Society Protection – Best Practices from Industry

The Nuts and Bolts
of the Dynamic Attack Chain

October 2015

You are an...

IT Security Manager (and a father of three teenagers – his wife is working in GOV site) at a an entity with 20 remote locations.

Managing a team of personnel that are responsible for maintaining remote/network operations & maintenance for his entity website and few applications.

Other areas have credentials for various applications to enable them to conduct business.

Monday 8:30am

Over a cup of tea, he gets a phone call from a well-known security blogger that your Internet-accessible server addresses showed up on an underground forum known for trading stolen information.

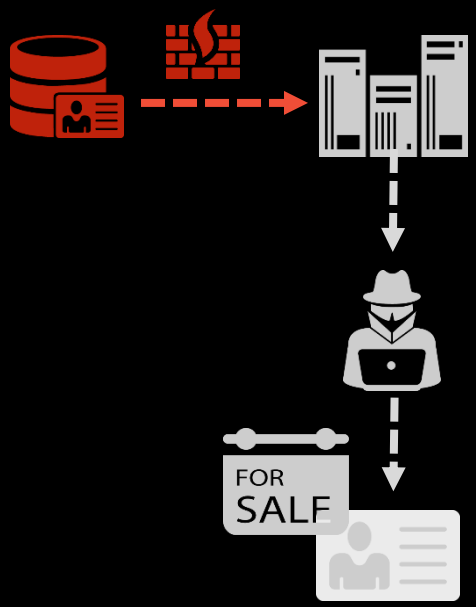
What is next … is your take home exercise

The previous Saturday

Investigating the server logs from the weekend shows a connection from a POS server to an external ABC server you don't recognize, hosted at the dynamic domain 1337.myABC-ftp.biz.

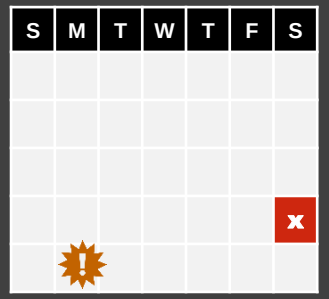
The attacker must have manually copied excerpts of the data

from the FTP server to the underground forum.



IBM Threat Protection System:

- Prevent
- Detect
- Respond



Attack Chain Stage:

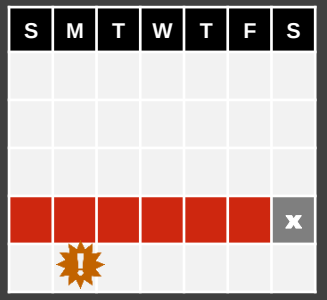
- Break-In
- Latch-on
- Expand
- Gather
- **Exfiltrate**

The previous week

You find evidence in the log files of transfers of DEF in the previous week from POS servers to a single internal server, the server that connected to the external FTP server.

IBM Threat Protection System:

