Looking Back Over a Quarter Century of Network Monitoring

Todd Heberlein

@toddheberlein

Security Onion Conference
11 Sep 2015

Analytics

Specifically, our goal is to develop monitoring techniques that will enable us to maintain information of normal network activity (including those of the network's individual nodes, their users, their offered services, etc.) The monitor will be capable of observing current network activity, which, when compared with historical behavior, will enable it to detect in real-time possible security violations on the network – regardless of the network type, organization, and topology.

System 1

Modelling patterns of life for each user and machine, it is the only software platform able to detect normal and abnormal behaviors as they emerge, without already knowing what it is looking for, and calculate the probability of threat based on the detection of behavioral anomalies.

System 2

Analytics

Specifically, our goal is to develop monitoring techniques that will enable us to maintain information of normal network activity (including those of the network's individual nodes, their users, their offered services, etc.) The monitor will be capable of observing current network activity, which, when compared with historical behavior, will enable it to detect in real-time possible security violations on the network – regardless of the network type, organization, and topology.

System 1

Modelling patterns of life for each user and machine, it is the only software platform able to detect normal and abnormal behaviors as they emerge, without already knowing what it is looking for, and calculate the probability of threat based on the detection of behavioral anomalies.

System 2

Analytics

Specifically, our goal is to develop monitoring techniques that will enable us to maintain information of normal network activity (including those of the network's individual nodes, their users, their offered services, etc.) The monitor will be capable of observing current network activity, which, when compared with historical behavior, will enable it to detect in real-time possible security violations on the network – regardless of the network type, organization, and topology.

System 1

Modelling patterns of life for each user and machine, it is the only software platform able to detect normal and abnormal behaviors as they emerge, without already knowing what it is looking for, and calculate the probability of threat based on the detection of behavioral anomalies.

