Pure IT CUSO

AXFI Cyber Security Track Session 4 : Risk Predictability

Gene Fredriksen

Principal Cyber Security Strategist

One of the top three Security Executives of the past 30 years.
-SC Media, 2019

The Truth

- Cybersecurity experts and analysts are constantly trying to keep pace with changes and trends in the volatile and ever-shifting landscape of IT security.
- Despite sophisticated tools and solutions that are being rolled out by cybersecurity vendors, every IT security officer knows that data breaches eventually happen — it's not about the *if* but the *when* — and they usually go undetected for a long time.

Problem: Financial Services Breaches 2018

Frequency	927 incidents, 207 with confirmed data disclosure
Top 3 patterns	Web Applications, Privilege Misuse, and Miscellaneous Errors represent 72% of breaches
Threat actors	External (72%), Internal (36%), Multiple parties (10%), Partner (2%) (breaches)
Actor motives	Financial (88%), Espionage (10%) (breaches)
Data compromised	Personal (43%), Credentials (38%), Internal (38%) (breaches)

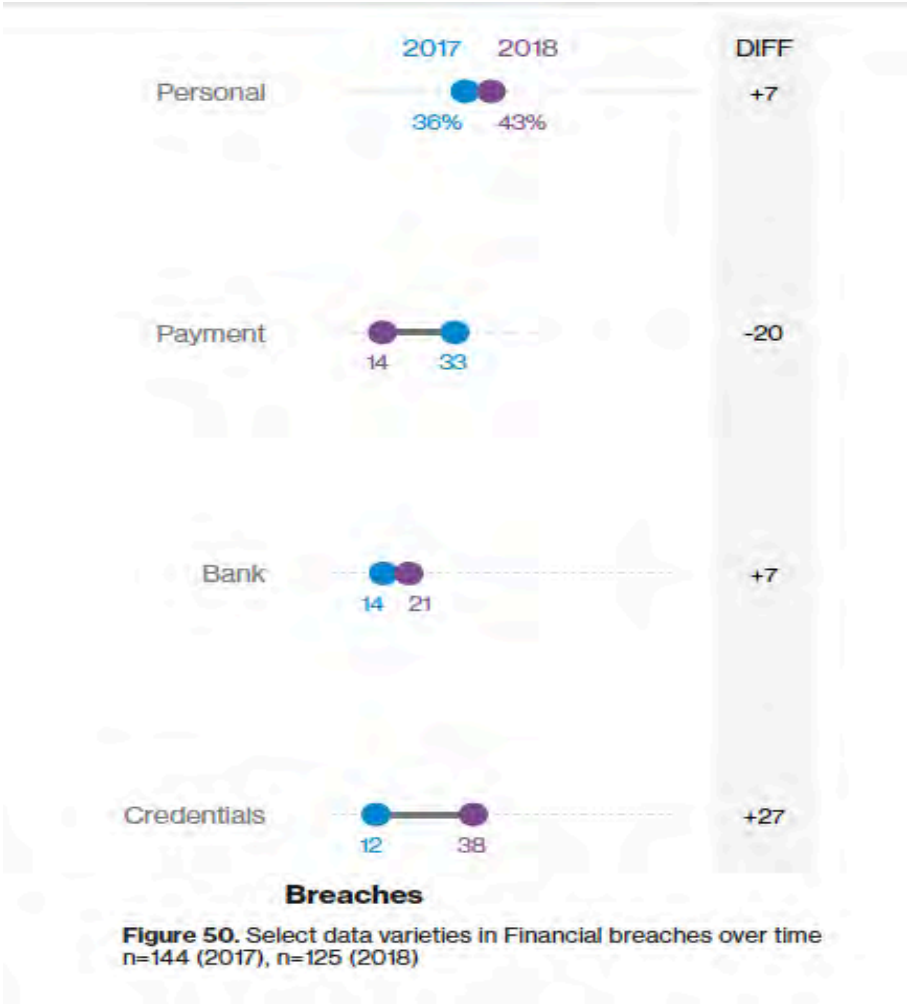
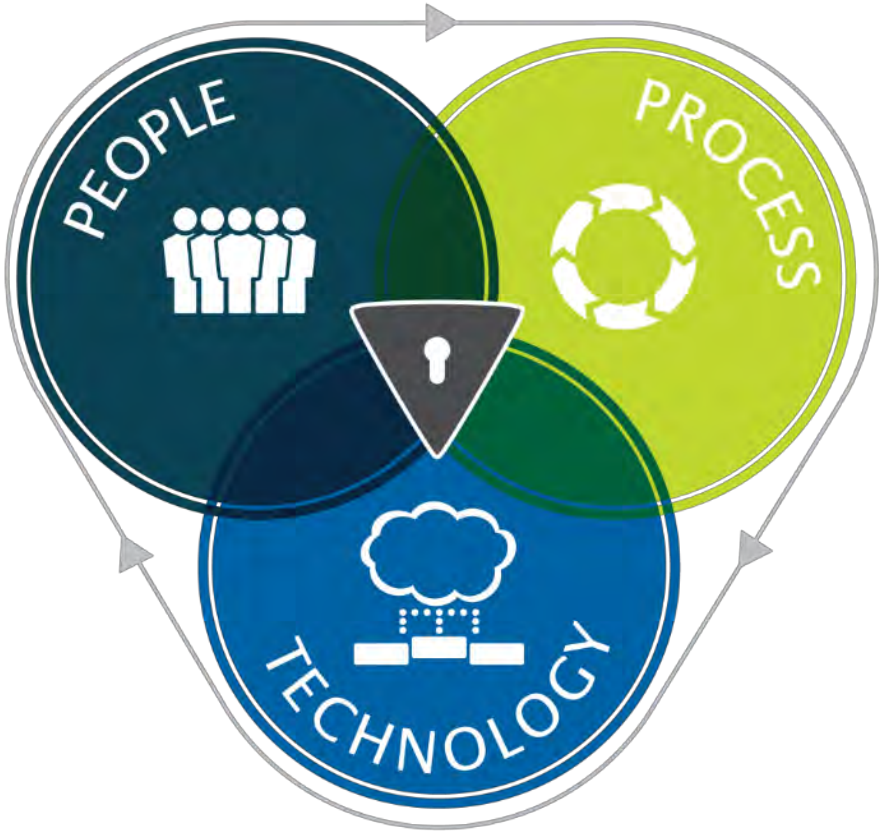


