters with a dot) and the result is an IP address for the server hosting the phishing page. This tactic allows cybercriminals to quickly change the location of their servers in order to avoid detection, Trend Micro said in a blog post. In one of the attacks analyzed by the security firm, the attackers leveraged exploits for two patched Internet Explorer vulnerabilities, CVE-2013-2551 and CVE-2014-0322, to deliver the malware. The exploit code is heavily obfuscated, but researchers have determined that it's similar to Sweet Orange, an exploit kit that has been used in several campaigns over the past period. This month, the cybercriminals have leveraged the Gongda exploit kit and a Windows vulnerability (CVE-2014-6332) patched by Microsoft last month.

Type	Subtype
c	CAMPAIGN
r	COURSE_OF_ACTION
e	EXPLOIT_TARGET
i	IDENTITY
m	MALWARE
x	RESOURCE
-	SENT
t	THREAT_ACTOR

Cognitive SoC



Accelerated Analysis

- Uses AI to analyze real-time incidents for triage
 - Automatically investigates evidence for an alert or anomaly against Watson and applies 'reasoning' to identify the likely threat
- Gathers external and internal threat indicators from alert
- Performs external (threat intelligence research) and internal research on indicators and entities (hash, domain, IP, users, filename etc.)
- Highlights the existence and identity of threat or outliers
- Offers natural language search bar for security only information to speed up assessment

Intelligent Investigation

- Identifies if communication with threat has occurred or was blocked
- Highlights if malware has executed
- Identifies criticality of systems impacted in incident and shows high value assets
- Gives visibility to higher priority risks and threats from insiders
 - Integrated with User Behavior Analytics (UBA) app to show user's risk scores
 - Reveals previous behaviors and actions of users
- Connects other threat entities from original offense to show relationship
- Provides input for ad-hoc investigation against collections of users and entities

Faster Response

- Provides pertinent information to take action on escalation
- Performs automatic hunting for indicators
- Exports threat and indicators to IR process for remediation and/or blocking
- Automatically adds additional discovered threat indicators to watch lists to reduce risk of missing threats

RSA® Conference 2018
Asia Pacific & Japan



USER BEHAVIOR

Predictive Analytics

The connected world has created new challenges



Customers want convenient mobile, online and cross-channel access

Threat mitigation can impact customer experience



New, faster transactions can create new risks

Customers' Value Drivers – Predictive Analytics



- Improve Customer Experience
 - Reduce user friction
 - Proactive fraud prevention
 - Faster dispute resolutions
- Strengthen authentication
 - Detection of Account Take Over, Remote Access Tools...
 - Real-time fraud detection
 - Continuous and Invisible passive user authentication
- Cost Reduction
 - Improve true positive detection rates (less fraud)
 - Reduce false positive detection rates (less work)
 - Faster fraud dispute resolutions (less fraud and less work)

Let's look at Keystroke Dynamics



Key Usage

Pattern Attributes Collection(JS Collectors)

- Capitalized letters(shift/caps lock)
- Changes(Delete/Backspace)
- Control Combinations(language)
- Traversing fields
- Pasting(Ctrl-V/right click)
- General Movements

Key Strokes

Pattern Attributes Collection(JS Collectors)

- Typing speed
- Dwell Time
- Flight Time
- Digraph patterns
- Trigraph Patterns
- Total Keystrokes