System 2

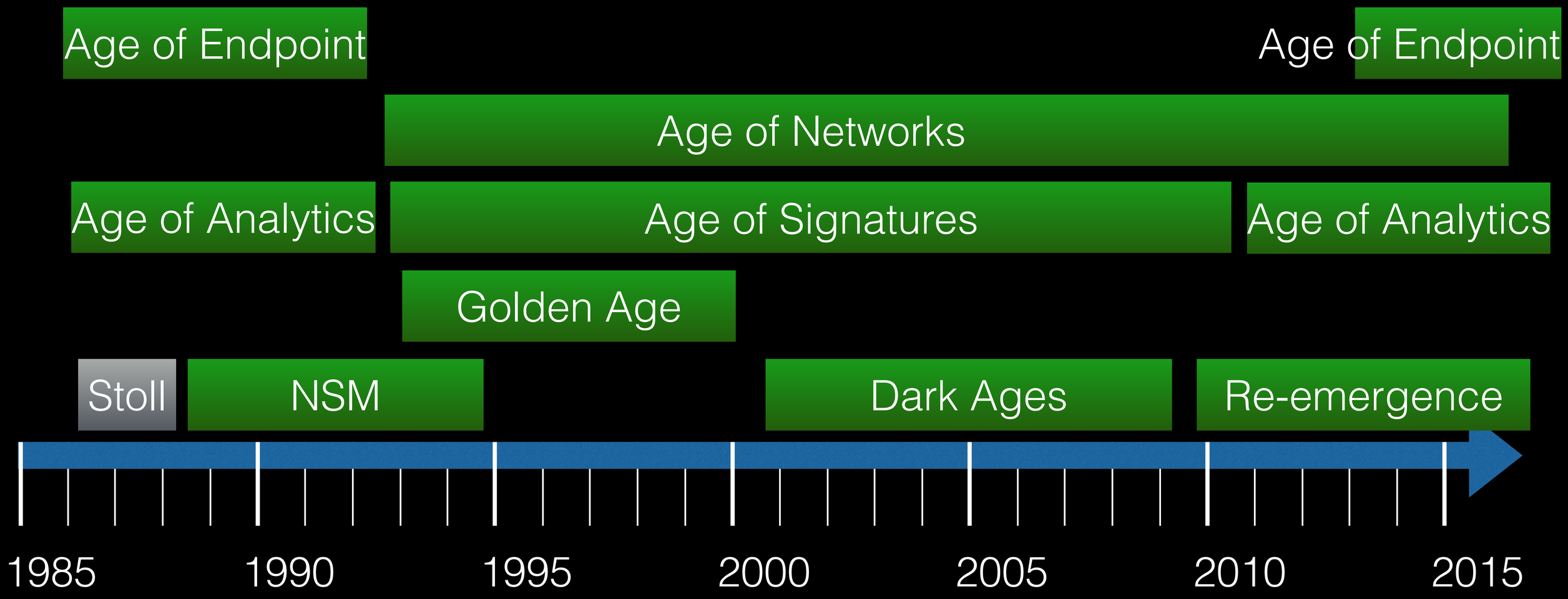
Analytics

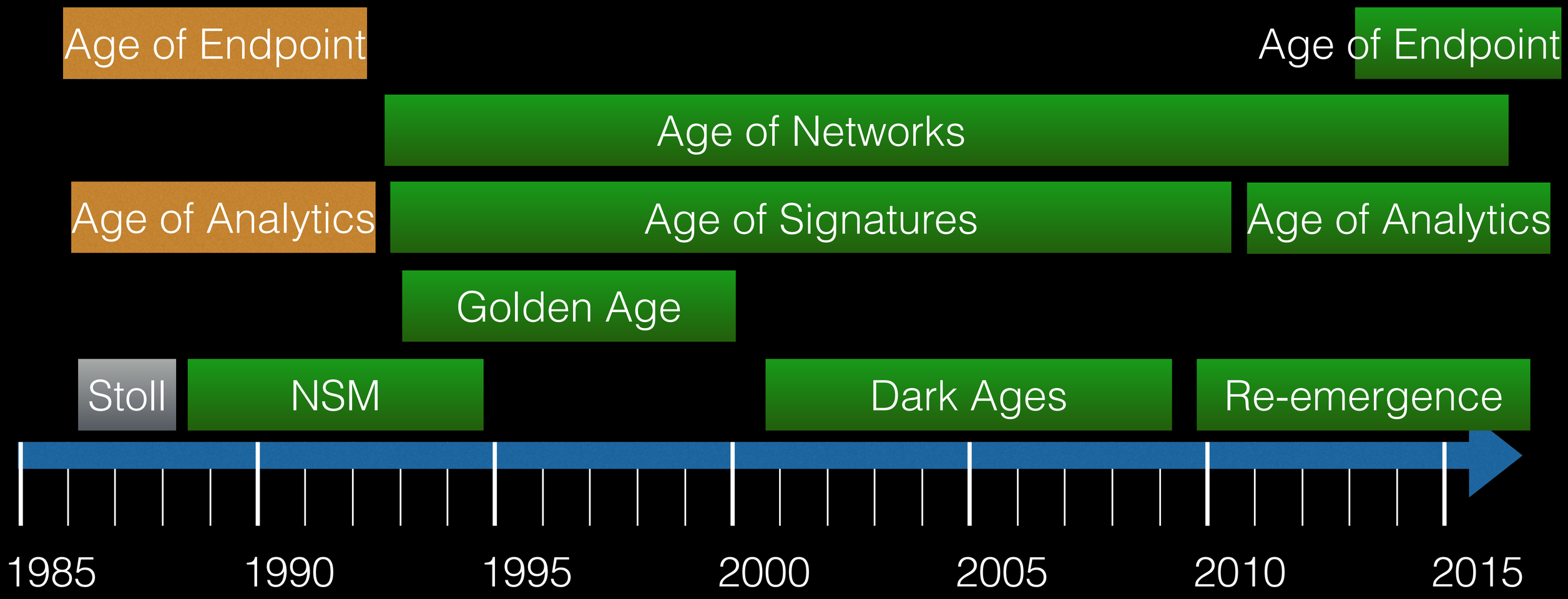
Specifically, our goal is to develop monitoring techniques that will enable us to maintain information of normal network activity (including those of the network's individual nodes, their users, their offered services, etc.) The monitor will be capable of observing current network activity, which, when compared with historical behavior, will enable it to detect in real-time possible security violations on the network – regardless of the network type, organization, and topology.

"A Network Security Monitor", May 1990

Modelling patterns of life for each user and machine, it is the only software platform able to detect normal and abnormal behaviors as they emerge, without already knowing what it is looking for, and calculate the probability of threat based on the detection of behavioral anomalies.

Darktrace web site, March 2015


Age of Endpoint
Age of Endpoint
Age of Networks
Age of Analytics
Age of Signatures
Age of Analytics
Golden Age
Stoll
NSM
Dark Ages
Re-emergence
1985
1990
1995
2000
2005
2010
2015


Age of Endpoint
Age of Endpoint
Age of Networks
Age of Analytics
Age of Signatures
Age of Analytics
Golden Age
Stoll
NSM
Dark Ages
Re-emergence
1985
1990
1995
2000
2005
2010
2015

“The distribution of the data was found to be generally multi-modal (and not Gaussian). … This is important since many statistical techniques assume the data to be Gaussian distributed.”

1990

“The biggest concern was the detection of unusual activity which was not obviously an attack. Often we did not have someone to monitor the actual connection, and we often did not have any supporting evidence to prove or disprove that an attack had occurred.”

1990

“One possible solution would be to save the actual data crossing the connection, so that an exact recording of what had happened would exist.”

“A second solution would be to examine audit trails generated by one of the hosts concerned.”

“Both approaches are currently being examined.”

1990

1-10-91

current_con_index num
overall_con_index num
warning num

initiator A.B.C.D
receiver A.B.C.D
proto number
src_port number
dst_port number
service_name string

start_time
stop_time
duration number

pkts number
bytes number
pkts number
bytes number

1st string-init-number
string-init-number
string-rec-number
rtn

connection record

sort by warning, ~~current_con_index, overall_con_index~~

filter by all : for numbers [>, <, =] number

addresses can take wild cards

start & stop times should be broken down

Take a list of connections & build a report

Take a connection & build a transcript

Money / Proposals — thesis proposal

Distribution

string matching

FY 92

provide research

1991

initiator	A.B.C.D	1 3 5 7 / 1 3 5 7
receiver	A.B.C.D	
proto	number	
src_port	number	11
dst_port	number	
service_name	string	12
start_time	YYYY MM DD HH MM SS	Y M D H M S
stop_time		13
duration	number	
# pkts	number	
# bytes	number	4
# pkts	number	
# bytes	number	
~~int~~ string-init-number		at most 15
string-init-number		some for inits some for recs
string-rec-number		

connection record

1991

1-15-91

Note: finished string searches the other day
finished transcript generator today

Tasks for NSM

1 • Continued development of NSM software ~~addtn~~.
- deliverable is code/documentation for mature prototype.
- Paper describing NSM / presentation @ DOE conference.