Figure 50. Select data varieties in Financial breaches over time n=144 (2017), n=125 (2018)

Type / Frequency of Attack

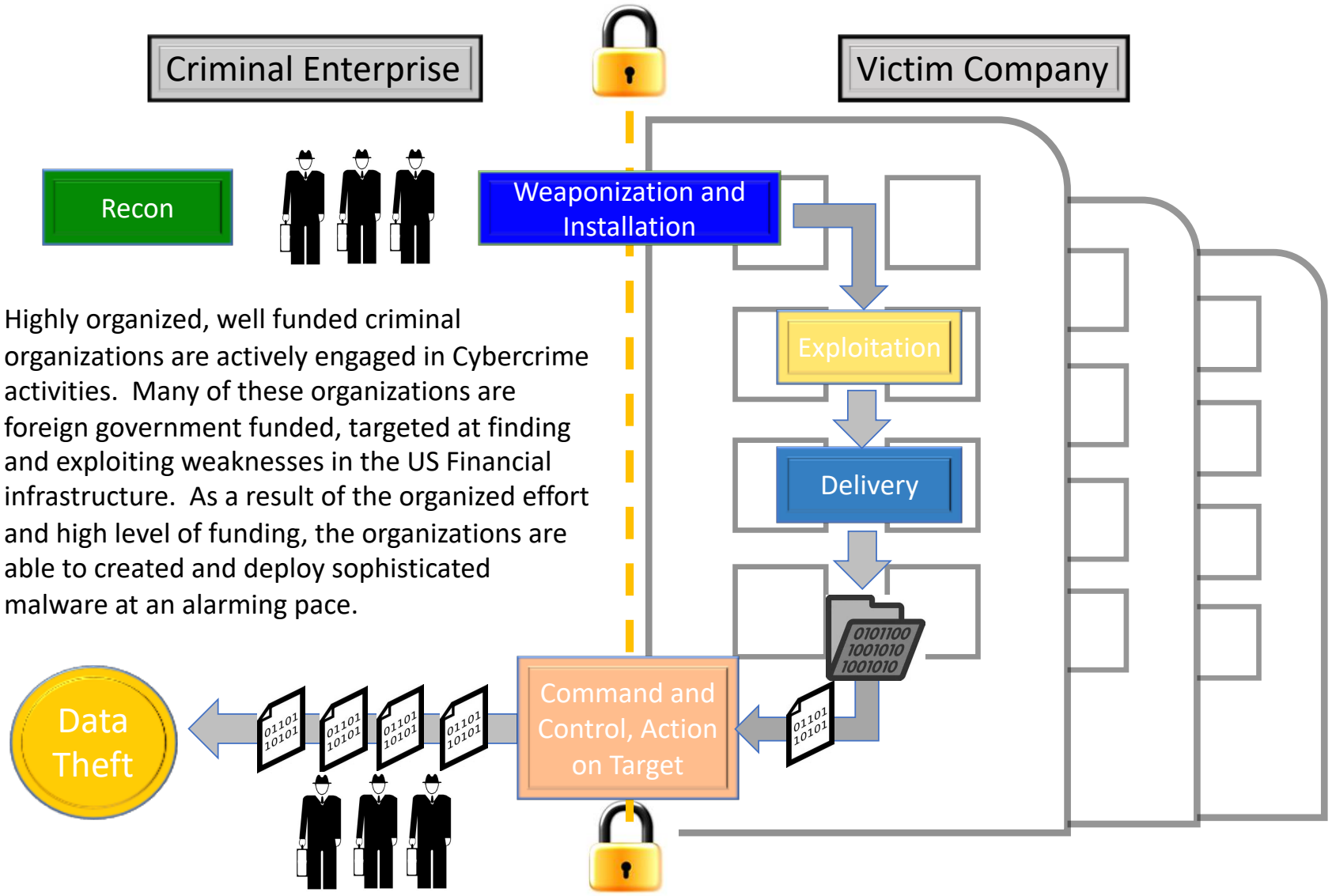
Action	Asset	Count
Hacking - Use of stolen creds	Server - Mail	43
Social - Phishing	Server - Mail	41
Hacking - Use of backdoor or C2	User Dev - Desktop	17
Malware - C2	User Dev - Desktop	16
Physical - Skimmer	Kiosk/Term - ATM	16
Misuse - Privilege abuse	Server - Database	14
Hacking - Use of stolen creds	Server - Web application	10
Social - Phishing	User Dev - Desktop	10
Error - Misdelivery	User Dev - Desktop	9
Malware - Backdoor	User Dev - Desktop	9

Technology Alone Can’t Make You Secure



- **Continuously train all employees through**
  - **Electronic learning - emerging threats & individual accountability**
  - **Department meetings & workstation security reminders**
- **Processes designed with a focus on**
  - **Segregation of duties across all critical areas**
  - **Continuously enhancing security to address evolving threats**
- **Implement security technology to**
  - **Enable enforcement of security protocols**
  - **Leverage security data to identify risks**
  - **Recognize active threats using data & analytical information**

The Emerging Cybercrime Ecosystem



The Intrusion “Kill Chain”

A kill chain is a systematic process to target and engage an adversary to create desired effects. Originally defined by the military to describe the process of finding and eliminating a threat, the concept has been adopted to describe the attack and exploitation process used by computer criminals. This is an integrated, end-to-end process described as a “Kill Chain" because any one deficiency will interrupt the entire process.

