

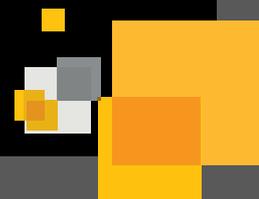


What's Your Incident Response Recipe?

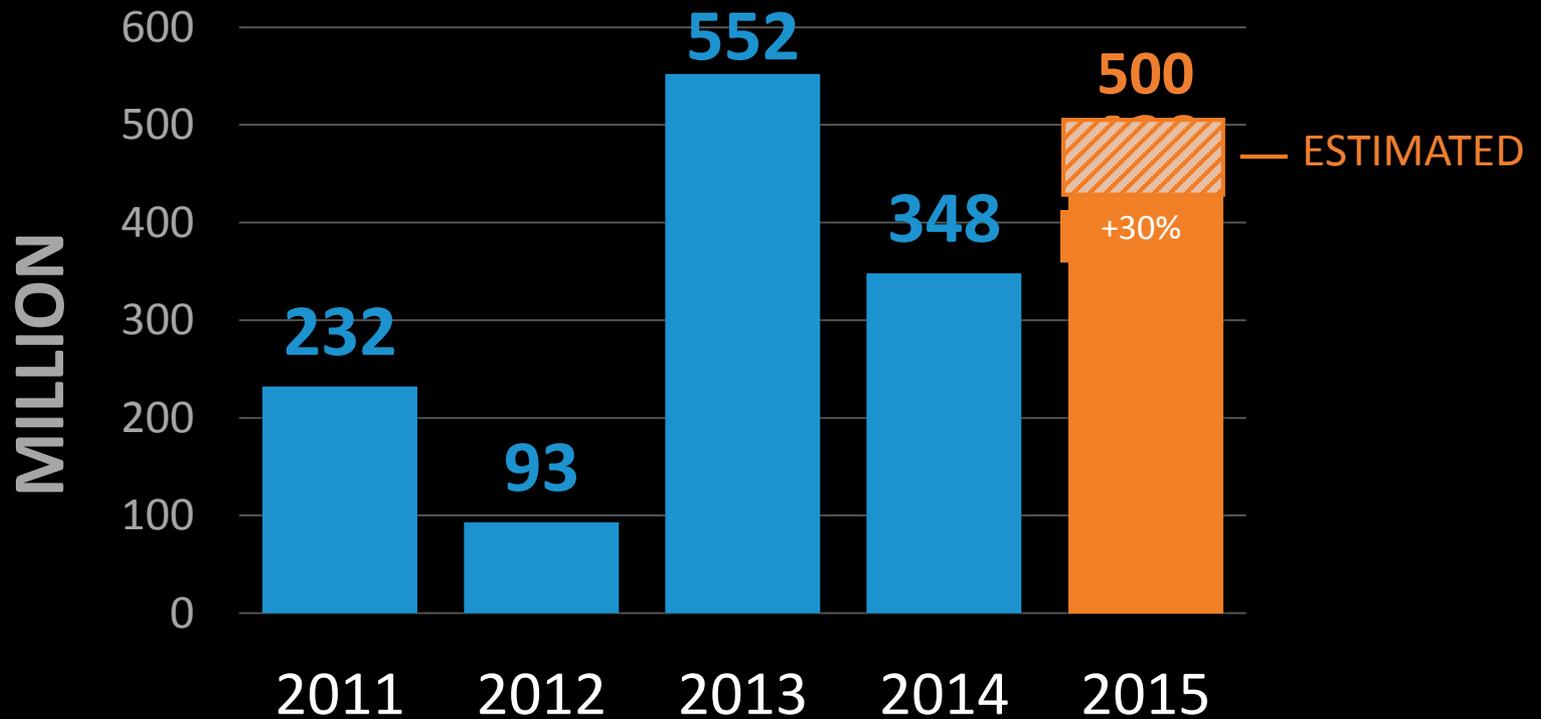
Renault Ross CISSP,MCSE,VCP5,CHSS

Chief Security Business Strategist
Symantec, North America

Is Compromise Inevitable?



Total Identities Exposed



In 2009 there were

2,361,414

new piece of malware created.

In 2015 that number was

430,555,582

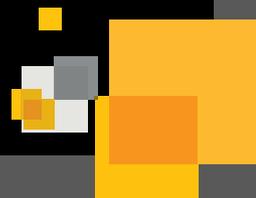
That's

1 Million 179 Thousand

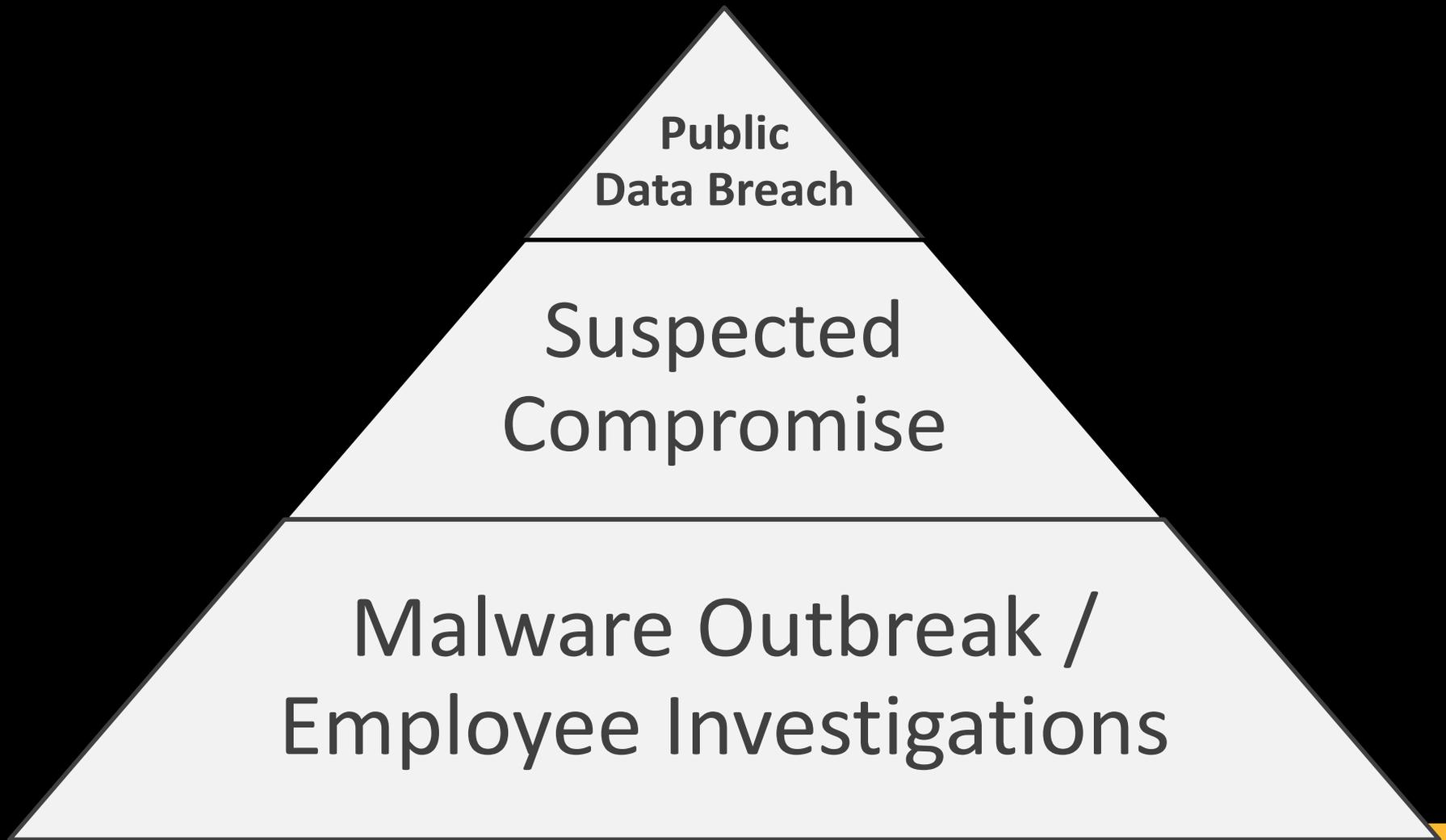
a day.



