DARKTRACE

Enterprise Immune System:

La nuova generazione della Cyber Defense

- Fondata da matematici di prim'ordine, da specialisti nel campo del 'machine learning' e da esperti dell'intelligence a livello governativo
- Vincitore del prestigioso premio 'Enterprise Start-up of the Year' al Techworld Awards 2014
- Menzione speciale all'Institute of Engineering and Technology Innovation Awards 2014
- Basata su innovativi studi della matematica probabilistica di Bayes
- Centro di Ricerca e Sviluppo di prim'ordine a Cambridge (UK)
- Oltre 50 installazioni: energia, telecomunicazioni, servizi finanziari, commercio al dettaglio e trasporti
- Tecnologia di comprovata efficacia

"a new generation of cyber security company"
- *Financial Times*

2014 TECHWORLD AWARDS

2014 Computing Security Awards ★ FINALIST ★

IET AWARDS The Institution of Engineering and Technology

SC MAGAZINE 2014 Europe AWARDS FINALIST

Il Team di Darktrace

Comitato esecutivo

Nicole Eagan, CEO

25 anni di esperienza nella tecnologia; è stata CMO di Peregrine, Quest, Verity ed Autonomy. Esperta di strategie per le aziende in rapida crescita e nello sviluppo dei mercati

Jim Penrose, EVP

17 anni all'NSA, dov'è stato Direttore (Defense Intelligence Senior Level); esperto a livello mondiale sulle minacce interne; nominato nel 2013 per il premio Presidential Rank

Jack Stockdale, CTO

Specialista nell'applicazione della matematica Bayesiana ai dati, su larga scala; è stato Direttore Tecnico di Autonomy e Direttore della Ricerca e Sviluppo di Blinkx

Comitato consultivo

Sir Jonathan Evans KCB

È stato direttore generale dell'MI5 con 33 anni di esperienza nei Servizi di Sicurezza britannici; Direttore non-executive in HSBC

Andrew France OBE

È stato Deputy Director delle Operazioni per la Cyber Defense al GCHQ; ha oltre 30 anni di esperienza nell'intelligence a livello governativo

Dr Mike Lynch OBE

Noto imprenditore in ambito tecnologico; fondatore di Autonomy e di Invoke Capital; consigliere tecnologico per il governo britannico

Presidente del consiglio di amministrazione

Robert Webb QC

Direttore dell'Ufficio Legale della Rolls-Royce; ex Direttore dell'Ufficio Legale della British Airways. Avvocato della Corona dal 1988. Direttore non-executive alla Borsa di Londra

La natura del rischio è cambiata

- Non solo perdita delle informazioni, ma anche la compromissione dell'integrità dei dati
- Le azioni si svolgono senza rumore: c'è del fuoco da spegnere?
- Le intrusioni possono cominciare da un'azione involontaria
- Non si può far sempre affidamento sul corretto operato dei dipendenti
- Le minacce interne sono enormemente sottostimate – è difficile risolverle

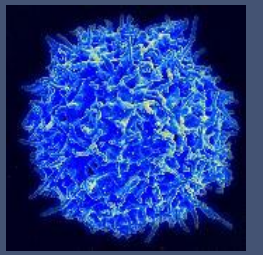
Che cosa potrebbe fermare uno Snowden dentro la vostra azienda?

È impossibile proteggere tutta la rete aziendale

Le minacce più sofisticate troveranno il modo di entrare nonostante le difese sul perimetro

Le minacce interne sono pericolose quanto quelle esterne

È impossibile gestire efficacemente difese basate su regole e firme in tempo reale, 24/7