2 • Development of an distributed NSM architecture
- Report

3 • Analysis of other IDS techniques and their possible use in a networked environment
- Report (Experts)

4 • ~~For~~ Study techniques for stalking hackers. techniques frequently used, ...
- A seminar in the use of the NSM (mature prototype)

1991

```
7
login: guest
Login incorrect
daemon:
passwd
login: root
Permission denied
CWD ~ROOT
218 267389 8.944 5.778 10.000 10.000 128.120.2.251 128.120.57.60 6 25858
    23 telnet Mon-Jun-03-18:12:03-1991 Mon-Jun-03-18:12:38-1991 35
    51 40 34 144 0-rec-1 1-rec-2
199 267370 8.944 5.778 10.000 10.000 128.120.2.251 128.120.57.14 6 10498
    23 telnet Mon-Jun-03-18:10:09-1991 Mon-Jun-03-18:10:36-1991 27
```

1991

From unify!tonga.unify.com!srm@csusac.ecs.csus.edu Thu Feb 28 13:29:54 1991
Received: by iris.eecs.ucdavis.edu (5.57/UCD.EECS.4.0)
id AA08857; Thu, 28 Feb 91 13:29:52 -0800
Received: from csusac.ecs.csus.edu by ucdavis.ucdavis.edu (5.61/UCD2.03)
id AA10151; Thu, 28 Feb 91 13:20:23 -0800
Received: by csusac.ecs.csus.edu (5.61/1.34)
id AA14720; Thu, 28 Feb 91 16:20:28 -0500
Received: from tonga
by unify.com (5.61/smail2.5/06-13-89/jwc.4)
with SMTP
id AA08207; Thu, 28 Feb 91 12:43:48 -0800
Received: by tonga. (4.0/SMI-4.0)
id AA05658; Thu, 28 Feb 91 12:43:41 PST
Date: Thu, 28 Feb 91 12:43:41 PST
From: srm@tonga.unify.com (Steve Maraglia)
Message-Id: <9102282043.AA05658@tonga.>
To: heberlei@iris.eecs.ucdavis.edu
Subject: Re: the scoop
Status: R

Todd,

Thank you for emailing the transcript!

Do you have any other information regarding Unify passwd hacking or unauthorized access to Unify? If so, can you send it to me?

This type of irresponsible behavior should be dealt with very harshly! Can any legal action be taken against these individuals? Will this "[redacted]" be removed from all systems at ucdavis? Can you tell me what, if any, action is being brought against these individuals?

Thanks for your help

Steve Maraglia - System Administrator internet: srm@unify.com
Unify Corporation ..![uunet,csusac,pyramid]!unify!srm
3901 Lennane Dr. Sacramento, CA 95834 (916) 928-6271

Id AA05658; Thu, 28 Feb 91 12:43:41 PST
Date: Thu, 28 Feb 91 12:43:41 PST
From: srm@tonga.unify.com (Steve Maraglia)
Message-Id: <9102282043.AA05658@tonga.>
To: heberlei@iris.eecs.ucdavis.edu
Subject: Re: the scoop
Status: R

Todd,

Thank you for emailing the transcript!

Do you have any other information regarding Unify passwd hacking or unauthorized access to Unify? If so, can you send it to me?

This type of irresponsible behavior should be dealt with very harshly! Can any legal action be taken against these individuals? Will this "[redacted]" be removed from all systems at ucdavis? Can you tell me what, if any, action is being brought against these individuals?

Thanks for your help

Steve Maraglia - System Administrator
Unify Corporation
3901 Lennane Dr. Sacramento, CA 95834
internet: srm@unify.com
..!{uunet,csusac,pyramid}!unify!srm
(916) 928-6271

Date: Thu, 28 Feb 91 12:43:41 PST
From: srm@tonga.unify.com (Steve Maraglia)
Message-Id: <9102282043.AA05658@tonga.>
To: heberlei@iris.eecs.ucdavis.edu
Subject: Re: the scoop
Status: R

Todd,

Thank you for emailing the transcript!

Do you have any other information regarding Unify passwd hacking or unauthorized access to Unify? If so, can you send it to me?

This type of irresponsible behavior should be dealt with very harshly! Can any legal action be taken against these individuals? Will this "[redacted]" be removed from all systems at ucdavis? Can you tell me what, if any, action is being brought against these individuals?