TWO TEAMS INDICTED!



Are all “Incidents” the same?



Proactive or Reactive?

Crisis Mode



- Experiencing a **security incident**
- Internal teams **unable to address issue** at hand
- **Pressure to resolve** the incident **quickly**
- Need to address legal/compliance **reporting requirements** post-incident
- Currently battling an incident and **need extra help**
- **Media coverage** of breach

Elevated Concern



- Realization that **gaps in security** may have led to an **undetected breach**
- Industry **peer suffered a breach** and they want to know **if they have been impacted**
- New **security alert** or intelligence that causes concern and the customer has **no way to determine if they might be impacted**

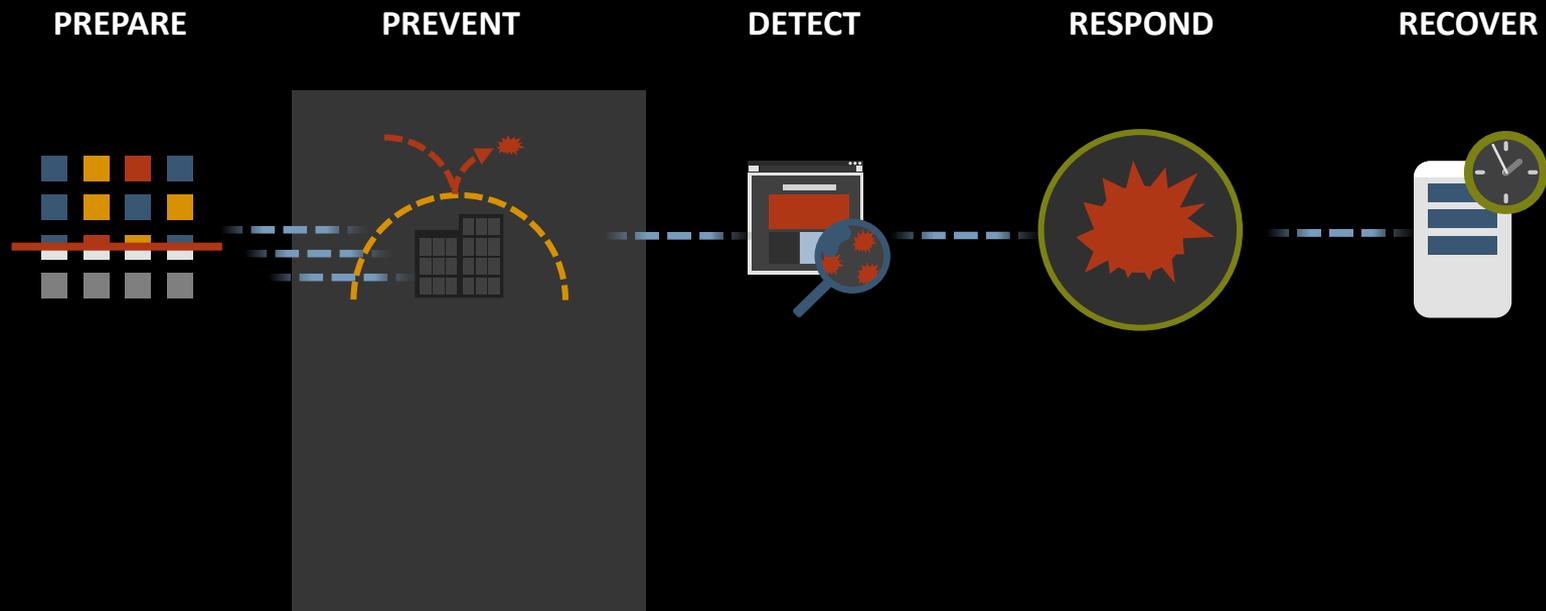
Proactive Planning



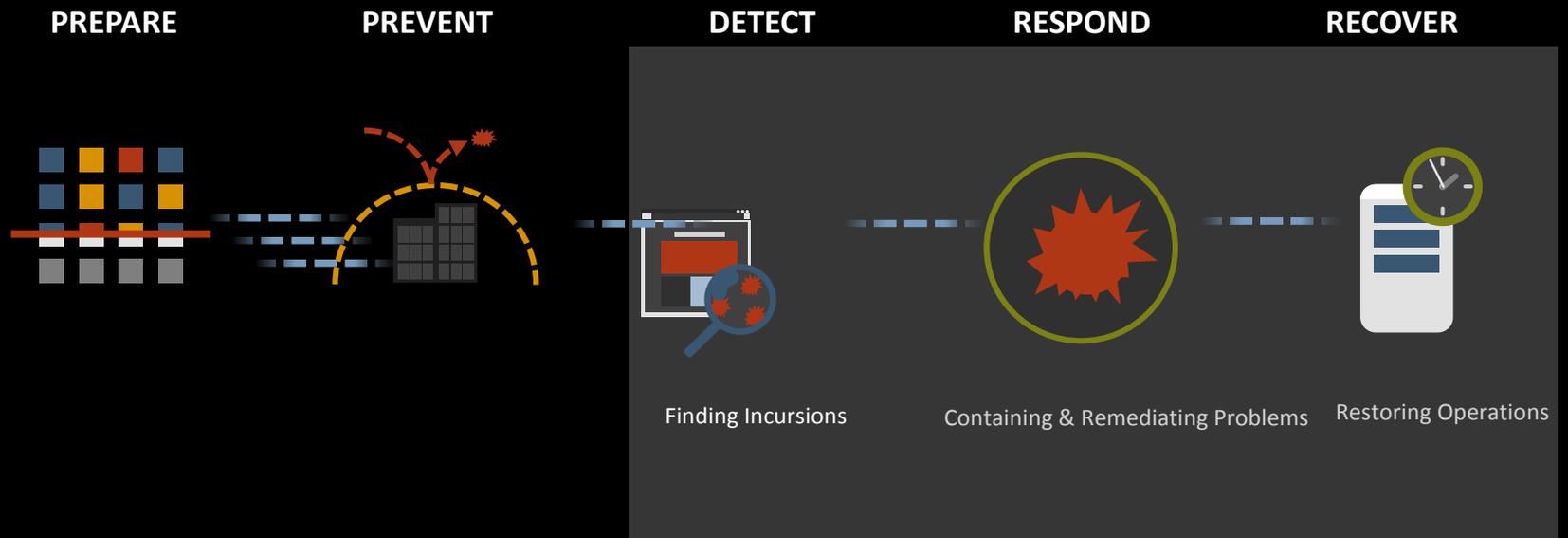
- Looking to turn **plans into optimized programs**
- Looking for ways to **improve or augment internal IR capabilities**
- Want to **pre-negotiate terms and rates** for faster action when 3rd party help is needed
- Have a **regulatory or legal requirement** to have a 3rd-party IR team on retainer



CAN YOU STOP ALL THREATS?



RECOVERY IS THE KEY!



CYBER SECURITY FRAMEWORK

Improving Critical Infrastructure Cybersecurity

Executive Order 13636

February 2013



“It is the policy of the United States to enhance the security and resilience of the Nation’s critical infrastructure and to maintain a **cyber environment** that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties.”



FUNCTIONS: HIGH-LEVEL GOALS

Functions		
ID	Identify	Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities
PR	Protect	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services