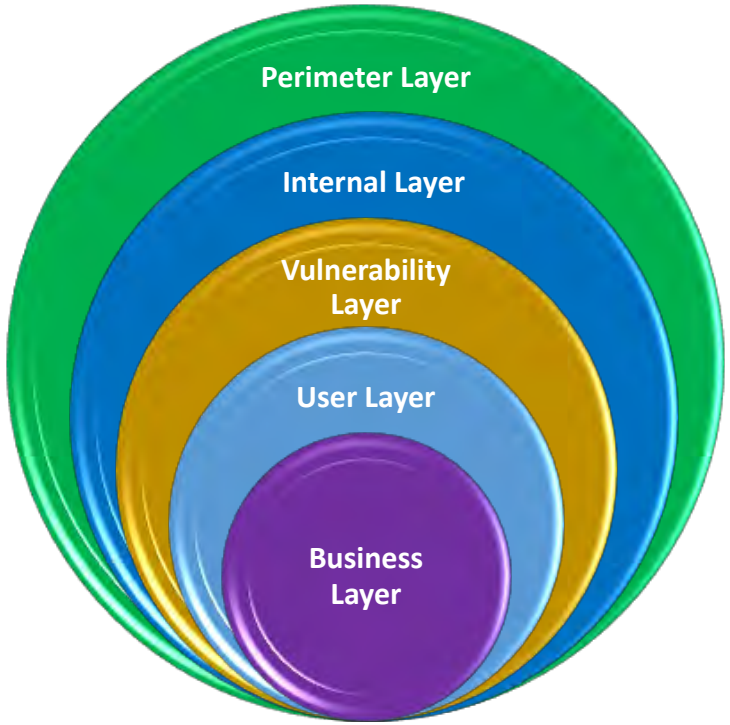
Rather than focusing all cyber protection efforts at one point (i.e. the perimeter), network and information defenses are designed to interrupt the “kill chain” at multiple layers in the system. This yields a much more robust security infrastructure that traditional methods.

Intelligence Driven Defense Approach

- Pragmatic approach
- Core set of best practices (NIST/ISO/COBIT/SOX)
- Combination of automated/manual controls, processes, and people/functions
- Defenses tuned as required by actionable intelligence – not static.

Information Security defined five layers of protection:

- ✓ **Perimeter Layer - To detect, block and remediate internal and external attacks** at the network level
- ✓ **Internal Layer - To detect, block and remediate internal and external attacks** at the host and client level
- ✓ **Vulnerability Layer - To detect, and reduce threats and vulnerabilities** to systems, applications and databases
- ✓ **User Layer - To safety support authorized users**
- ✓ **Business Layer - To minimize business losses and maximize effectiveness**



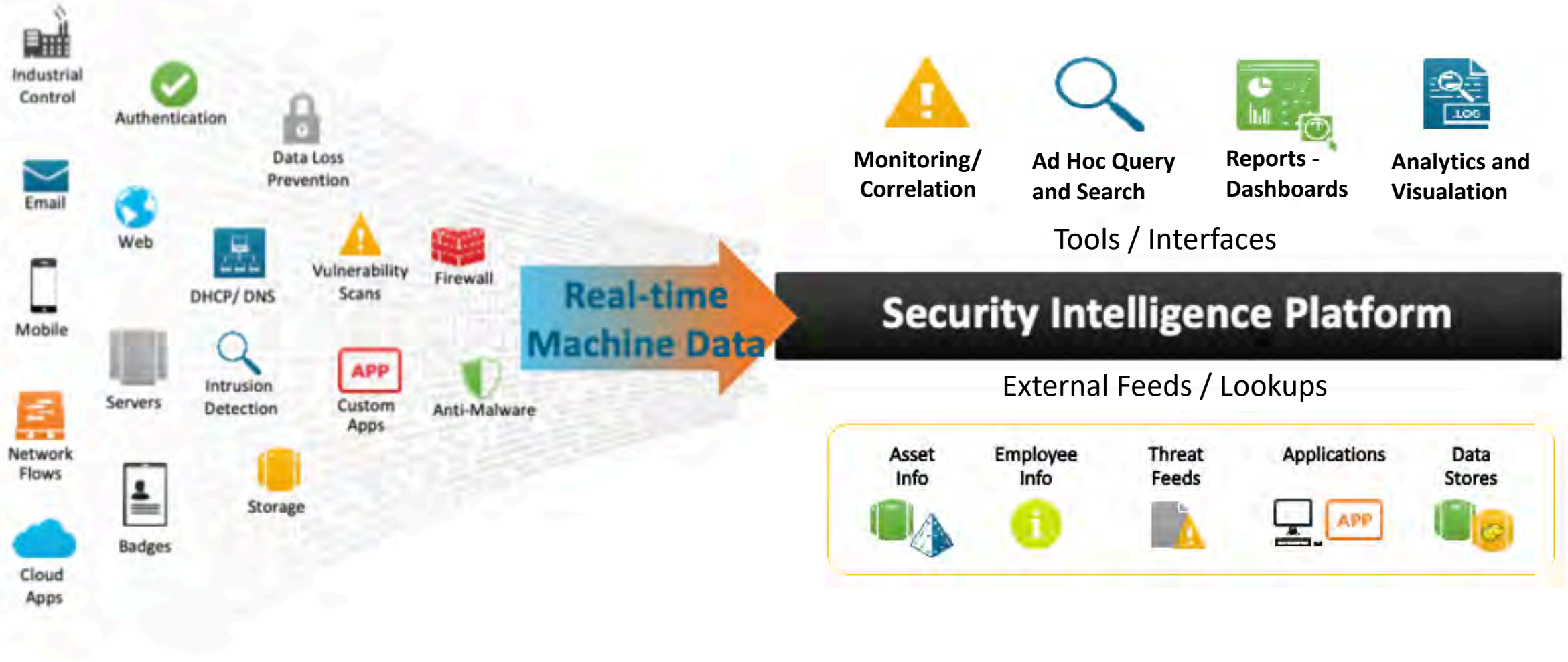
Interrupting the “Kill Chain”

