

Advanced Threats Detection

Machine Learning Approach

Petr Cernohorsky
Security Business Group
November 2017

It's not If, it's When

DynDNS attack *"A massive cyberattack knocked out major websites across the internet"*

-Business Insider

"CryptoLocker bursts onto scene again, targeting Europe and U.S."

- SC Magazine

"Worse than WannaCry... Nyetya is deemed worse than WannaCry mainly because it spreads laterally, meaning it targets computers within networks and affects even systems that have been patched."

- TechAdvisory.org



New Cyber Threat Reality



Your environment
will get breached



You'll most likely be
infected via email



Hackers will likely
command and control
your environment via web

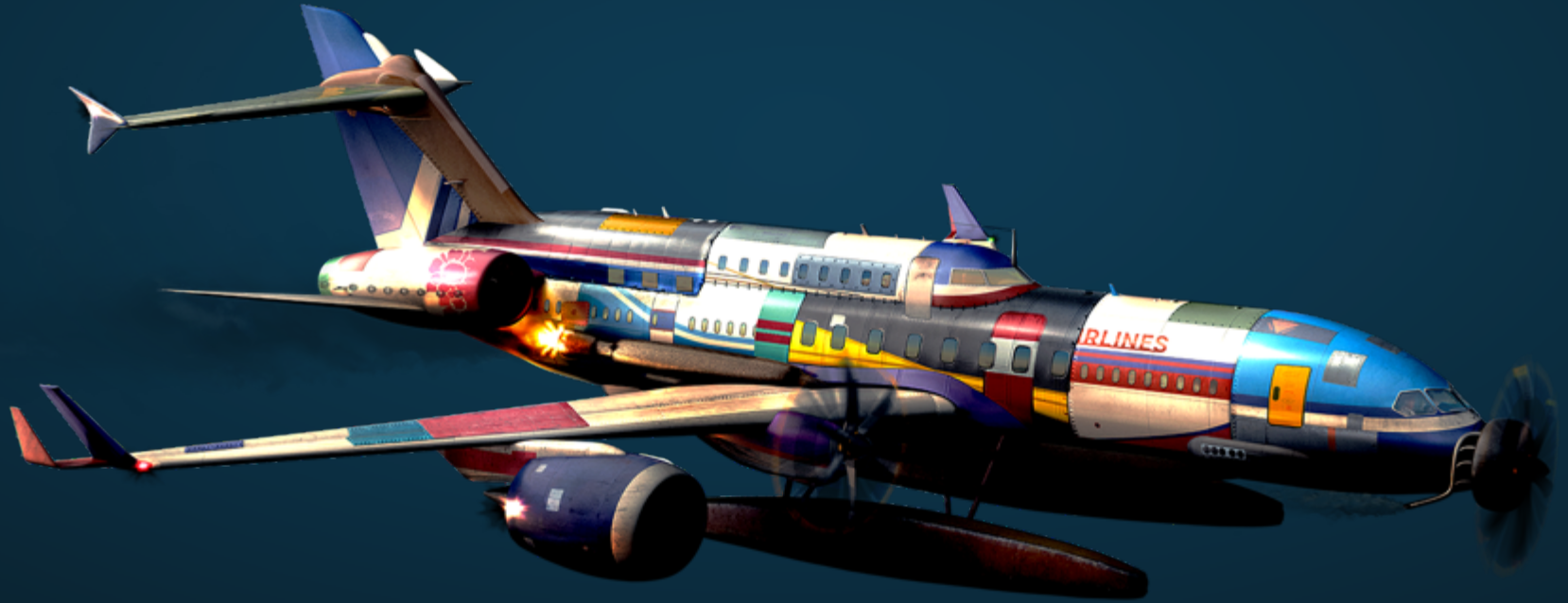
A vendor buffet is not a strategy

The image displays a comprehensive grid of security vendor logos, organized into 15 distinct categories. Each category is represented by a black header box with white text. The logos themselves are small, colorful icons of various companies, densely packed within each category box. The categories include:

- Network Security:** Network Firewall, Network Monitoring/Forensics, Intrusion Prevention Systems, Unified Threat Management.
- Endpoint Security:** Endpoint Prevention, Endpoint Detection & Response.
- Application Security:** WAF & Application Security, Vulnerability Assessment.
- Managed Security Service Provider:** A collection of various MSSP logos.
- Web Security:** Various web security and proxy logos.
- Messaging Security:** Logos for email and messaging security.
- Risk & Compliance:** Logos for risk management and compliance.
- Security Operations & Incident Response:** Logos for SIEM and incident response.
- Threat Intelligence:** Logos for threat intelligence and analysis.
- Specialized Threat Analysis & Protection:** Logos for specialized threat analysis.
- Data Security:** Logos for data protection and security.
- Mobile Security:** Logos for mobile device security.
- Identity & Access Management:** Logos for IAM solutions.
- Cloud Security:** Logos for cloud security solutions.
- Industrial / IoT Security:** Logos for industrial and IoT security.
- Fraud Prevention / Transaction Security:** Logos for fraud prevention and transaction security.