DE	Detect	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event
RS	Respond	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event
RC	Recover	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services



CATEGORIES: SPECIFIC ACTIVITIES

Function	Categories		
Identify (ID)	ID.AM	Asset Management (AM)	The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.
	ID.BE	Business Environment (BE)	The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
	ID.GV	Governance (GV)	The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cyber risk.
	ID.RA	Risk Assessment (RA)	The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
	ID.RM	Risk Management Strategy (RM)	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions .



WAYS TO USE THE FRAMEWORK

Basic
Review
of
Cybersecurity
Practices



“How well are
we doing
today?”

Establishing
or Improving
a
Cybersecurity
Program



“Can we assess
and improve?”

Let's focus here

Communicating
Cybersecurity
Requirements
with
Stakeholders



“Can we speak
the same
language?”

Identifying
Opportunities
for Updated
Informative
References



“What else
should we
consider?”

Methodology
to
Protect Privacy
and
Civil Liberties

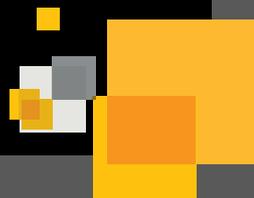


“Can we protect
data better?”



The Goals Of Incident Response

- Primary Goal of Incident Response:
 - Effectively remove a threat from the organization's computing environment, while minimizing damages and restoring normal operations as quickly as possible.
- Primary Goal is Accomplished Through Two Main Activities:
 - Investigation: Involves Diagnosis, Analysis and Containment Strategy
 - Remediation: Involves Containment, Mitigation and Remediation
- What Else Should Be Involved For A More Comprehensive Incident Response?