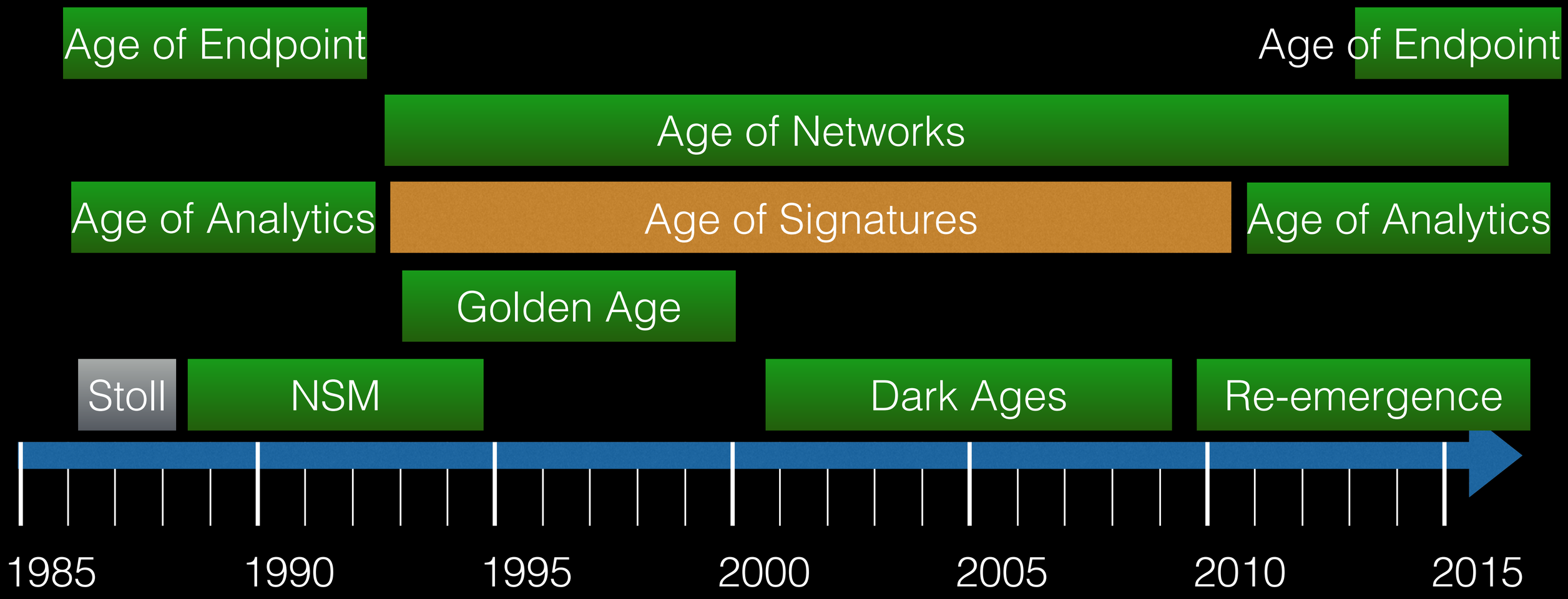
Thanks for your help

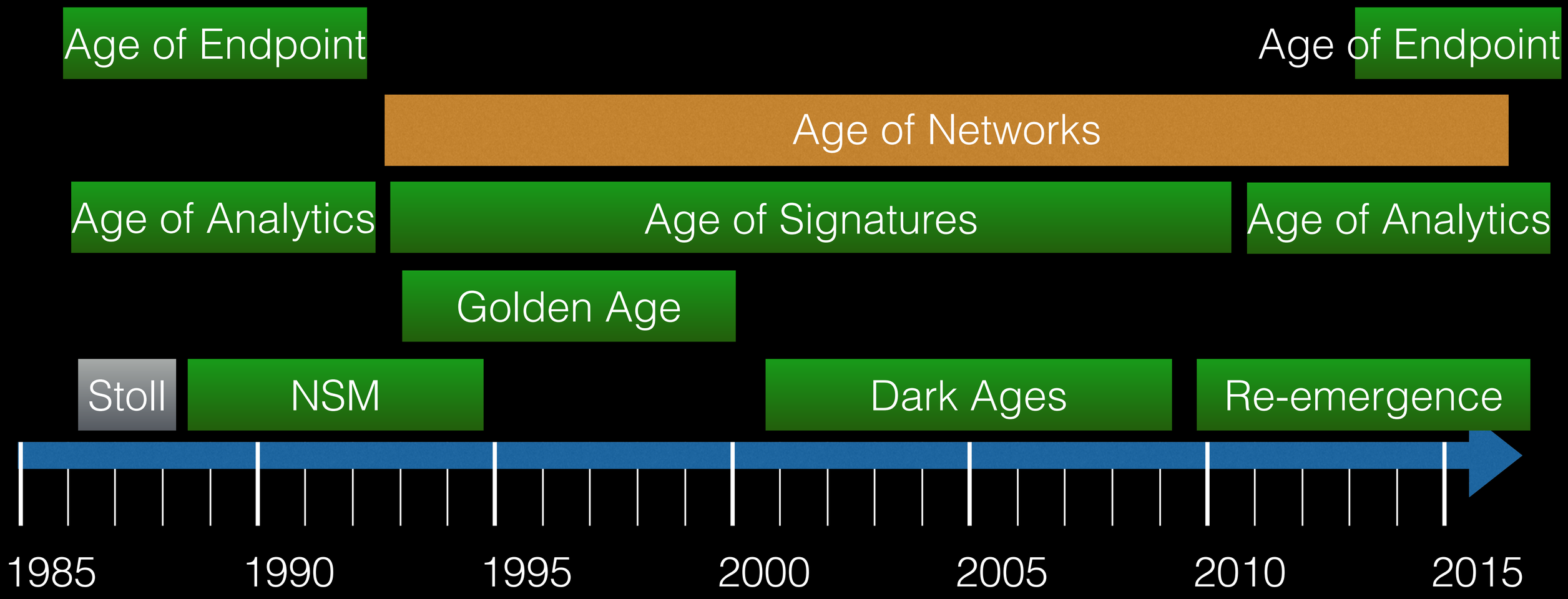
Steve Maraglia - System Administrator
Unify Corporation
3901 Lennane Dr. Sacramento, CA 95834
internet: srm@unify.com
..!{uunet,csusac,pyramid}!unify!srm
(916) 928-6271

```
#define ATTACK_MODEL_WEIGHT      2.0
#define PROFILE_WEIGHT           1.0
#define ES_WEIGHT                5.0
```