- Prevent
- Detect
- Respond

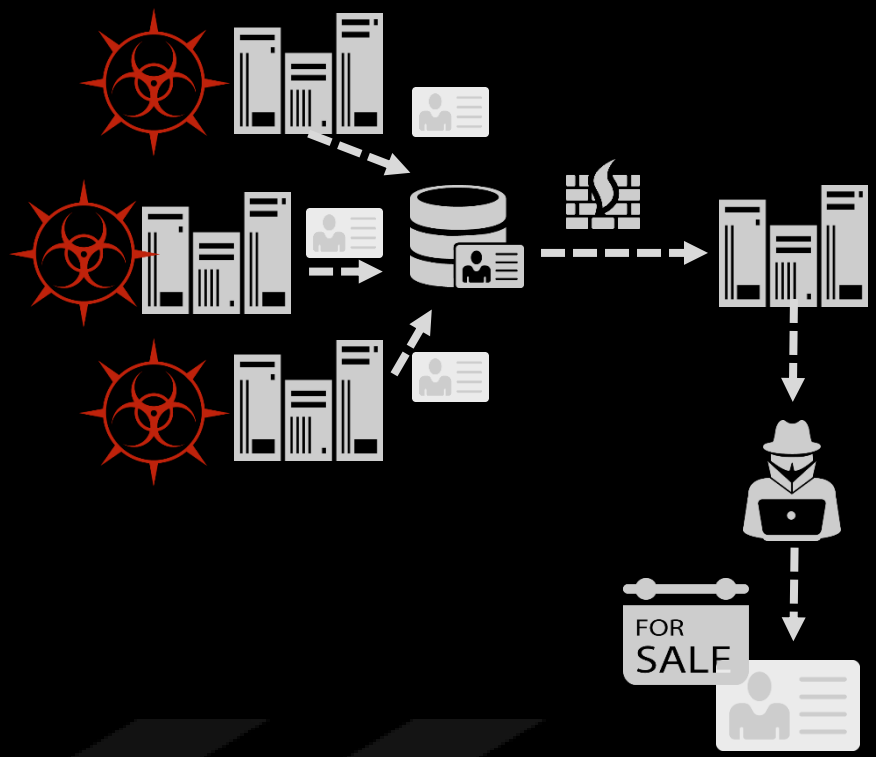


Attack Chain Stage:

- Break-In
- Latch-on
- Expand
- **Gather**
- Exfiltrate

The previous 2-3 weeks

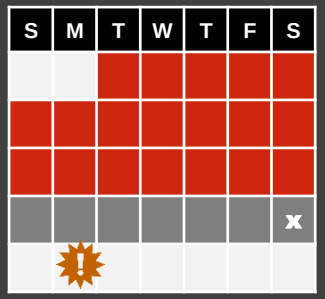
You find a copy of the file ccper.exe on each of the POS servers that sent DEF to the server that made the external connection.



In the 2-3 week prior, that malware (and ransomware) hunted for additional POS servers, copying toolchains and password crackers to them, and infiltrating the network.

IBM Threat Protection System:

- Prevent
- Detect
- Respond



Attack Chain Stage:

- Break-In
- Latch-on
- **Expand**
- Gather
- Exfiltrate

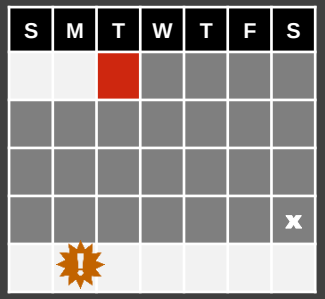
28 days earlier

Probing further, you find a RAT (Remote Access Trojan) named svch0st.exe, which acted as a dropper to secretly install, execute, and avoid anti-virus detection.

This program downloaded ccper.exe from an external server located at IP Address XXX.XXX.73.32 and copied it to the POS servers.

IBM Threat Protection System:

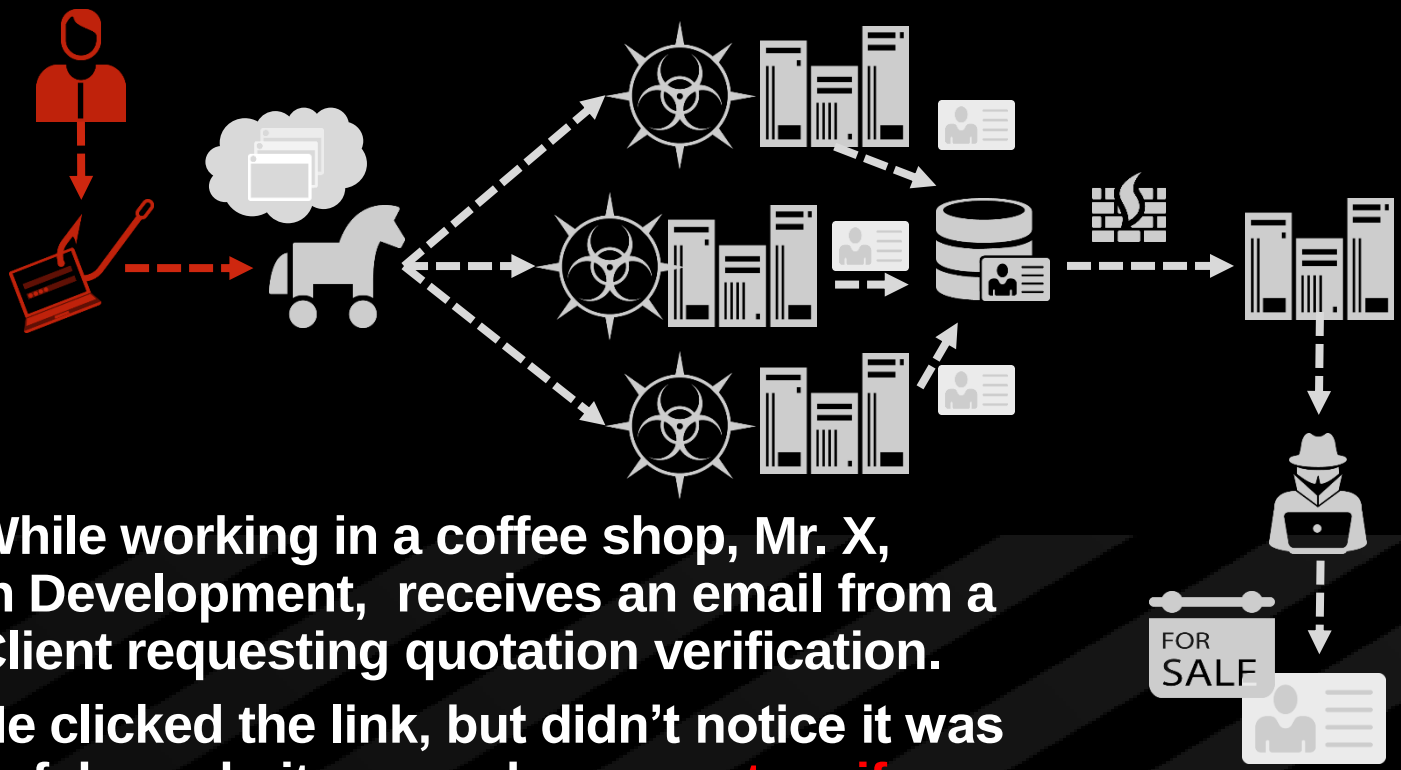
- Prevent
- Detect
- Respond



Attack Chain Stage:

- Break-In
- **Latch-on**
- Expand
- Gather
- Exfiltrate

29 days earlier



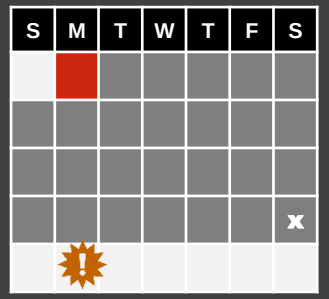
While working in a coffee shop, Mr. X, in Development, receives an email from a Client requesting quotation verification.

He clicked the link, but didn't notice it was to fake website named acccount-verify.com, which launched a zero-day exploit to his browser and downloaded the trojan svch0st.exe to his system.

Mr. X drives to work where he logs into the network, allowing svch0st.exe to slip into the network and start the chain of events leading to the breach.

IBM Threat Protection System:

- Prevent
- Detect
- Respond



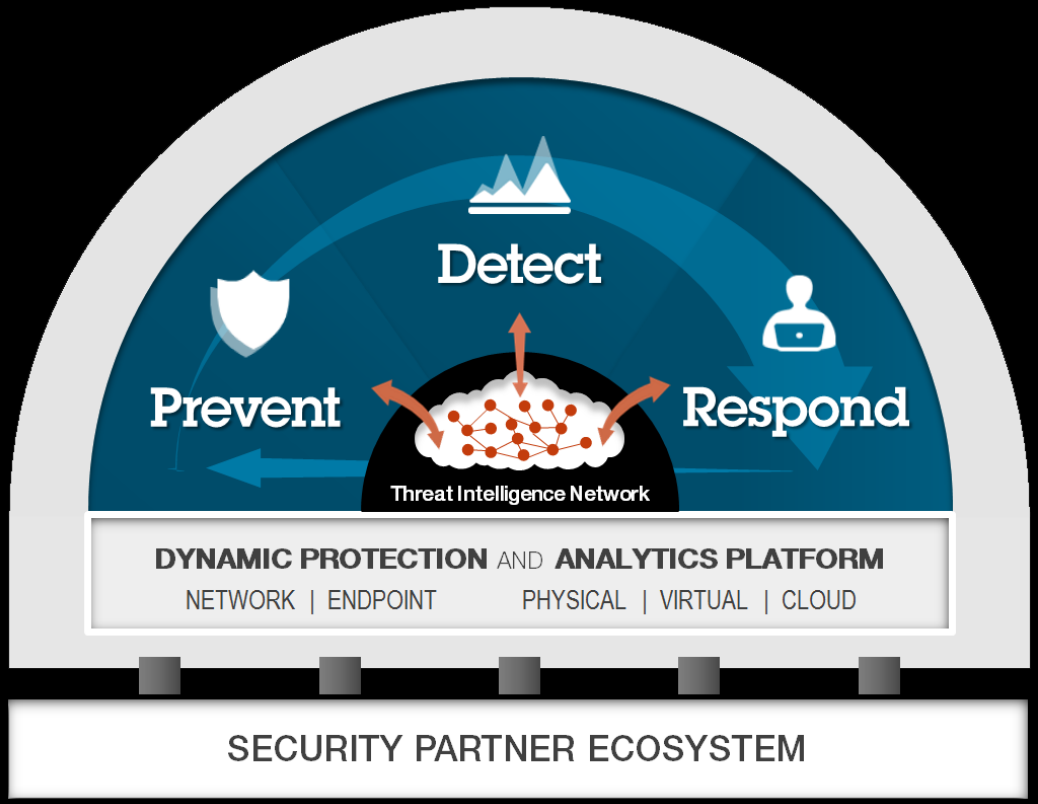
Attack Chain Stage:

- **Break-In**
- Latch-on
- Expand
- Gather
- Exfiltrate

Let's start from the beginning to see how the attack could have been disrupted...

IBM Threat Protection System

A dynamic, integrated system to disrupt the entire lifecycle of advanced attacks



Smarter Prevention

Stop unknown threats with behavioral-based defenses on both the endpoint and network

Security Intelligence

Automatically detect weaknesses and anomalies with enterprise-wide visibility and insights

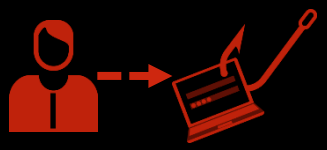
Continuous Response

Quickly understand incidents and use findings to strengthen real-time defenses

Open Integrations

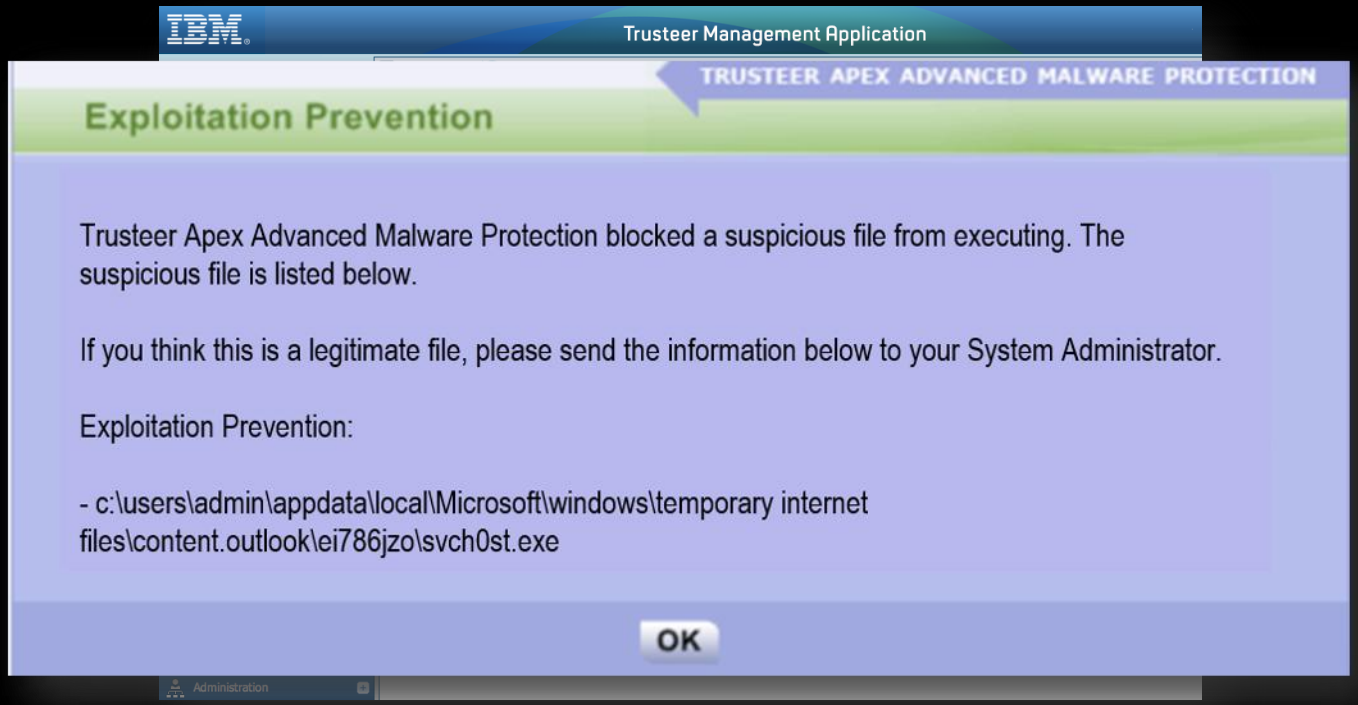
Share context between domains and third party products using an open platform and ecosystem