Incident Response Today

Un-prioritized Alerts



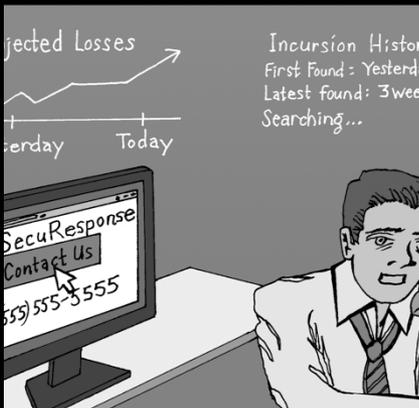
Manual IR Call Trees



Triage Begins



External Response Team Called



Delays in Ramp-up



Manual Correlation of Evidence

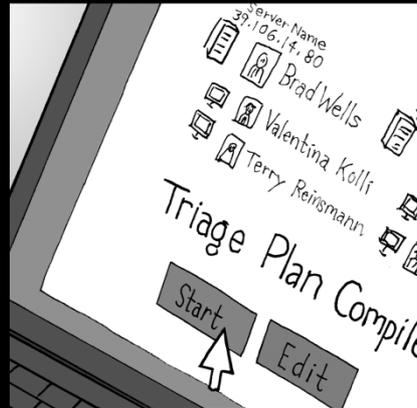


Incident Response Tomorrow

Prioritized/Correlated Alerts



Automated Triage Workflow



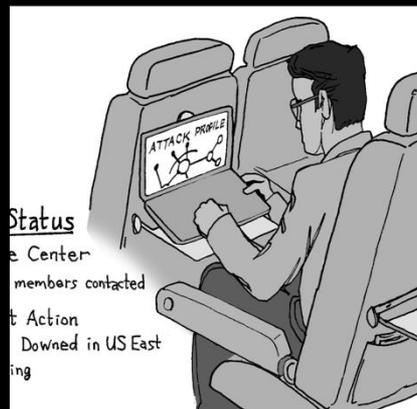
Collaborative Triage



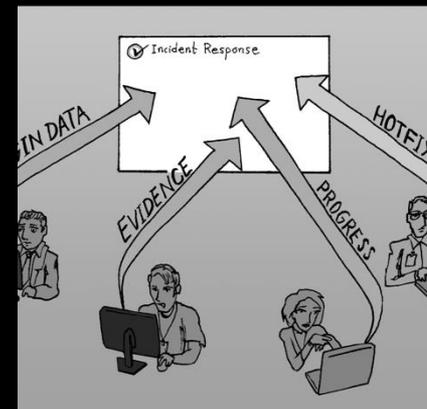
Clear Line of Site



Real-time updates



Collaborative Response



Incident Response Recipe

1	Threat Identification & Intelligence
2	3 rd Party Security Services
3	Incident Response
4	Cyber Team Readiness
5	Conclusion



Threat Identification & Intelligence

Security Intelligence Defined

collection

analysis

**impacts
risk posture**

**actionable insight
lowers security risk**



Threat Identification & Intelligence

Intelligence Use Cases

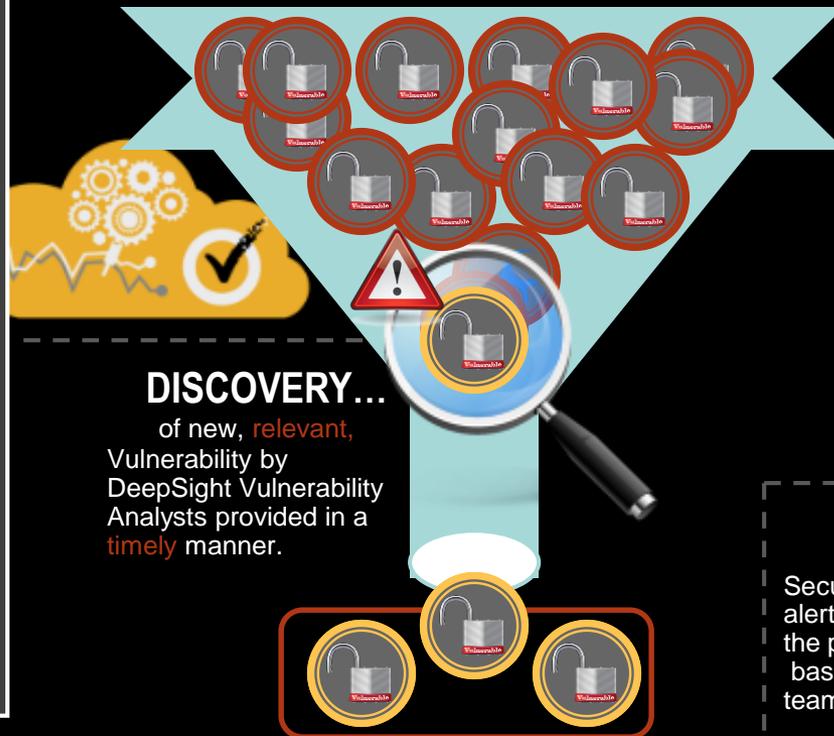
Use **Vulnerability alerts** and **Vulnerability datafeeds** to help identify and prioritize vulnerabilities based on technologies relevant to an organization

State of NY IT Products
in the organization



SETUP "TECH LIST"

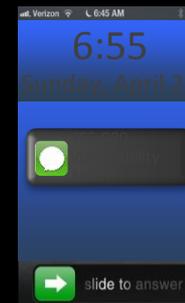
Security Analyst sets up a "Tech List" on the DeepSight portal to match the products being used in the organization



DISCOVERY...

of new, **relevant**,
Vulnerability by
DeepSight Vulnerability
Analysts provided in a
timely manner.

GET ALERTERED



FOR ORGANIZATIONS,
using **DeepSight Portal**,
Security Analysts receives an
vulnerability alert based on the
"Tech List" that was setup via
SMS or email

FOR ORGANIZATIONS, using
DeepSight Datafeeds,
DeepSight Vulnerability
intelligence is 'fed' into customer
governance, risk and compliance
(GRC) systems.

Irrespective of org size, product vulnerabilities including info such as: CVSS Scores, Exploit details, Work Around, Solution & Fix, Availability of a Patch, and more.

APPLY PATCHES

Security Analysts tracks the vulnerability via DeepSight alerts and/or feeds and applies the patch as and when it becomes available based on priority. Thus allowing security team to **focus** on securing IT systems.



Threat Identification & Intelligence Intelligence Use Cases

Adversary Intelligence - Portal

ADVERSARY INTELLIGENCE



Director of Security of a financial services company in the US, receives a Managed Adversary and Threat Intelligence (MATI) report, which lists out the details of a campaign targeting the financial vertical in the US.

SETUP MATI REPORT ALERT

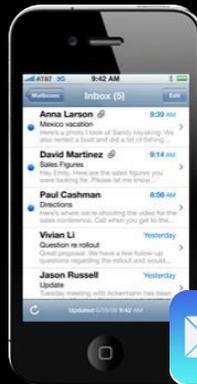
Director of Security sets up a MATI report alert on the DeepSight portal. Such that he is emailed a report as it gets published.



DISCOVERY...
of a campaign by a DeepSight MATI Analyst

GET ALERTERED

Director of Security receives an MATI report alert via email



INFORM SECURITY OPS TEAM

Provides the "Technical Indicators" in the report to the Security Operations team to put in place counter-measures.