	Perimeter Layer	Internal Layer	Vulnerability Layer	User Layer	Business Layer
“Kill Chain” Phase	Recon	Coding, Installation, Action on Target	Recon, Coding, Exploitation	Delivery	Command & Control, Action on Target
Layer Definition	To detect, block and remediate attacks at the network level	To detect, block and remediate internal and external attacks at the host and client level	To detect/stop threats and vulnerabilities to systems, applications and databases	To safety support authorized users	To minimize business losses and maximize effectiveness
Mitigating Controls	Firewalls	Network Access Control	Patch Management	Identity and Access Management	GRC Compliance
	IDS/IPS	System Checking and Monitoring	WAF	Anti-Spam	Awareness and Training
	System Behavior Analysis	Network Discovery Tools	Data Encryption at Rest	Anti-Malware	Threat Feeds and Analysis
	Malware Detection Gateway	Integrity checking and hardening	Dynamic Code Analysis	Secure Gateways Content Monitoring	Incident Response
	Analytics	Gold Image	Configuration and Policy Monitoring	Mobile Device Management	BCP/DR
	Data Encryption in Motion	End Point Security	Network System Vuln. Management		Media Sanitization
	Audit Log Store		HIPS		

What If We Could Predict Bad Acts?

- What if we could stay ahead of threat actors and predict their next attack before they take their first destructive step?
- Predictive analytics is the science that is gaining momentum in virtually every industry and is enabling organizations to modernize and reinvent the way they do business by looking into the future and obtaining foresight they lacked previously.
- This rising trend is now finding its way into the domain of cybersecurity, helping to determine the probability of attacks against organizations and agencies and set up defenses before cybercriminals reach their perimeters.