Self-learning

Genera modelli matematici del comportamento normale

Comprende il comportamento

Per ogni utente, dispositivo e rete

Adattativo

Calcola costantemente le probabilità basandosi sull’evoluzione delle prove

Real time

Rileva le minacce mentre avvengono

DARKTRACE CYBER INTELLIGENCE PLATFORM

Data Capture & Interpretation

Real-time Total Network Immersion

Network Data

Log Data

User Behavior Data

Darkflow
Data Capture

Raw packet storage forensics

300+ Dimensions

Recursive Bayesian Estimation

Unsupervised real-time mathematical engines

Human Modeling

Device Modeling

Network Modeling

Threat Classifier

Compliance Module

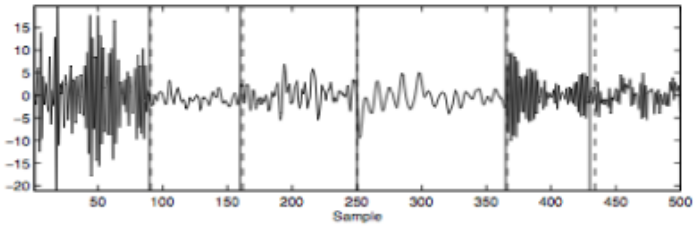
Notification Module

Threat Visualizer

3D Topological Network Projection

Notifications & SIEM outputs

- Innovativa Matematica Bayesiana sviluppata all'Università di Cambridge
- La Recursive Bayesian Estimation rileva, in tempo reale, i minimi cambiamenti nella serie di dati aggiornandone dinamicamente i modelli
- Vengono usati diversi approcci per classificare la probabilità di un'azione sulla base di comportamenti precedenti ed emergenti
- Nessuna supposizione 'a priori' sul valore dell'azione: i modelli matematici sono unici in una organizzazione
- La modellazione è costituita da un insieme complesso di osservazioni a basso livello dell'host, della rete e da caratteristiche peculiari del traffico



$$P(\theta_k|\mathbf{D},\mathcal{M}_k) = \frac{P(\mathbf{D}|\theta_k,\mathcal{M}_k)\,P(\theta_k \mid \mathcal{M}_k)}{P(\mathbf{D} \mid \mathcal{M}_k)}$$

$$P(\mathbf{D} \mid \mathcal{M}_k) = \int P(\mathbf{D} \mid \theta_k,\mathcal{M}_k)P(\theta_k \mid \mathcal{M}_k)\,d\theta_k.$$

$$P(\mathcal{M}_k \mid \mathbf{D}) \propto P(\mathbf{D} \mid \mathcal{M}_k)P(\mathcal{M}_k),$$

$$BF_{a,b}(\mathbf{D}) = \frac{P(\mathcal{M}_a \mid \mathbf{D})}{P(\mathcal{M}_b \mid \mathbf{D})} \Big/ \frac{P(\mathcal{M}_a)}{P(\mathcal{M}_b)}.$$

La sfida

- Fa parte dell'infrastruttura nazionale ed è un obiettivo importante per gli attacchi informatici
- Protezione limitata contro le minacce interne
- Nonostante gli investimenti nei sistemi di sicurezza tradizionale, i sistemi critici erano compromessi e vulnerabili

La soluzione

- Ha scelto l'approccio Enterprise Immune System per proteggersi da attacchi sofisticati
- Progetto pilota, realizzato con Darktrace, conclusosi positivamente dopo quattro settimane
- Rilevate, in tempo reale, anomalie mai viste in precedenza
- Attivata la DCIP per analizzare costantemente le attività sulla rete interna e per rilevare minacce emergenti
- Capacità di mitigare attacchi in corso ed eventi preoccupanti

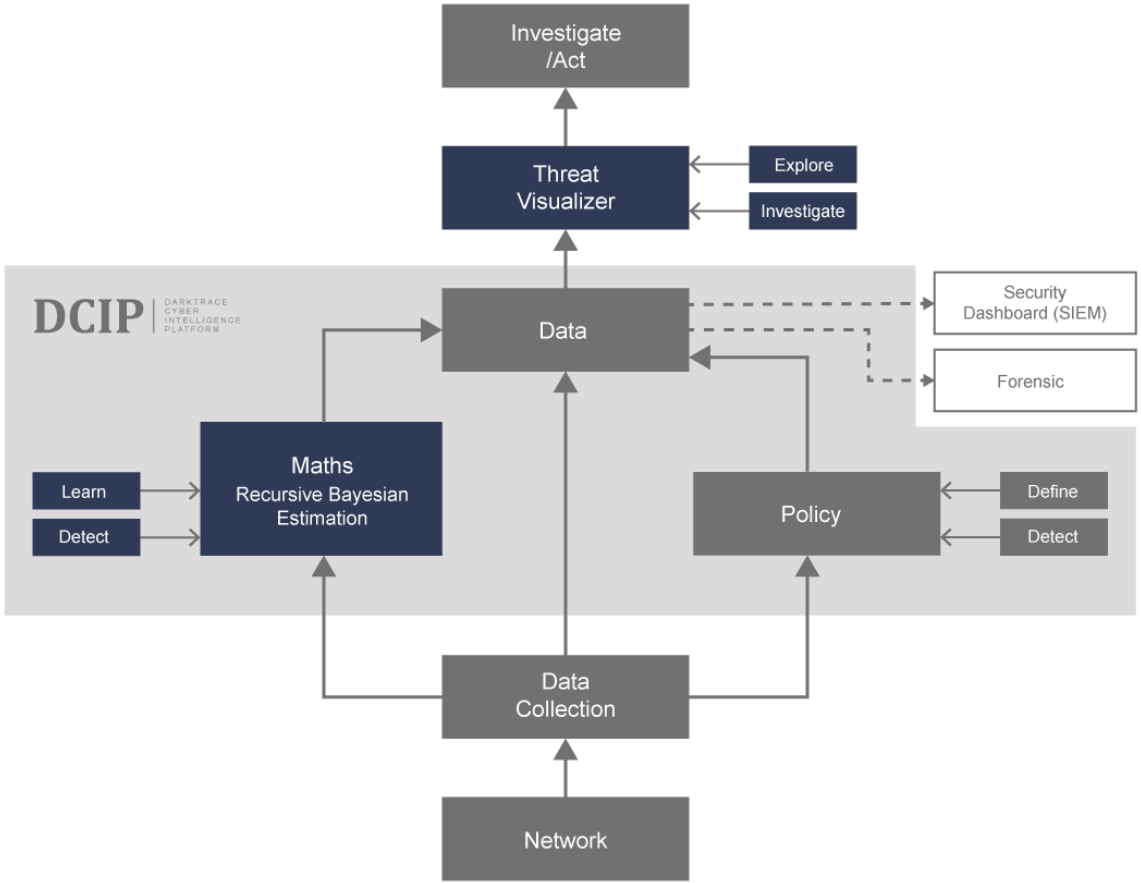
- L’approccio ‘legacy’ è fallito; l’intrusione è inevitabile
- Le minacce sono sofisticate e in costante cambiamento
- Le minacce interne sono sottostimate