USE MATI REPORT FOR:

- Executive Communication
- Strategic Planning and Risk Mitigation
- Showcase to management the threat landscape knowledge



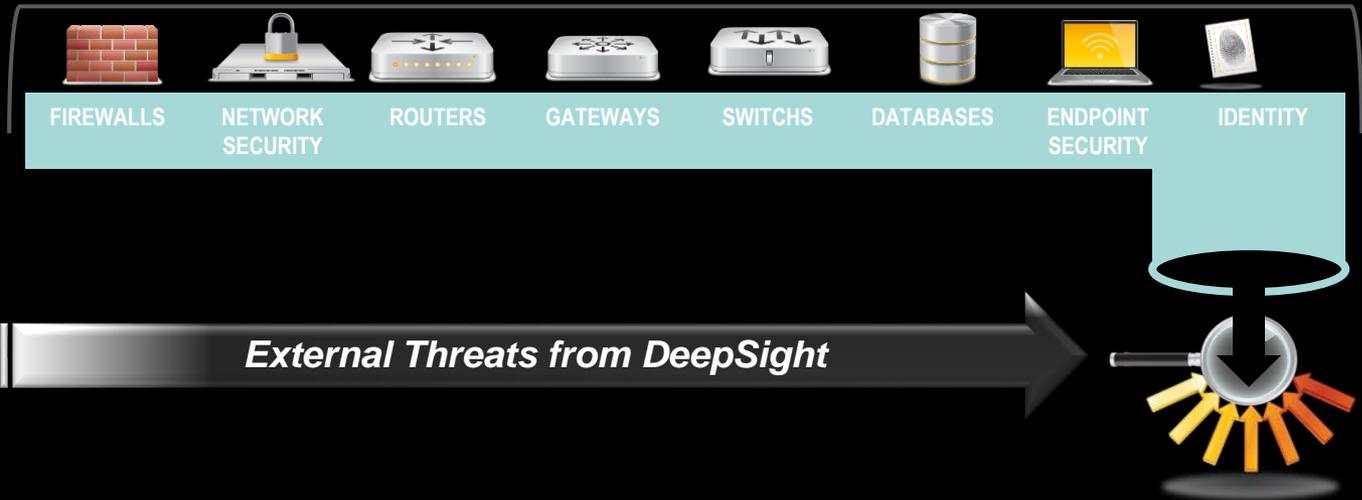
Threat Identification & Intelligence

Intelligence Use Cases

Detection of Unknown External Threats - Datafeeds

Security Operations Center (SOC)

Central location to collect information on threats such as: external, internal, user activity, and loss of sensitive data



EXTERNAL UNKNOWN THREATS

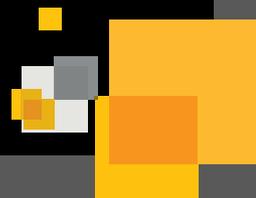
DeepSight Datafeeds provide external threat data, not known to the security infrastructure, to SOC's/SIEM's for detection & prevention.

REPUTATION DATAFEEDS

DeepSight reputation Datafeeds provides an up-to-date list of "Command and Control" servers of botnets known to DeepSight. Allowing for the detection and the prevention of exfiltration of sensitive data.

CONTROL POINTS

SIEM is used to detect and Network control points such as Firewalls and Gateways are used to prevent exfiltration using the DeepSight data



3rd Party Security Services Experienced People



Events, Attacks and Incidents – Defined

45,000

Number of Events
in a typical week

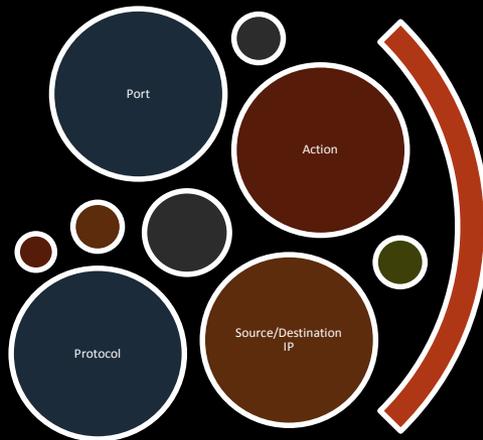
14,000

Number of Attacks
in a typical week

2

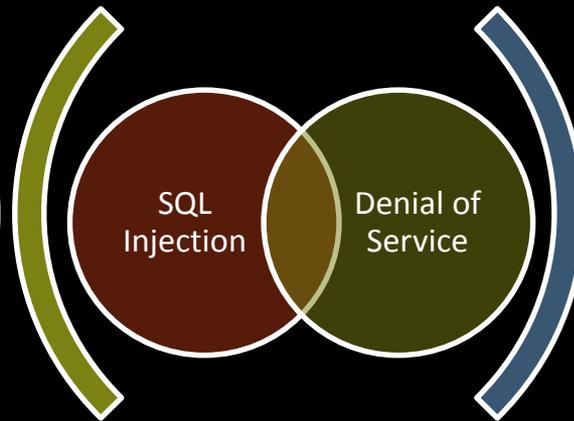
Number of
Incidents in a
typical week

Event



e·vent
ə'vent

Attack



at·tack/ə'tak

Incident



in·ci·dent/'insəd(ə)nt

Events are something happened, either malicious or not. Some for communication passed through a particular technology. e.g. accessed a dB, an peer to peer protocol request was sent

Security events that been identified by correlation and analysis tools as malicious activity attempting to collect distroy information – e.g. SQL Injection, denial of service

Attacks and/or security events that have been reviewed by and expert human analyst and have been deemed necessary for deeper investigation or corrective action. Declaring an incident is a big decision made by several stakeholders.

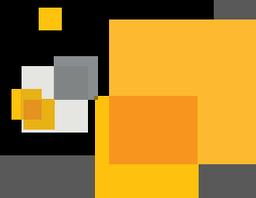
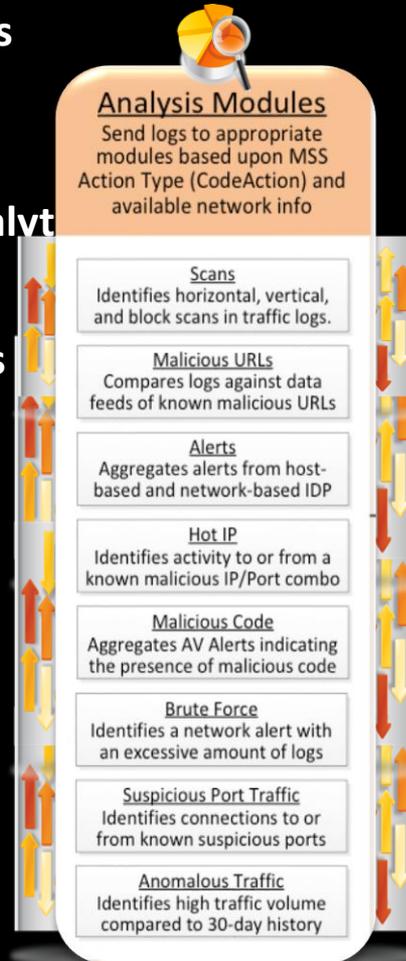