1995

NSM’s analyze.h


Age of Endpoint
Age of Endpoint
Age of Networks
Age of Analytics
Age of Signatures
Age of Analytics
Golden Age
Stoll
NSM
Dark Ages
Re-emergence
1985
1990
1995
2000
2005
2010
2015


Age of Endpoint
Age of Endpoint
Age of Networks
Age of Analytics
Age of Signatures
Age of Analytics
Golden Age
Stoll
NSM
Dark Ages
Re-emergence
1985
1990
1995
2000
2005
2010
2015

The Great Forgetting

Questions in the late 1990s

Why did the warnings go down when we ran the data a second time?

I added a string, but why didn’t the warning didn’t go up?

Why is “Last login” a signature?

“Last login” Indicator

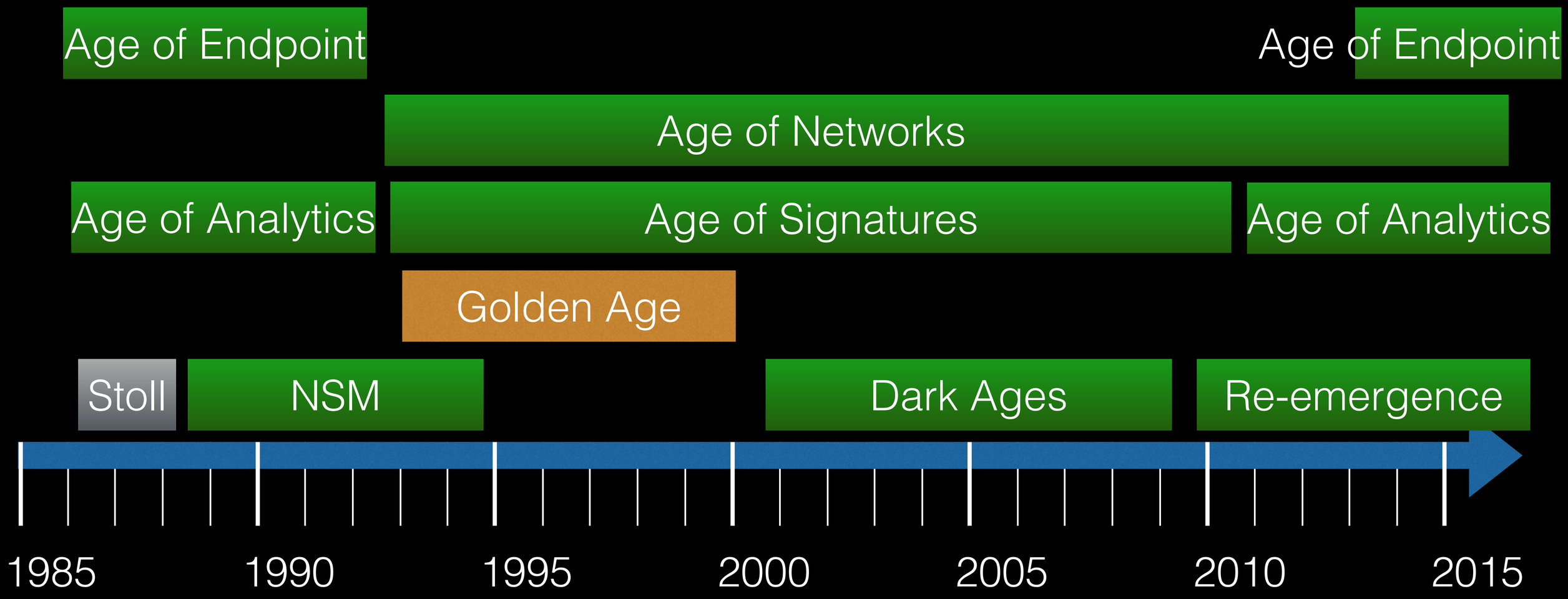
```
if ((num_of_last_login > 0)
|| (num_of_login_last_used > 0)){
    logged_in = TRUE;
    warn_value -= DEFAULT_TCP_WARN;
}
else {
    warn_value += 2.0;
}
```