L’approccio self-learning del sistema immunitario è fondamentale

- Rilevazione, in tempo reale, di comportamenti anomali mai visti prima
- Matematici Bayesiani di prim’ordine e specialisti nel ‘machine learning’.

DARKTRACE

Architettura



Esempi di attacchi e anomalie

Atipica attività DNS – trovato processo anomalo su varie macchine che generava grandi volumi di traffico DNS per sondare la rete interna e carpire informazioni per un attacco

Identificato Trojan per l'accesso remoto – l'appliance di Darktrace ha notato che un gran numero di dati offuscati fuoriusciva dal sito del cliente. L'analisi post-evento ha mostrato che i dati fluivano verso un dominio sotto il controllo di una terza parte

Installato un browser hijacker che manipolava i risultati mostrati dai motori di ricerca – l'appliance ha identificato una macchina che inviava i termini ricercati ad un server adware che manipolava i risultati per generare reddito per il proprietario dell'adware

Web drive-by Trojan – l'utente ha scaricato un exploit Java maligno, dopo che l'attaccante ha compromesso un servizio di pubblicità usato da un sito per la vendita di macchine di seconda mano. La combinazione fra il download, comunicazioni inusuali verso un server in Medio Oriente e collegamenti criptati che utilizzavano un certificato SSL creato di recente ha causato l'alert

Attaccante che imitava l'infrastruttura Amazon – è stata identificata una macchina sulla rete aziendale che effettuava contatti regolari verso un dominio che imitava volutamente quello di Amazon. Investigazioni da parte del cliente hanno mostrato che questo rappresentava comunicazioni 'command and control' iniziato da malware

Software maligno – falso software Adobe Acrobat Reader scaricato ed installato inavvertitamente da un utente

Uso non autorizzato di cloud storage da parte di un dipendente

Sistema CRM che caricava dati su LinkedIn – dopo l'installazione di un plugin per monitorare l'accesso aziendale a questo sito, Darktrace ha notato che il plugin tentava di estrarre dati provenienti dal sistema CRM ed inviarli verso Linkedin

Dispositivi mobili non autorizzati collegati alla rete interna dell'azienda – alcuni utenti abusavano del Wifi aziendale per accedere a internet tramite cellulari personali, mettendo a rischio l'integrità della rete dato che Darktrace ha mostrato che alcune applicazioni anomale si collegavano frequentemente a internet

Dati di log – appaltatori lavorando fuori gli orari normali condividevano le credenziali per la rete aziendale

Ricognizione della rete

Web Drive-By – consegna del payload

- Il payload si è installato via una pubblicità sul sito di AutoTrader, senza la consapevolezza dell'utente

Violazione della policy

- Un iPhone si era collegato alla rete aziendale
- Il 'beaconing' inviava dettagli sulla pila e altri dati sul sistema al server esterno

‘Framework for Improving Critical Infrastructure Cybersecurity’, febbraio 2014, National Institute of Standards & Technology