29 days earlier



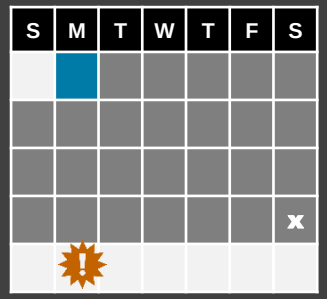
Mr. X is the subject of a scam and more

IBM Security Advanced Malware Protection stops the zero-day exploit from attacking his web browser and executing the RAT named “svch0st.exe”



IBM Threat Protection System:

- Prevent
- Detect
- Respond



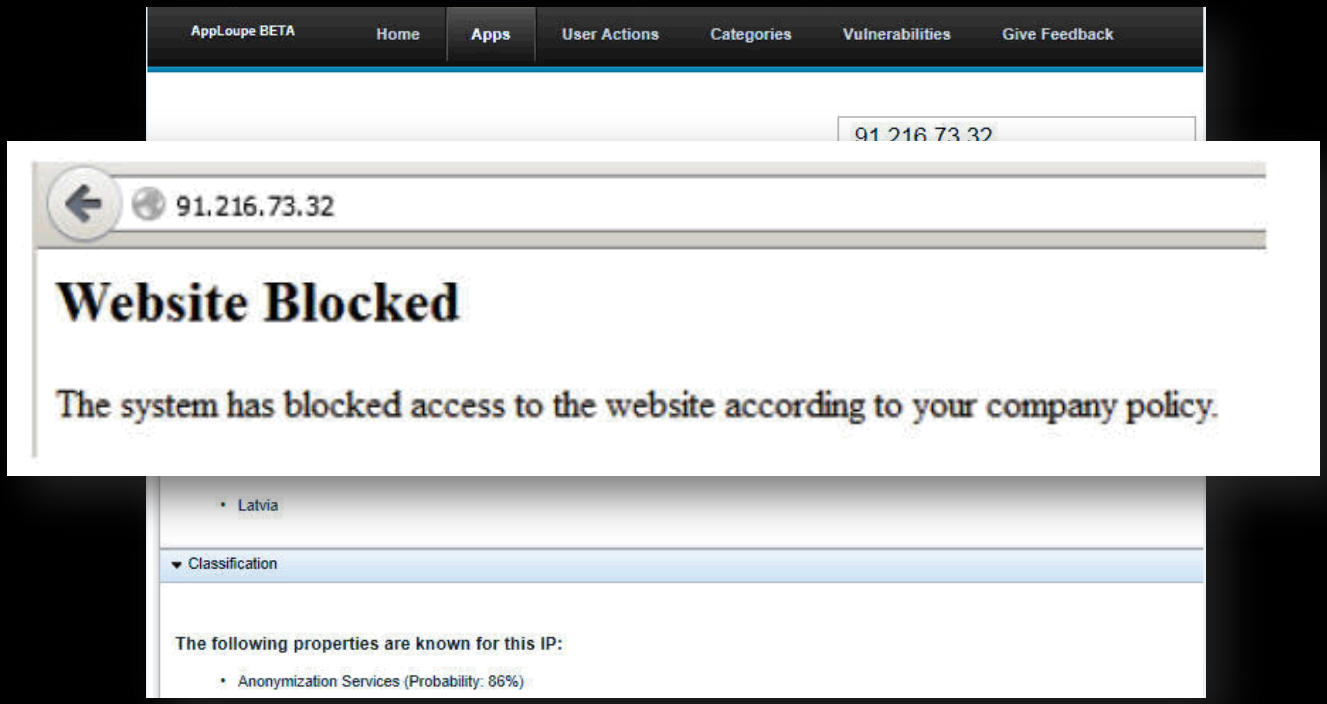
Attack Chain Stage:

- **Break-In**
- Latch-on
- Expand
- Gather
- Exfiltrate

28 days earlier

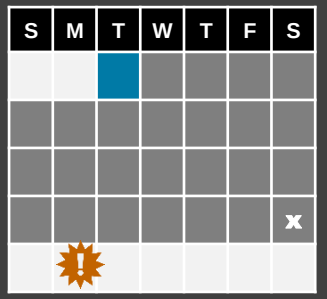
The RAT downloads ccper.exe and the malware starts to replicate

IBM Security Network Protection prevents C&C activity on the server by blocking the remote IP 91.216.73.32 hosting ccper.exe based on IP reputation



IBM Threat Protection System:

- **Prevent**
- Detect
- Respond



Attack Chain Stage:

- Break-In
- **Latch-on**
- Expand
- Gather
- Exfiltrate

28 days earlier

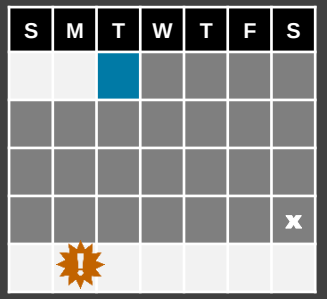
The RAT downloads ccper.exe and the malware starts to replicate

IBM technologies detects the RAT install from system event logs, giving it a magnitude score of 8 and raising a flag in the security analyst's dashboard

Event Information			
Event Name	HTTP:HOTMAIL:EXE-DOWNLOAD		
Low Level Category	Executable Code Detected		
Event Description	HTTP: MSN Hotmail Executable File Extension Download		
Magnitude	(8)	Relevance	10
Username	N/A		
Start Time	Oct 20, 2013, 7:22:48 PM	Storage Time	Oct 20, 2013, 7:22:48 PM
Executable (custom)	CardScraper.exe		

IBM Threat Protection System:

- Prevent
- **Detect**
- Respond



Attack Chain Stage:

- Break-In
- **Latch-on**
- Expand
- Gather
- Exfiltrate

The previous week

PII was transferred from infected POS servers to a single server

IBM Security Network Protection and communication behavior technologies detects and blocks the transfer of the credit card number files

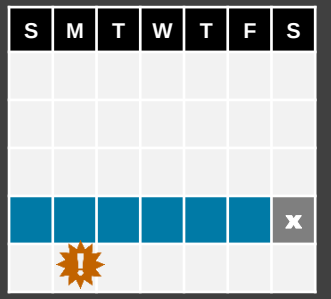
Tag Name	Status	Severity	Event Count	Source Count	Target Count
Content_Analyzer_Credit_Card_Num	Detected event	Low	1	1	1
System	Detected event	Low	19	2	2
HTTP_Get	Detected event	Low	6	1	1
EventCollector_Info	Detected event	Low	39	1	1

Tag Name	Status
Content_Analyzer_Credit_Card_Num	Detected event

Source IP	Source Network	Source Port	Destination IP	Destination Port	Protocol	Application
10.0.110.37	POS_Server	64935	151.56.78.9	20	udp_ip	DataTransfer.FTP
10.0.110.120	POS_Server	64935	151.56.78.9	20	udp_ip	DataTransfer.FTP

IBM Threat Protection System:

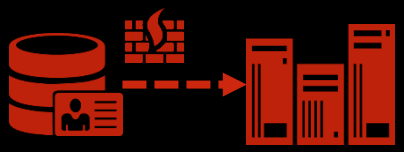
- **Prevent**
- Detect
- Respond



Attack Chain Stage:

- **Break-In**
- **Latch-on**
- **Expand**
- **Gather**
- **Exfiltrate**

The previous Saturday



A POS server connects to an unknown external FTP server and the PII is exfiltrated.

IBM technologies would detect anomalous flow out from a server that never connected outbound before with a "Connection Outbound to Internet from Critical Asset" flag

Id	Description	Offense Type	Offense Source	Magnitude	Source IPs
1471	Multiple Login Failures for the Same User containing Root Login Failed	Username	root		Multiple (10)
1458	Assess potential inbound connections from the internet to regulatory assets	Event Name	Assess potential inboun...		Multiple (5)
1463	Assess actual inbound connections from the Internet to regulatory assets	Event Name	Assess actual inbound c...		Multiple (5)
2670	Anomaly Detection: Connection Outbound to Internet from Critical Asset	Source IP	10.0.120.50		10.0.120.50
1482	Potentially Successful Exploit preceded by Exploit Followed by Suspicious Host Activity - Chained preceded by Multiple Vect...	Source IP	10.0.240.4		dhcp-4-users-1.ac...
1511	Attack Followed by an Attack Response preceded by Policy: Chat or IM Traffic Detected preceded by Exploit Followed by Su...	Source IP	10.0.230.231		dhcp-231-vpn.acm...
1461	Compliance: assess regulatory assets using insecure protocols	Event Name	Compliance: assess reg...		Multiple (5)