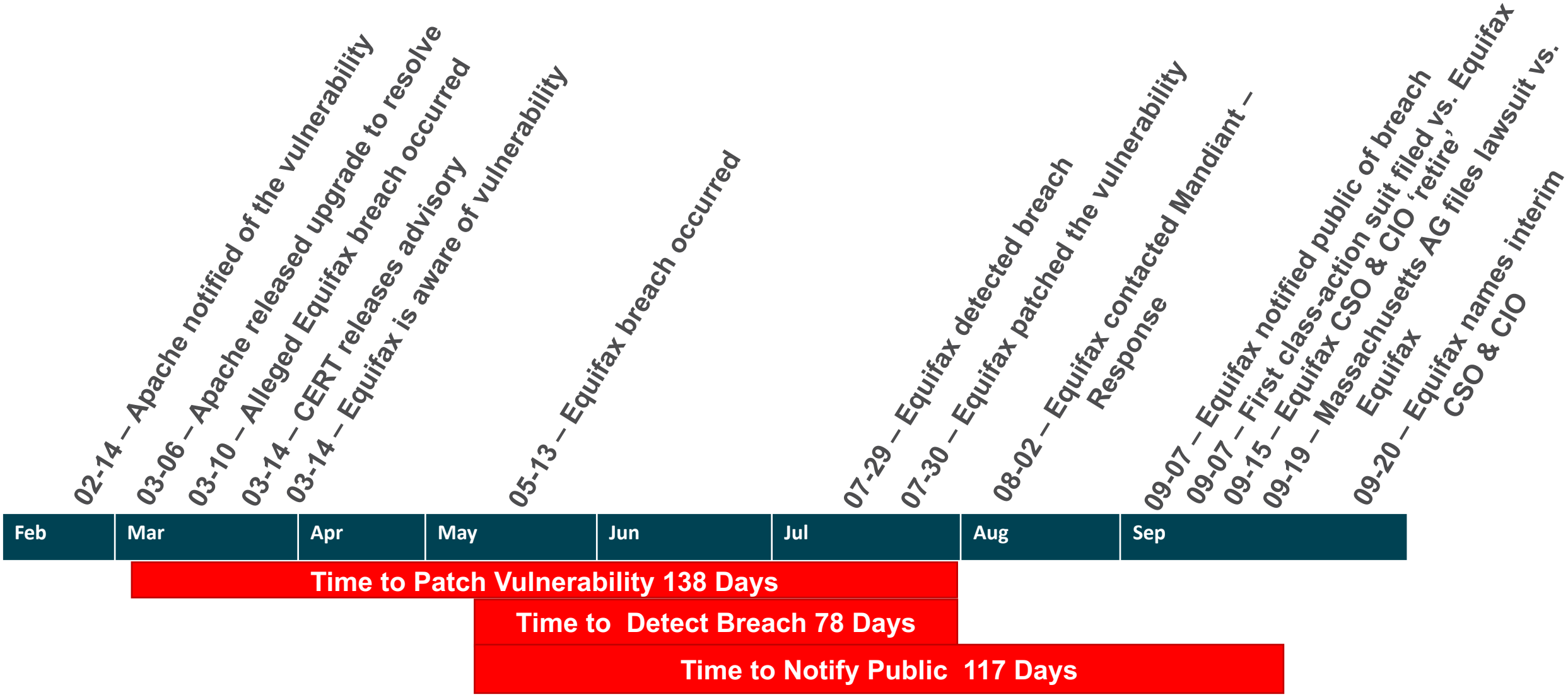
Applying Analytics to Security Questions



The Hardest to Detect: Inside Job

- There were 45 confirmed breaches associated with misuse of privileges.
- The details were light on most of these but tried and true controls are still relevant.
- Monitor and log access to sensitive financial data (which we think you are already)
- Make it quite clear to staff that it is being done and just how good you are at recognizing fraudulent transactions.
- In other words, “Misuse doesn’t pay.”