How MSS detects attacks

Detect

Assess

- **Events are collected from customer devices**
 - Logs from firewalls and network devices
 - Alerts from products such as IDS, SEP, DLP, etc
- **MSS stores the logs and sends them to analysts**
 - Default storage period is 90 days
- **MSS analytics engines detect specific kinds**
 - Scans
 - Malicious URLs
 - Alerts
 - Hot IPs
 - Malicious Code
 - Brute Force Attacks
 - Suspicious Ports
 - Anomalous Traffic



Event triage (assessment phase)

Detect

Assess

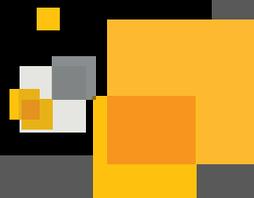
- **Narrow down alerts to identify potential incidents**
- **Research threats using Analysis & Research Console tools**
 - Search knowledgebase & review known threat data
 - Query across multiple customer databases for relevant context
 - Perform DNS lookups and external searches
- **Publish incident (escalate to customer)**
 - In accordance with customer defined escalation rules



What happens during an investigation?



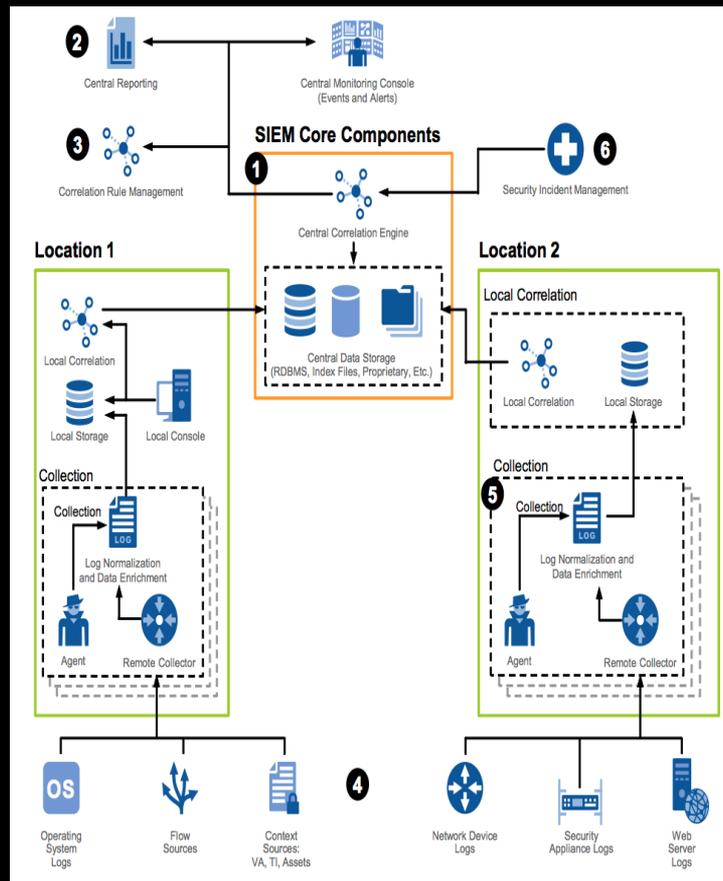
- **Incidents are annotated by the SOC analyst and published to the portal where they can be viewed by the customer**
- **Customer can view incidents on the portal or via the API**
- **For high severity incidents, customers are notified immediately, 24x7**
- **Incidents are handled by the customer's internal CRT, Symantec IR, or a third party**



3rd Party Security Services

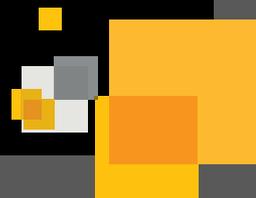
How would a customer detect attacks without MSS?

SIEM Architecture Blueprint



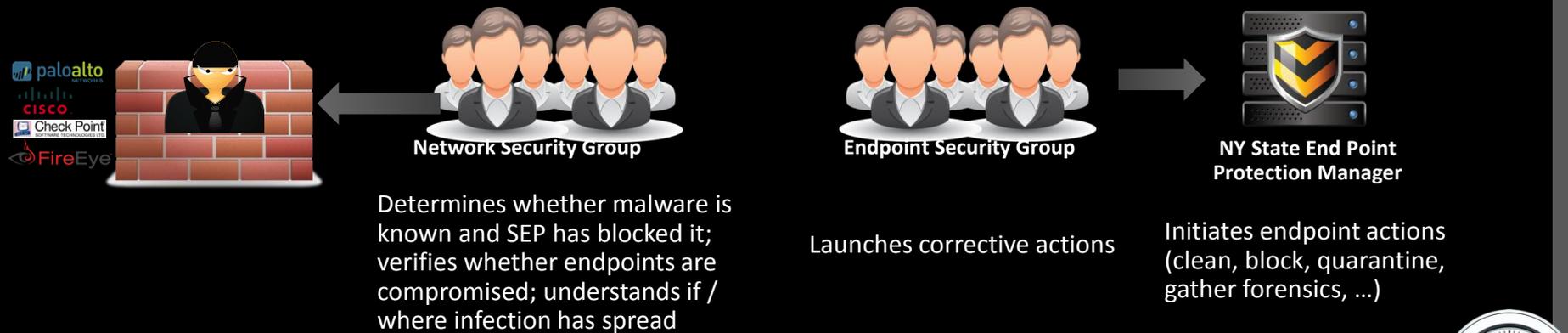
Key Takeaways

- Many organizations start with basic log management functions (log storage & query) and eventually adopt SIEM technology for alerting
- Log management technology remains a necessary component for forensics and security operations, with or without MSS
- Many SIEM deployments result in a system that is difficult to manage on an ongoing basis, leading the organization to consider alternatives such as MSS
- Globally, computing forensic investigation skills are generally limited. Some companies, such as accounting and financial firms, have mature, established and sizable computing and accounting forensic teams that are part of their audit and assurance practices