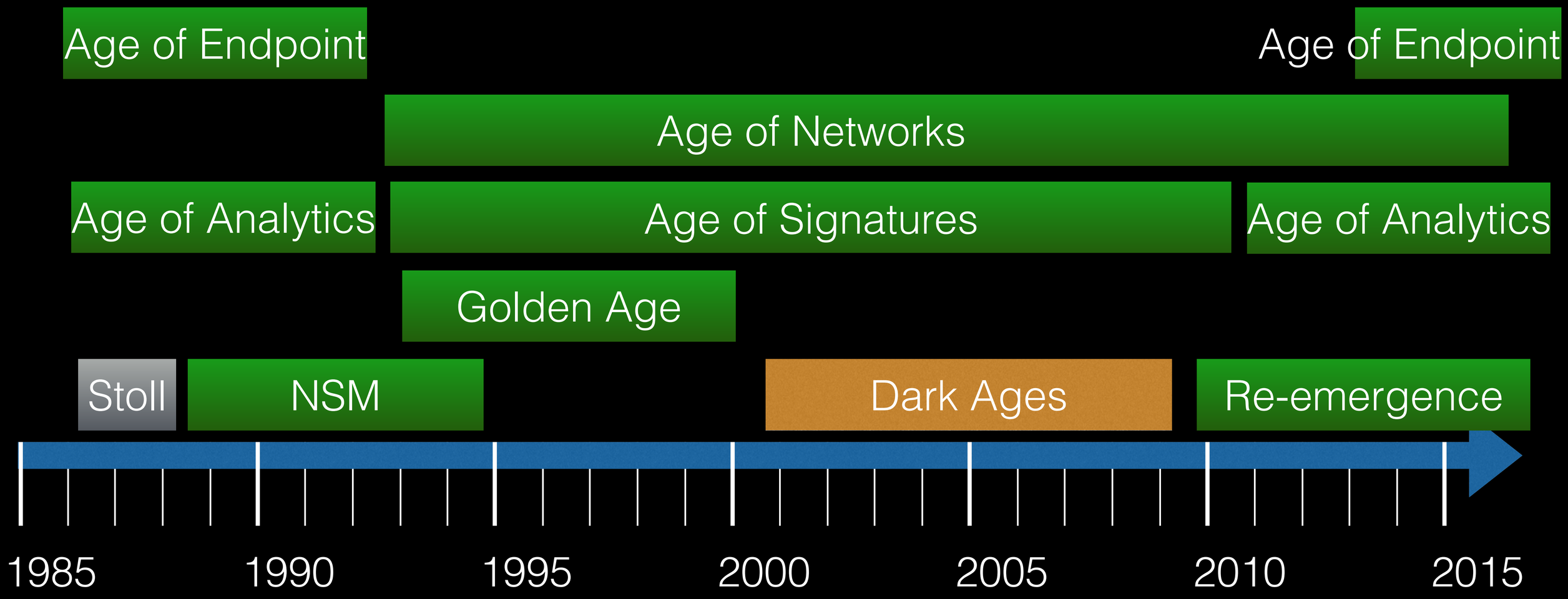
“daemon:” Indicator

```
if ((num_of_passwd_file > 0) &&
(num_of_passwd_file < 3)){
    warn_value += 5;
}
else if (num_of_passwd_file >= 3)
    warn_value += 6.0;
```