Notably, the 'Security Operations & Incident Response' category features a large, prominent logo for **Momentum CyberScape - 2017** in the center. The overall layout is a dense, multi-colored mosaic of corporate branding.

No algorithm needed to figure out
how ineffective this is!



Cisco Security Architecture

Threat intelligence - **TALOS**



Network



Endpoint



Cloud

Services

1% of Customer Devices Are Infected



Sample report demonstrating an advanced threat visibility gap: <http://cognitive.cisco.com/preview>

Cognitive Threat Analytics (CTA)

10B

requests
per day

Early Detection & Response with Artificial Intelligence

50K

incidents
per day



Anomaly
detection



Trust
modeling



Event
classification



Relationship
modeling

Anomalous
Traffic

Malicious
Events

Threat
Incidents

Attacks Use Encrypted Traffic



80%

of organizations
are victims of
malicious activity

41%

of attacks used
encrypted traffic to
evade detection

Malware Detection

Cisco Research



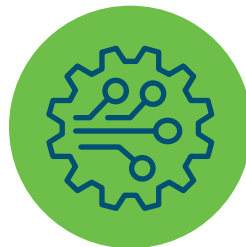
Known
Malware Traffic



Known
Benign Traffic



Extract Observable
Features in the Data



Employ Machine
Learning techniques
to build detectors



Known Malware
sessions detected
in encrypted traffic

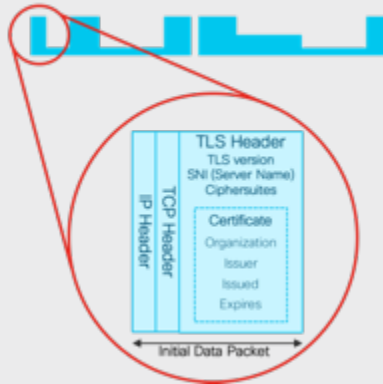
“Identifying Encrypted Malware Traffic with Contextual Flow Data”

AI Sec '16 | Blake Anderson, David McGrew (Cisco Fellow)

How can we inspect encrypted traffic?