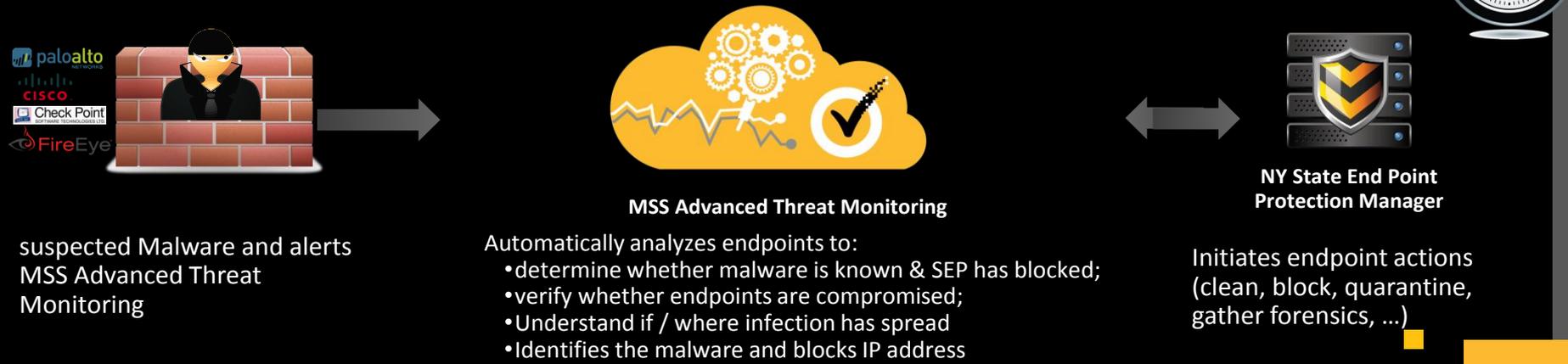


3rd Party Security Services

WITHOUT MSS Manual correlation and remediation



WITH MSS Automated correlation and remediation



Incident Response

Incident Response (IR) Defined



Incident Response is an *organized approach* to addressing and managing the aftermath of a security breach or attack (also known as an **incident**).

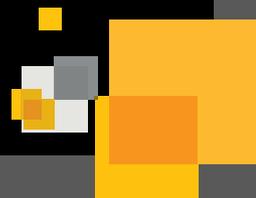
The goal is to handle the situation in a way that limits damage and reduces recovery time and costs.



Incident Response

Who's Involved In The Process

- Incident response (IR) is a multifaceted discipline. It demands capabilities that require resources from several operational units in an organization. One example is shown below.



Incident Response

The IR Process & Desired Outcomes



1 Improve Response Times

2 Lower Response Costs

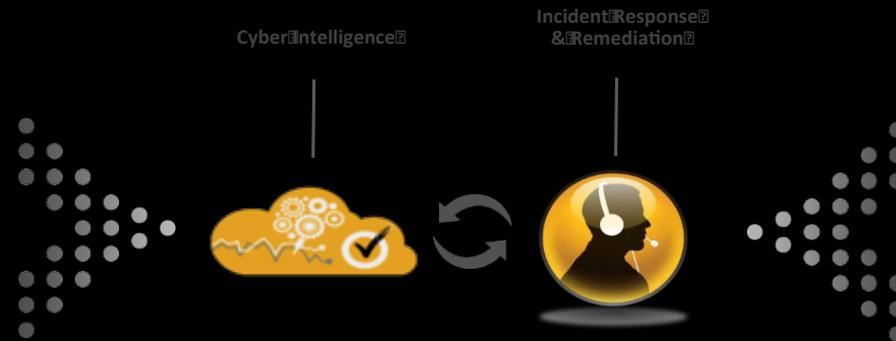
3 Improve Response Effectiveness

4 Enable Continuous Improvement



Incident Response

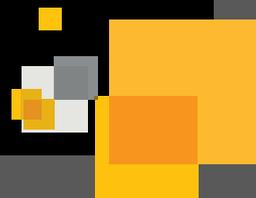
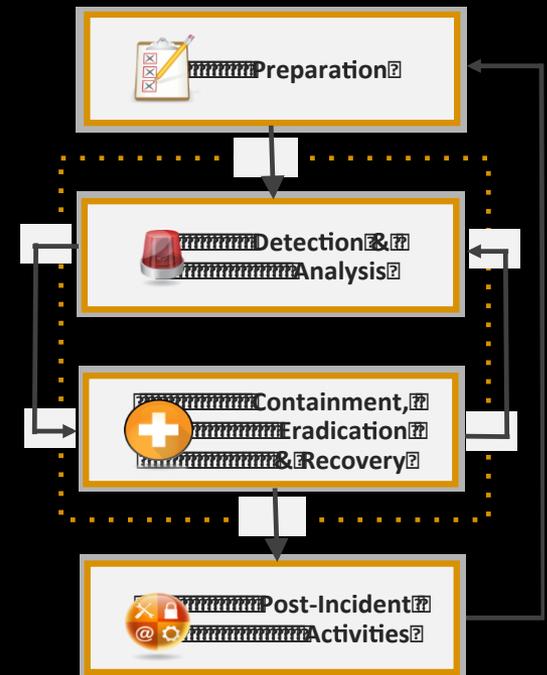
A Real World Example