Let's look at Keystroke Dynamics



User Name

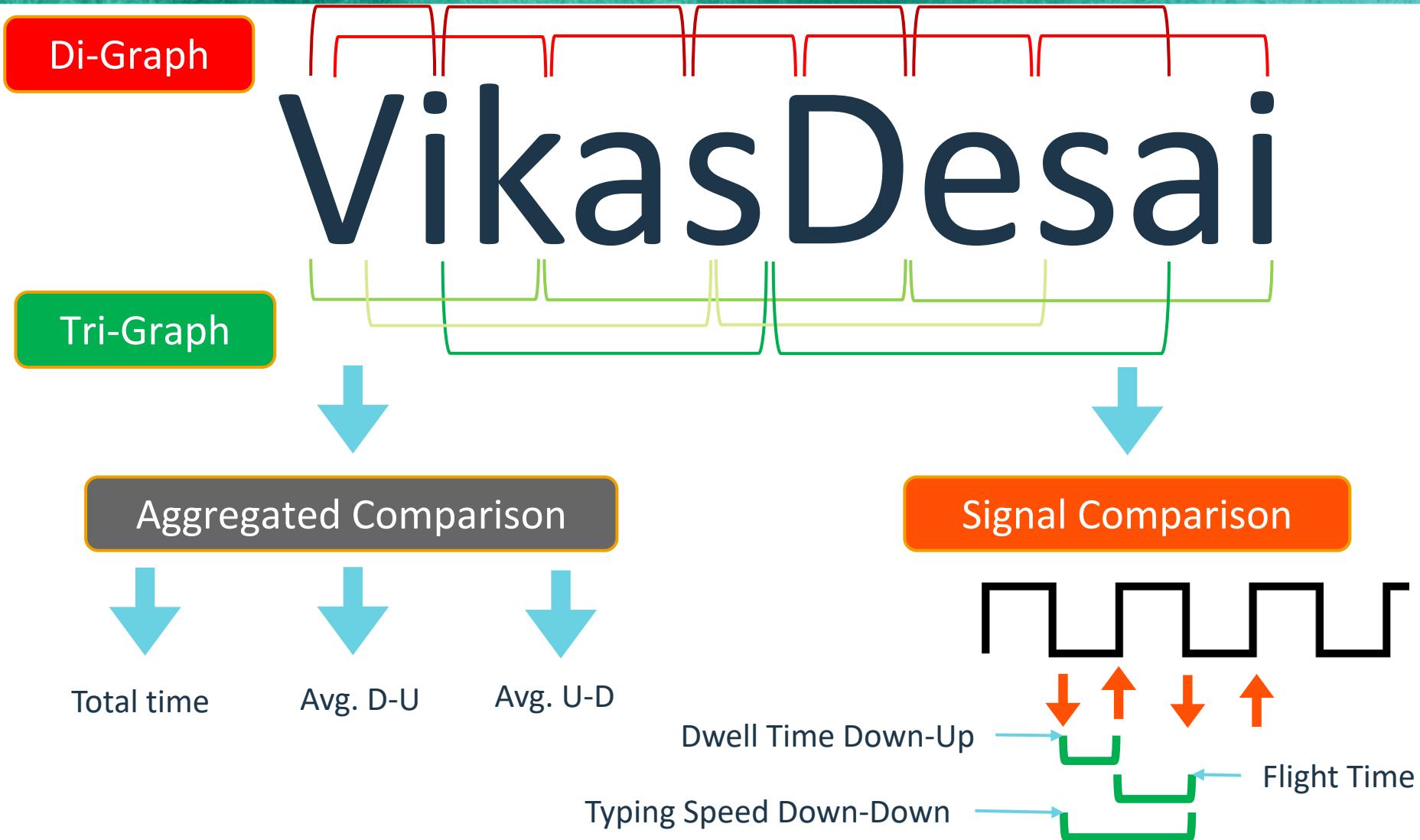
VikasDesai

Password

Security2018



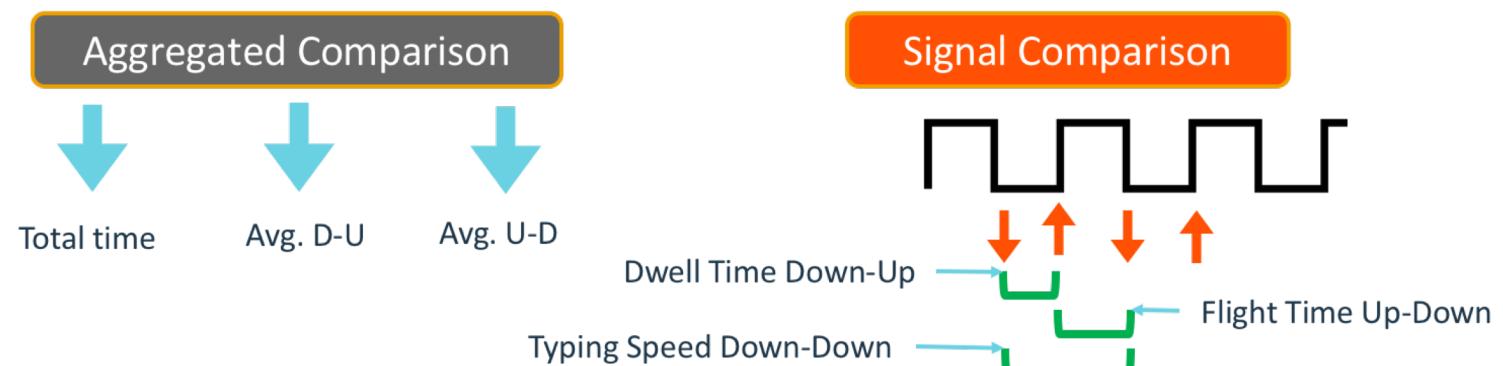
Let's look at Keystroke Dynamics



Feature Engineering



- Dwell Time – The amount of time a key stays pressed
 - Down-Up (DU)
- Flight Time – The amount of time needed to release the previous key and press the next key
 - Up-Down (UD)
- Typing Speed – The amount of time between 2 key presses
 - Down-Down (DD)
- Average Dwell time
- Average Flight Time
- Average Typing Speed



RSA® Conference 2018
Asia Pacific & Japan



DEMO

Keystroke Dynamics

<https://vikasdesai.github.io/keystroke-dynamics/>



Learn + Explore = Apply

Educate yourself

Stay informed

Leverage AI to secure
yourself

<https://vikasdesai.github.io>

<https://www.ibm.com/security/artificial-intelligence>

<https://github.com/IBM/adversarial-robustness-toolbox>