Case Study: Equifax Timeline



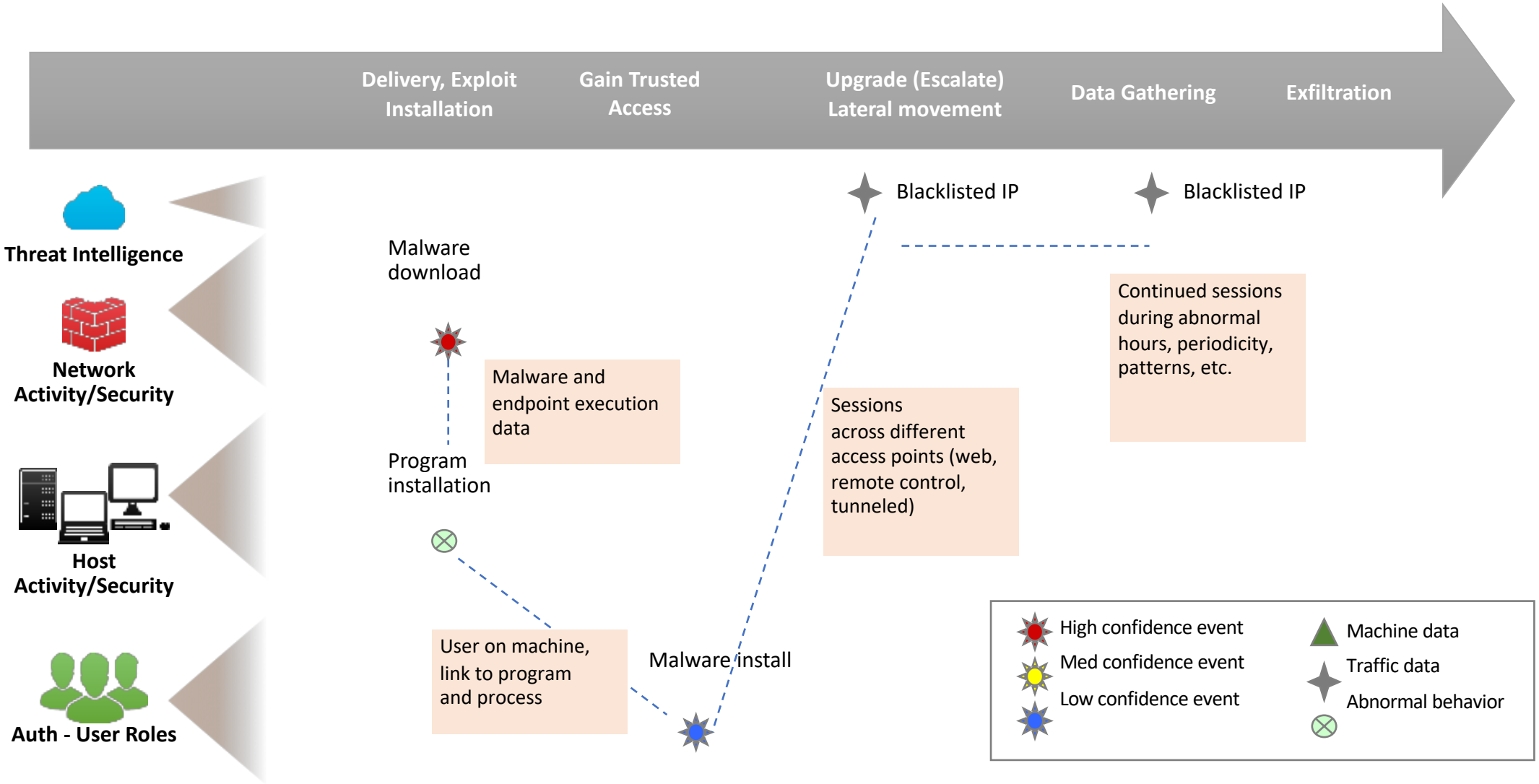
Insider Threat

Problem: **Data Theft is a significant issue today – Affects costs and member goodwill**

Problem: **Detection takes too long today**

Solution: **Build a predictive model to identify and alert on anomalous transfer patterns and behavior**

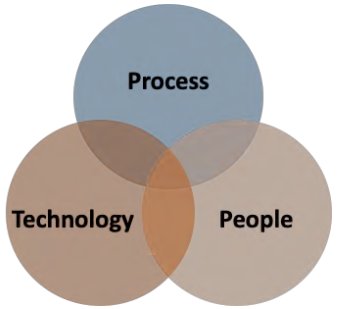
- Data Access and Transfer
- Establish Predictive Model
- Define/Refine “Normal Behavior”
- Detect significant deviations
- Investigate


Delivery, Exploit Installation
Gain Trusted Access
Upgrade (Escalate) Lateral movement
Data Gathering
Exfiltration
Threat Intelligence
Network Activity/Security
Host Activity/Security
Auth - User Roles
Malware download
Malware and endpoint execution data
Program installation
User on machine, link to program and process
Malware install
Blacklisted IP
Blacklisted IP
Continued sessions during abnormal hours, periodicity, patterns, etc.
Sessions across different access points (web, remote control, tunneled)
High confidence event
Med confidence event
Low confidence event
Machine data
Traffic data
Abnormal behavior

Moving beyond signatures

- The traditional approach to fighting cyberattacks involves gathering data about malware, data breaches, phishing campaigns, etc., and extracting relevant data into signatures, i.e. the digital fingerprint of the attack. These signatures will then be compared against files, network traffic and emails that flow in and out of a corporate network in order to detect potential threats.
- While signature-based solutions will continue to remain a prevalent form of protection, they do not suffice to deal with the advanced and increasingly sophisticated cybercriminals who threaten organizations.
- A Verizon Data Breach Investigations Report reveals that more than 50 percent of data breaches remain undiscovered for months. In contrast, thanks to the array of innovative malware, botnets and other advanced data-theft tools at their disposal, attackers only need minutes to gain access to the critical data they seek after they compromise a target.
- The variety and volume of data involved in identifying and predicting security threats are overwhelming.