Golden Years of Commercial IDS

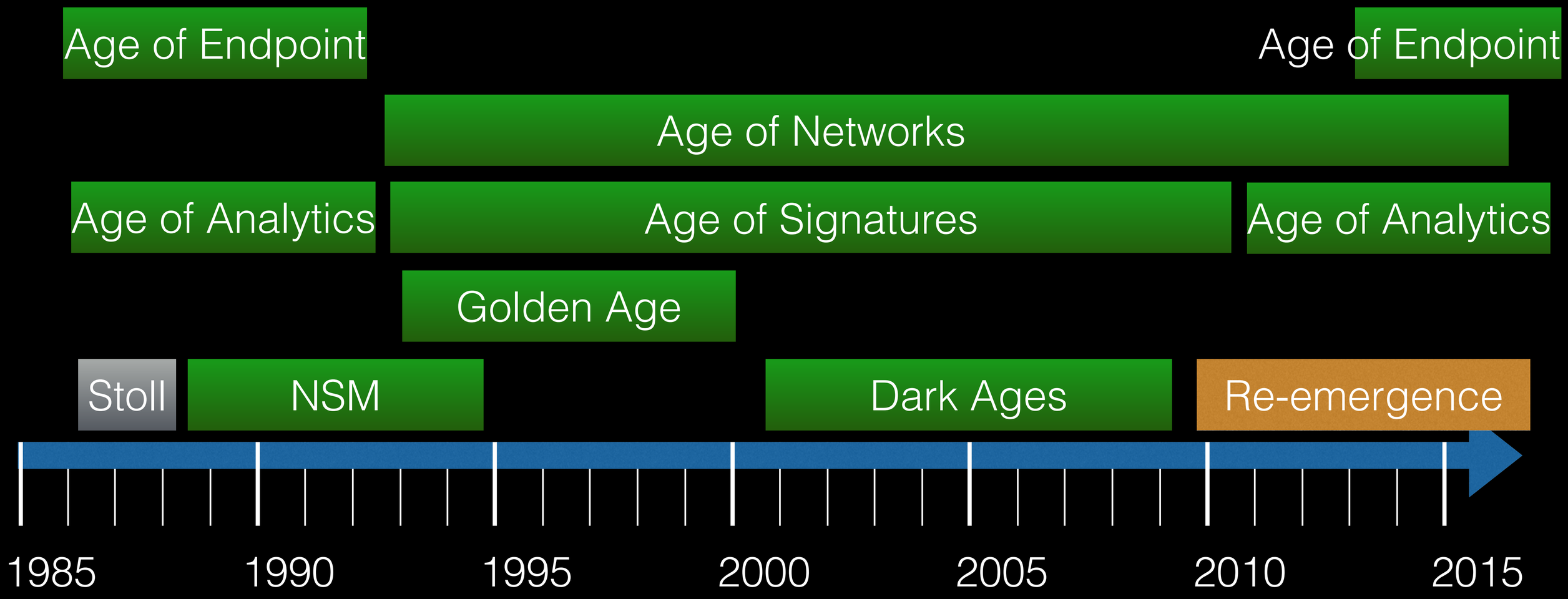
1993-2000


Age of Endpoint
Age of Endpoint
Age of Networks
Age of Analytics
Age of Signatures
Age of Analytics
Golden Age
Stoll
NSM
Dark Ages
Re-emergence
1985
1990
1995
2000
2005
2010
2015


Age of Endpoint
Age of Endpoint
Age of Networks
Age of Analytics
Age of Signatures
Age of Analytics
Golden Age
Stoll
NSM
Dark Ages
Re-emergence
1985
1990
1995
2000
2005
2010
2015

Rest In Peace

2003


Age of Endpoint
Age of Endpoint
Age of Networks
Age of Analytics
Age of Signatures
Age of Analytics
Golden Age
Stoll
NSM
Dark Ages
Re-emergence
1985
1990
1995
2000
2005
2010
2015

High Profile Attacks

KIM ZETTER SECURITY 01.14.10 8:01 PM

GOOGLE HACK ATTACK WAS ULTRA SOPHISTICATED, NEW DETAILS SHOW

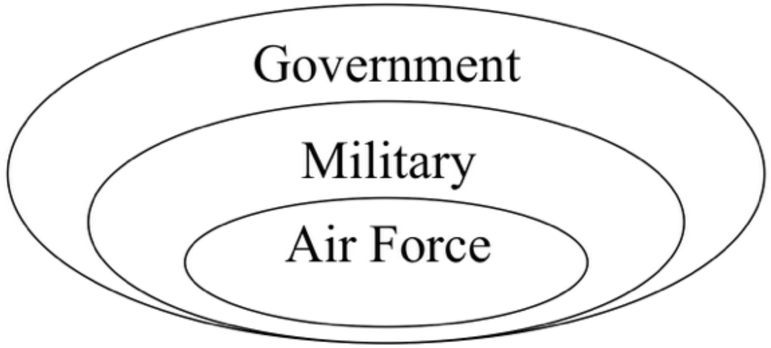
HACKERS SEEKING SOURCE code from Google, Adobe and dozens of other high-profile companies used unprecedented tactics that combined encryption, stealth programming and an unknown hole in Internet Explorer, according to new details released by the anti-virus firm McAfee.

http://www.wired.com/2010/01/operation-aurora/

The Value of Scale

Amazon Purchase Circles

- Identifies top sellers unique to defined groups.
- Groups are defined a priori
- Our model:
  - may indicate an attack targeted at a specific group (e.g., Air Force or power grid)



2000

Bestsellers for U.S. Air Force

Purchase Circles > Government > Military > U.S. Air Force

Books: Bestsellers for U.S. Air Force

More:

1 **Harry Potter and the Goblet of Fire**

2 **Harry Potter and the Chamber of Secrets**

3 **Harry Potter and the Sorcerer's Stone**

4 **Harry Potter and the Prisoner of Azkaban**

Activity unique to Air Force, and perhaps most important to the Air Force, is lost in the noise.

2000

Unique to U.S. Air Force

Purchase Circles > Government > Military > U.S. Air Force

Books: Unique to U.S. Air Force More: Pur

1. **Air Power: A Centennial Appraisal**
2. **They Also Flew: The Enlisted Pilot Legacy, 1912-1942**
3. **Victor Padrini: A Novel of the United States Air Force Academy**
4. **The Limits of Air Power: The American Bombing of North Vietnam**

These books are important to people in the Air Force. What attacks might be unique to the Air Force, and should we pay closer attention to them?

2000

No one organization can field the depth of expertise or the range of sensors needed to fully understand everything that may occur on their systems. A community effort is needed.

Scans on Port 1024 and 3072

File Edit View Tools Message Hel

From: cert@cert.mil
Date: Friday, December 01, 2000 4:01 AM
To: intrusion@sans.org
Subject: Scans on Port 1024 and 3072