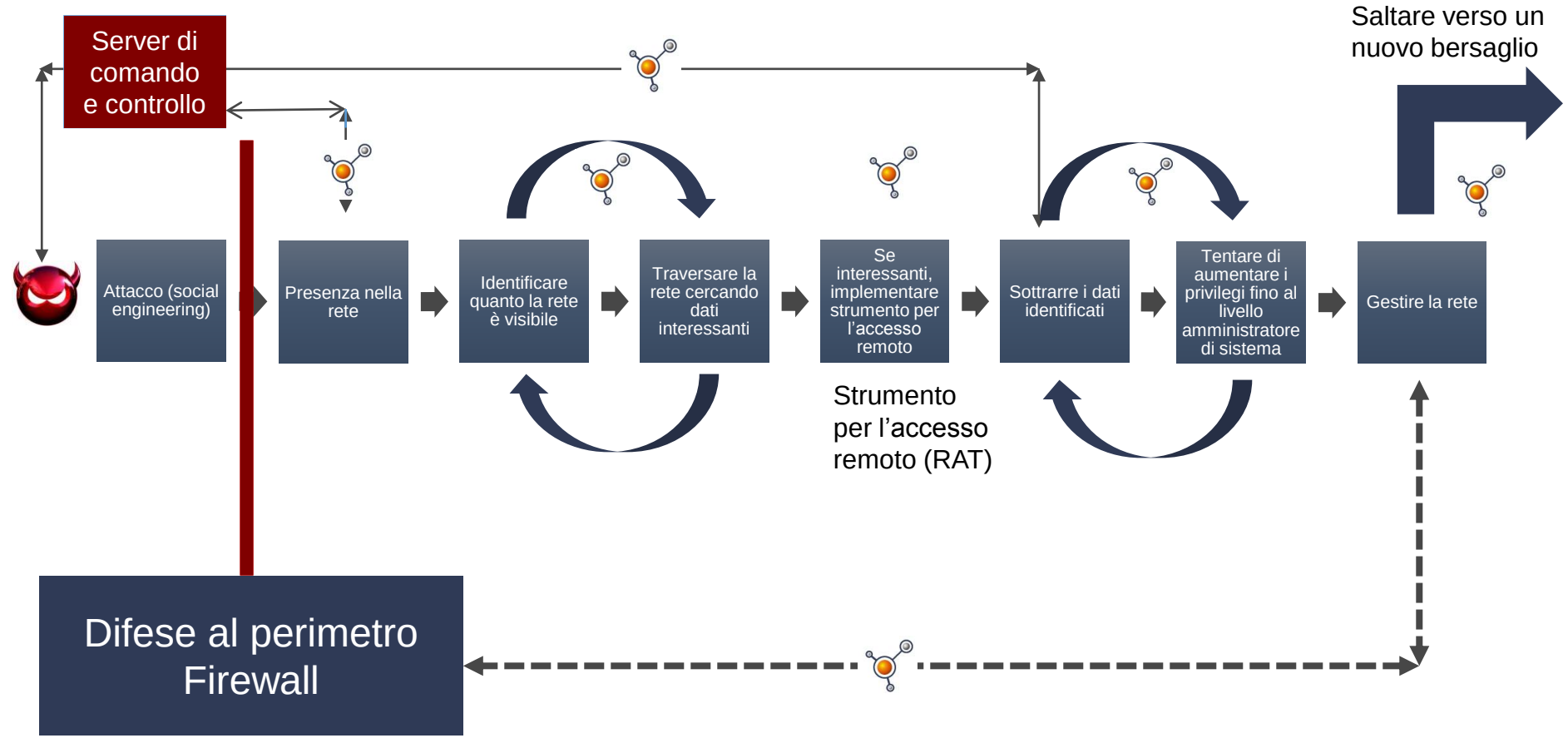
La SEC ha pubblicato un allarme sulla governance della Cyber Security ad aprile 2014:

- Richieste di informazioni per:
  - controllo dei privilegi degli utenti non autorizzati e dei media removibili
  - Linee guida per “eventi attesi” su una rete
  - “Aggregazione e correlazione di eventi provenienti da molteplici fonti”
  - “Monitoraggio della rete aziendale per rilevare eventuali eventi inerenti la Cyber Security”
  - “Valutazione delle richieste di trasferimenti provenienti dall’esterno … per identificare richieste anomale e potenzialmente fraudolenti”
- Divulgazione su malware identificato, DDoS, risorse web compromesse, violazioni della rete, compromissioni da accesso remoto, email fraudolenti, estorsioni, cattiva condotta da insider, ecc.