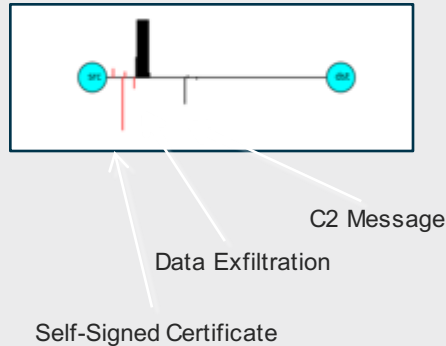
Initial Data Packet

Make the most of the unencrypted fields



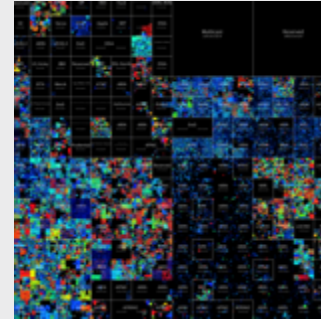
Sequence of Packet Lengths and Times

Identify the content type through the size and timing of packets



Global Risk Map

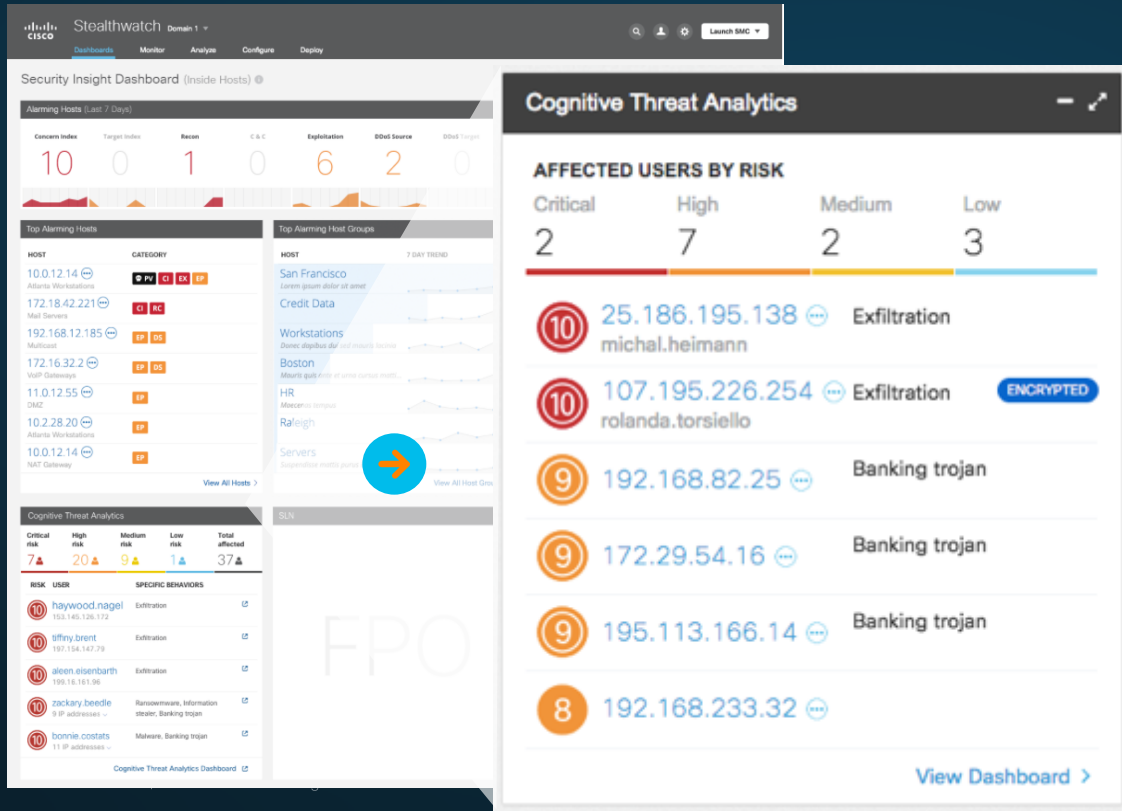
Who's who of the Internet's dark side



Broad behavioral information about the servers on the Internet.



Encrypted Traffic Analytics



Detect malware without decryption

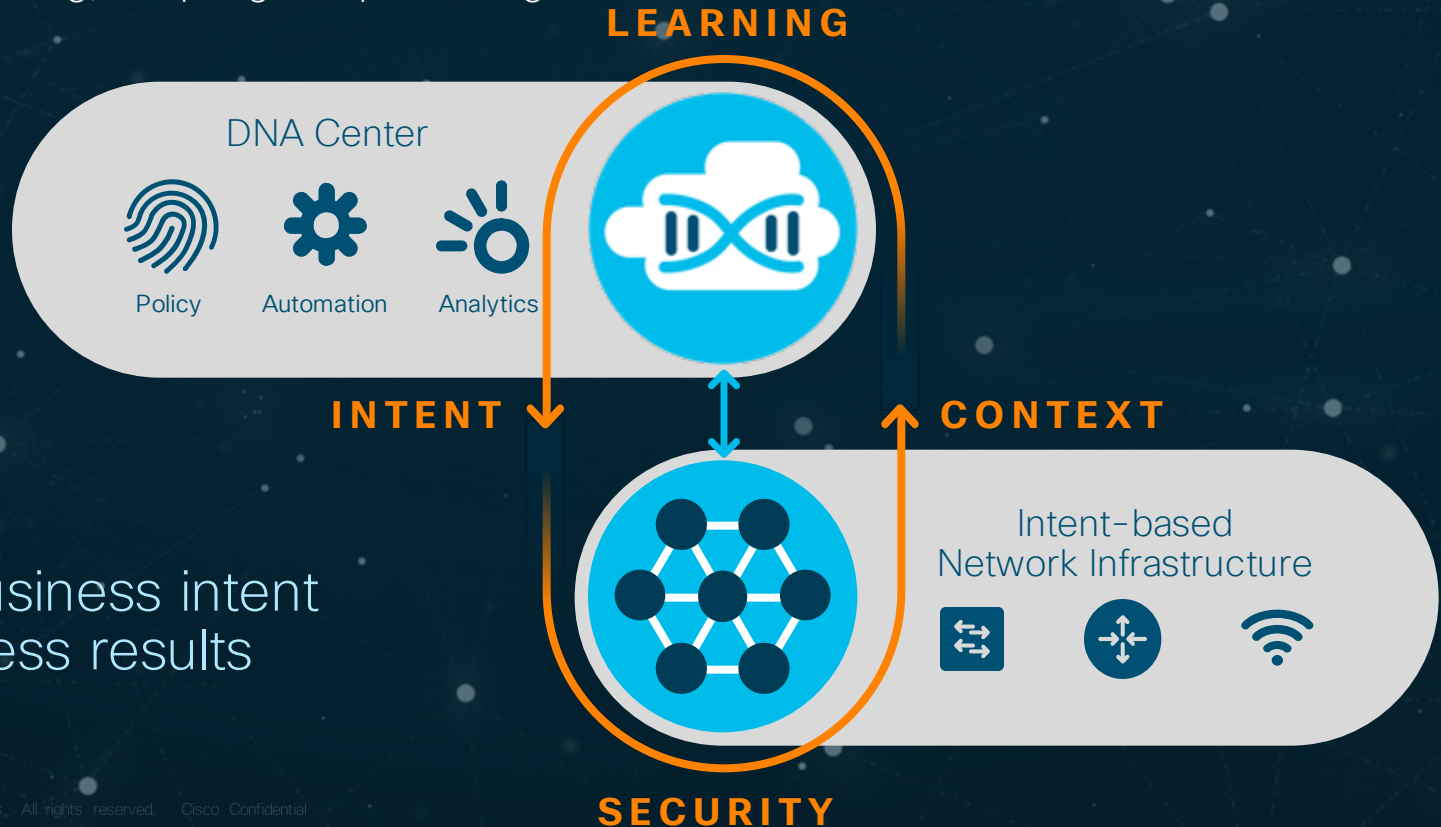
... through

MACHINE LEARNING &

correlation of global threat behaviors

The Network. Intuitive.

Constantly learning, adapting and protecting.



Turns business intent
to business results