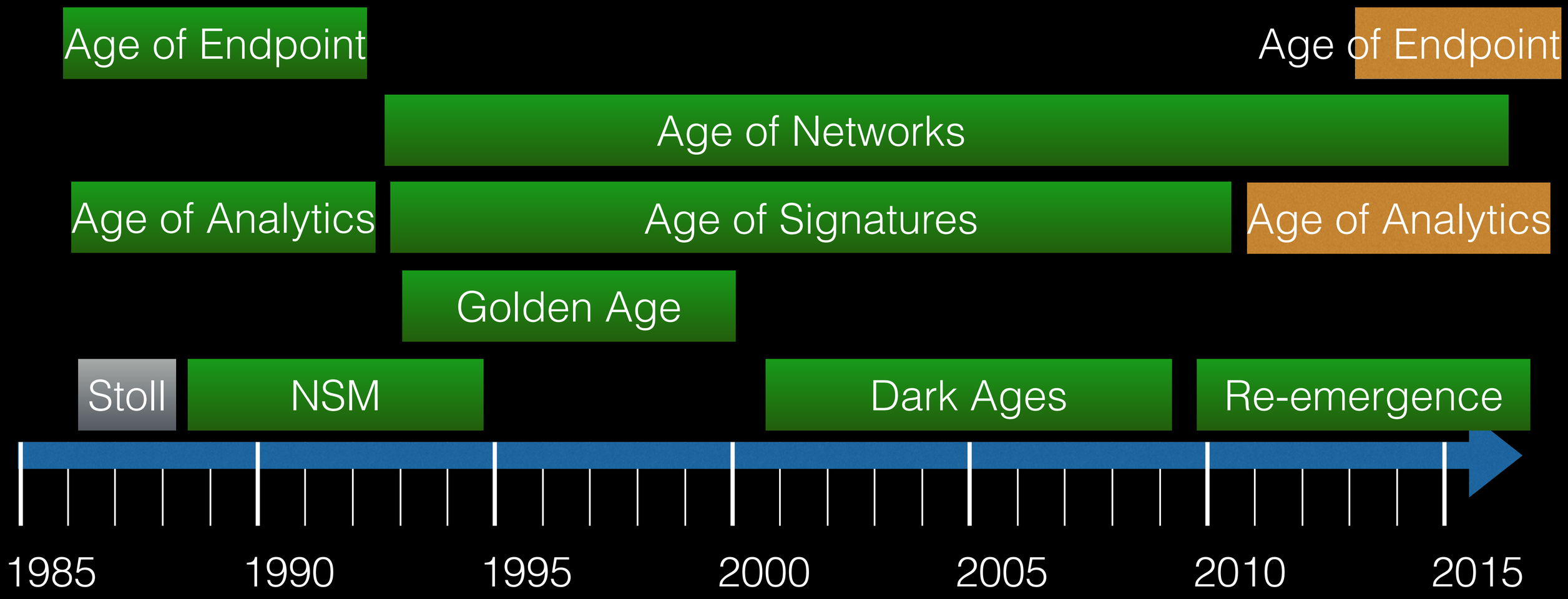
```
Matt;

I'm puzzled by a scan I have been seeing and would like to know if
anyone else is seeing this, and maybe have some ideas on what might be
the cause.

 For at least two weeks now I have been seeing scans on port 1024 and
3072.  I know port 1024 has been associated with NetSpy, and at first, I
thought this might be the cause.  However, I have since seen scans on
port 1024 in conjunction with scans on port 3072.  Sometimes scans to
these ports alternate and sometimes they are sequential.  I have
attached an excerpt of a log showing the scan.

001130.06:49:04  64.229.96.233:21  >  [illegible]24:3072 RST:ACK:-
001130.06:49:04  64.229.96.233:21  >  [illegible]:3072 RST:ACK:-
001130.06:49:04  64.229.96.233:21  >  [illegible]:3072 RST:ACK:-
001130.06:49:04  64.229.96.233:21  >  [illegible]:3072 RST:ACK:-
001130.06:49:04  64.229.96.233:21  >  [illegible]:3072 RST:ACK:-
001130.06:49:04  64.229.96.233:21  >  [illegible]:3072 RST:ACK:-
001130.06:49:04  64.229.96.233:21  >  [illegible]:3072 RST:ACK:-
001130.06:49:04  64.229.96.233:21  >  [illegible]:3072 RST:ACK:-
```

2000


Age of Endpoint
Age of Endpoint
Age of Networks
Age of Analytics
Age of Signatures
Age of Analytics
Golden Age
Stoll
NSM
Dark Ages
Re-emergence
1985
1990
1995
2000
2005
2010
2015

FICO

PRODUCTS & SOLUTIONS | ANALYTIC CLOUD | LEARN | ABOUT US | myFICO.com | English

Home / Fraud & Security | Cyber Security

Cyber Security

Identify Emerging Threats and Fight Cyber Crime in Real Time

Cyber Security | Entity Resolution & Social Network

---

sas THE POWER TO KNOW.

Log In | Worldwide Sites | Contact Us | Search

Products & Solutions | Industries | Support & Training | Customer Stories | Partners | Community | About SAS

Home > Products & Solutions > Fraud & Security Intelligence > SAS Cybersecurity

SAS® Cybersecurity

The essential layer for cyberdefense

DARKTRACE

US: +1 917 363 0822
Europe: +44 (0) 20 7925 3551

Company | Technology | Products | Resources | Industries | News & Events | Partners | Contact | Proven Track Record

Press Releases | In the News | Events

DETECT UNKNOWN THREATS

Cyber threats are pervasive and already inside your network now. Tackling emerging anomalies is critical to get ahead of today's persistent adversaries.

Read more >

toddheberlein.com/blog/

Before there was Mandiant there was WheelGroup
September 7, 2015

An early Managed Security Service Provider (MSSP)
September 7, 2015

NSM Source Code from 1995
September 9, 2015