Esistono tecnologie che proteggono utilizzando l’Enterprise Immune System.

Siete « compliant » ?

Dove vengono identificati i comportamenti anormali



Cosa succede se la rete è già compromessa?

- Darktrace non ha bisogno di dati perfetti – può rilevare intrusioni già esistenti che sono anomale rispetto al comportamento normale

Com'è scalabile Darktrace?

- Dimensioniamo l'appliance sulla base del throughput in GB, ed è scalabile linearmente

Chi dovrebbe utilizzare il Threat Visualizer?

- Non è necessario possedere una laurea in matematica, ma basta avere una buona comprensione dell'infrastruttura della rete

Che formati di file vengono accettati?

- Quasi tutti – lavoriamo tipicamente con il traffico interno della rete

Quali tipi di anomalie vengono rilevate?

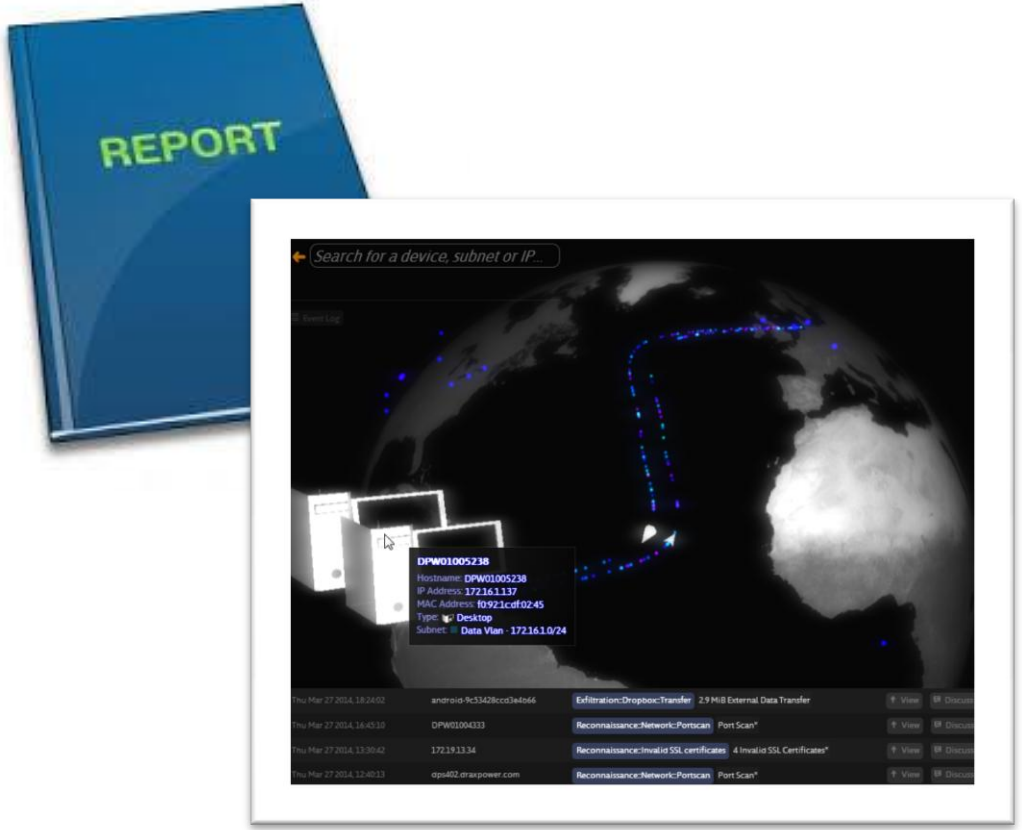
- La gamma di anomalie è molto ampia perché siamo posizionati al centro della rete. Darktrace ha rilevato varie minacce, inclusi 'insider', criminalità cyber e missioni sponsorizzate da Stati sovrani.

Quanto sono comprensivi gli algoritmi?

- Darkrace indicizza oltre 300 fonti di informazione (metriche) e crea un modello per ogni dispositivo, utente e rete. Gli algoritmi sono stati sviluppati all'Università di Cambridge, il centro più importante a livello mondiale per il 'machine learning'.

Proof of Value (POV)

- È semplice fare un Proof of Value
- Installazione veloce
- Sono supportate ‘policy’ per ogni azienda
- L’appliance è operativa fin dal primo giorno
- Vengono forniti relazioni settimanali che forniscono una panoramica delle minacce e delle anomalie individuate da Darktrace nell’organizzazione




DARKTRACE