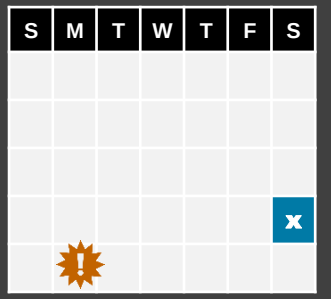
Assess actual inbound connections from the Internet to regulatory assets

Anomaly Detection: Connection Outbound to Internet from Critical Asset

Potentially Successful Exploit preceded by Exploit Followed by Suspicious Host Activity - Chained preceded by Multiple Vect...

IBM Threat Protection System:

- Prevent
- Detect
- Respond



Attack Chain Stage:

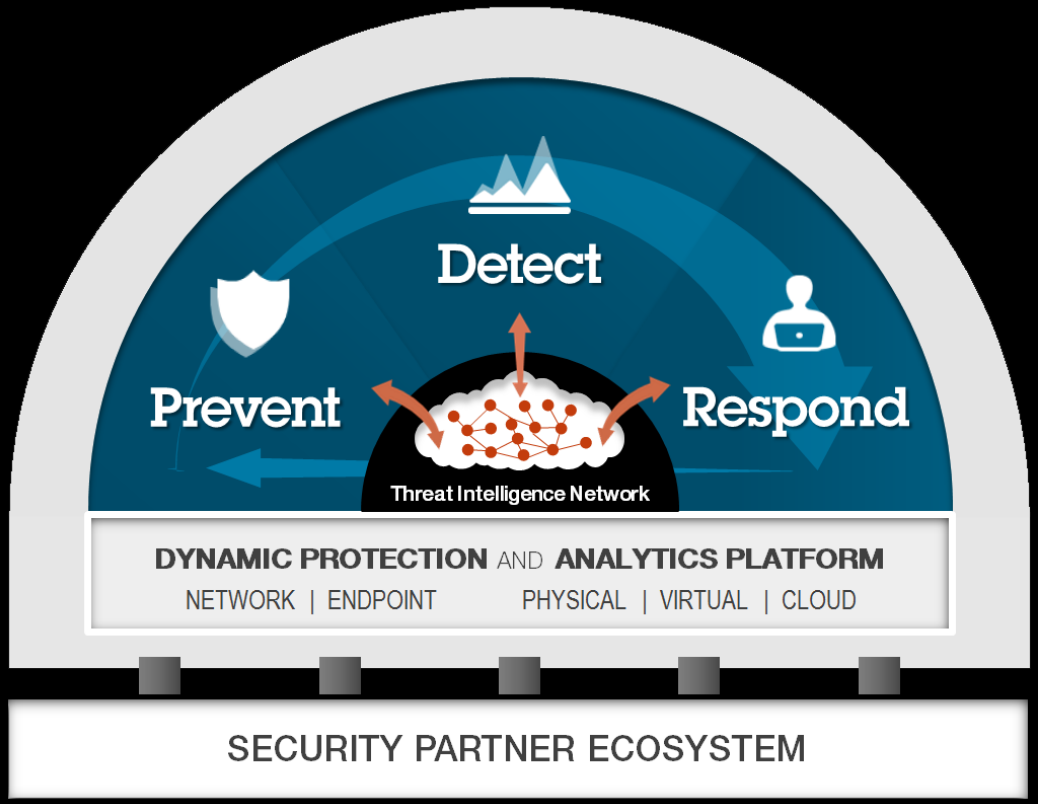
- Break-In
- Latch-on
- Expand
- Gather
- **Exfiltrate**

Where is the Society Protection Story?

1.
2.
3.

IBM Technologies to protect our Kids' access …

A dynamic, integrated system to disrupt the entire lifecycle of advanced attacks



Smarter Prevention

Stop unknown threats with behavioral-based defenses on both the endpoint and network

Security Intelligence

Automatically detect weaknesses and anomalies with enterprise-wide visibility and insights

Continuous Response

Quickly understand incidents and use findings to strengthen real-time defenses

Open Integrations

Share context between domains and third party products using an open platform and ecosystem

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Thank You

www.ibm.com/security