Predictive analytics is not panacea

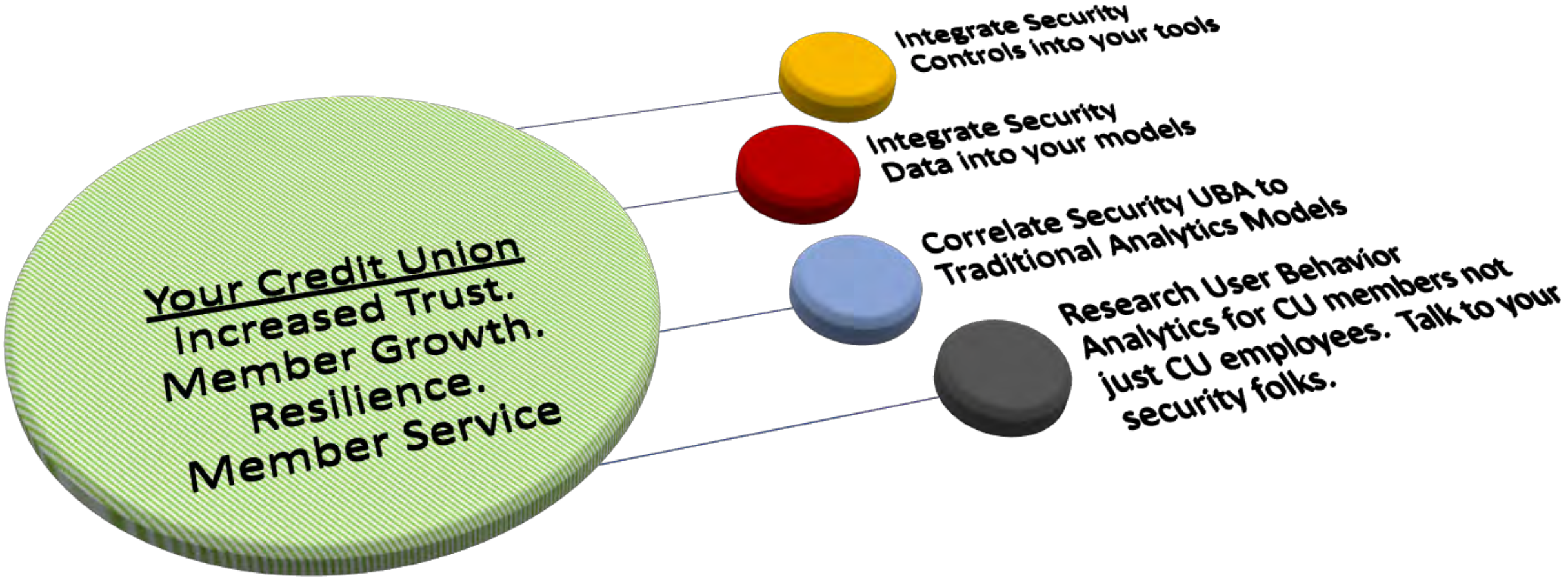


- Firstly, the value and volume of online assets are exploding at and exponential rate.
- Secondly, hackers are increasingly growing in sophistication due to their easy and inexpensive access to large compute resources through cloud computing.
- Think first:
  - Rethink why and how you store valuable data in the first place
  - Rethink Training Programs
  - Review Processes, Remove Unnecessary Steps

Predictive analytics will have a pivotal role in shaping the future of cybersecurity

- **Predictive analytics and machine learning**
- Predictive analytics in security provide a forecast for potential attacks — but no guarantees
- Must be coupled with the right machine learning solution in order to be able to harness its full potential.
- Signature Free – Detect previously unknown threats
- Detect Hidden Trends
- The use of predictive analytics coupled with machine learning and natural language processing allows for cybersecurity to move beyond the cumbersome strategy of maintaining black-lists.

Homework….


Your Credit Union
Increased Trust.
Member Growth.
Resilience.
Member Service
Integrate Security Controls into your tools
Integrate Security Data into your models
Correlate Security UBA to Traditional Analytics Models
Research User Behavior Analytics for CU members not just CU employees. Talk to your security folks.

Time for Action