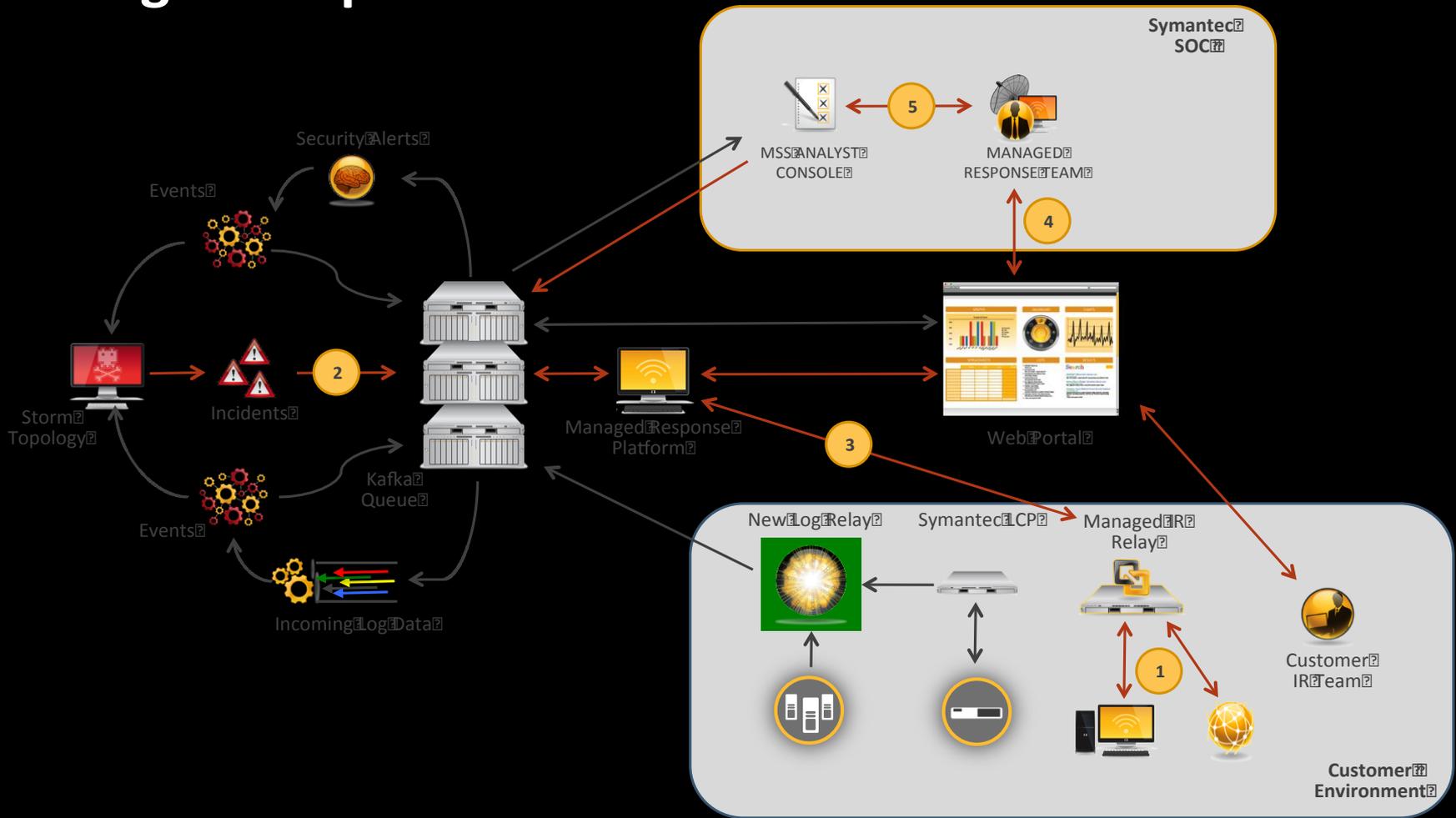
Shift from high-cost and reactive to programmatic and proactive

Prepare, assess, contain, and remediate incidents quickly

Build and refine a robust incident response program



Incident Response Managed Response



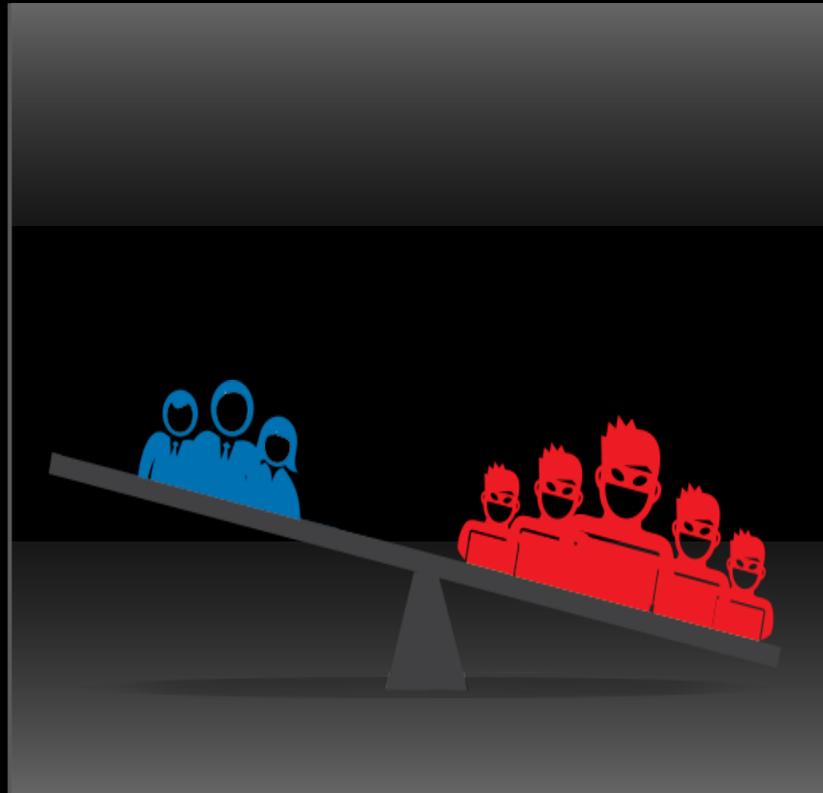
Cyber Team Readiness

Organizations are Fighting an Asymmetric Battle

Cyber security
top IT skills
shortage for 4th
year in a row*

Preparation—
lack of hands-on
experience

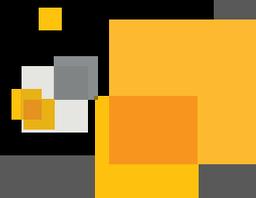
Organizations
uncertain of
cyber-readiness



Seemingly
limitless
resources

Sophisticated,
multi-stage
attacks

Attacker tactics
constantly
morphing



Cyber Team Readiness

Security Simulation Strengthens Cyber Readiness

- Cloud-based, web-enabled virtual training experience
- Live-fire simulation of multi-staged, advanced targeted attack scenarios
- Players assume the identity of their adversaries to learn motives, tactics and tools
- Hands-on experience



Cyber Team Readiness Security Simulation

Security Simulation strengthens cyber-readiness through live-fire simulation of today's most sophisticated advanced targeted attacks



THINK LIKE AN ATTACKER

- Cloud-based, virtual training experience simulates multi-staged attack scenarios allowing players to take on the identify of their adversaries
- Gamification provides a more engaging, immersive educational experience
- Frequent scenarios updates ensure team stays current on latest adversaries, motives and techniques
- Scenarios imparts knowledge gleaned from Symantec security experts and threat analysis and current threat landscape



ASSESS AND DEVELOP YOUR TEAM

- Leaders and participants receive in-depth security skill assessments
- Provides structured recommendations for cybersecurity skill development
- Identify gaps in team coverage and assess skills of new-hire candidates



Conclusion

