servicenow

Integrated Security Operations – The Difference between Knowing and Guessing

John Pescatore, Director of Emerging Security Trends at SANS Institute

Matthew O'Brien, Global Director, Security Detection and Investigation Services at DXC Technology

Piero DePaoli, Senior Director, Security Business Unit at ServiceNow

Integrated Security Operations - The Difference between Knowing and Guessing

John Pescatore, SANS
Matthew O'Brien, DXC
Piero DePaoli, ServiceNow

Obligatory Agenda Slide

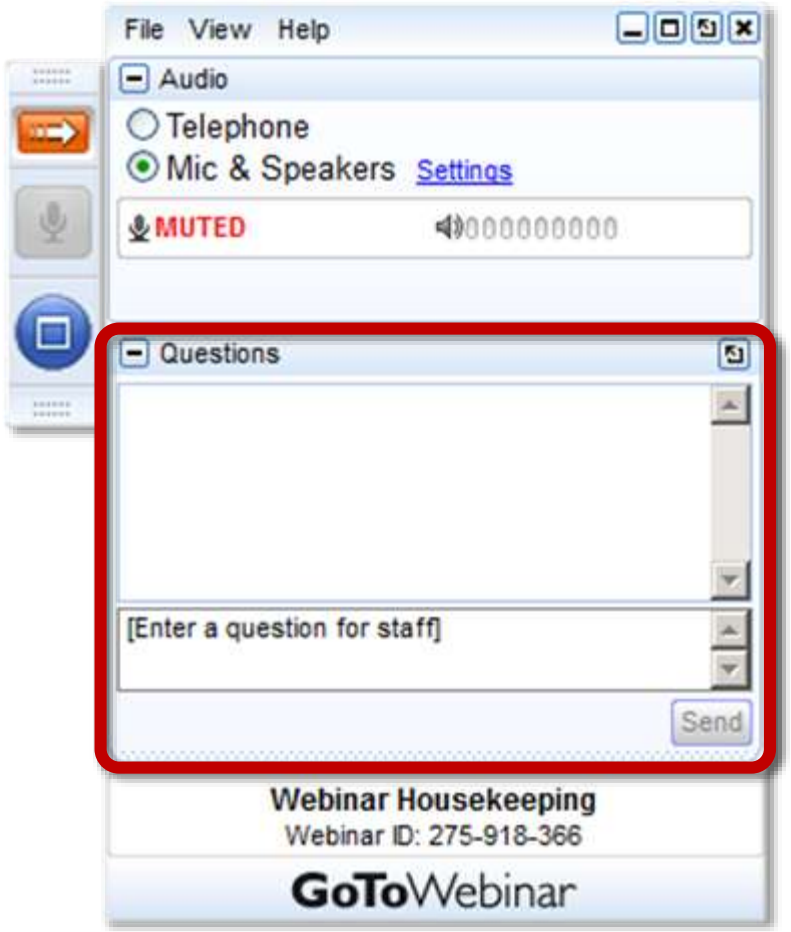
- Housekeeping info
- Here's what we will do
  - **3:35 – 3:50 Overview** – John Pescatore
  - **3:50 – 4:05 DXC SOC Services** – Matthew O'Brien
  - **4:05 – 4:15 Service Now** - Piero DePaoli
  - **4:15 – 4:30 Q&A**

Thanks to our sponsor:

Q & A

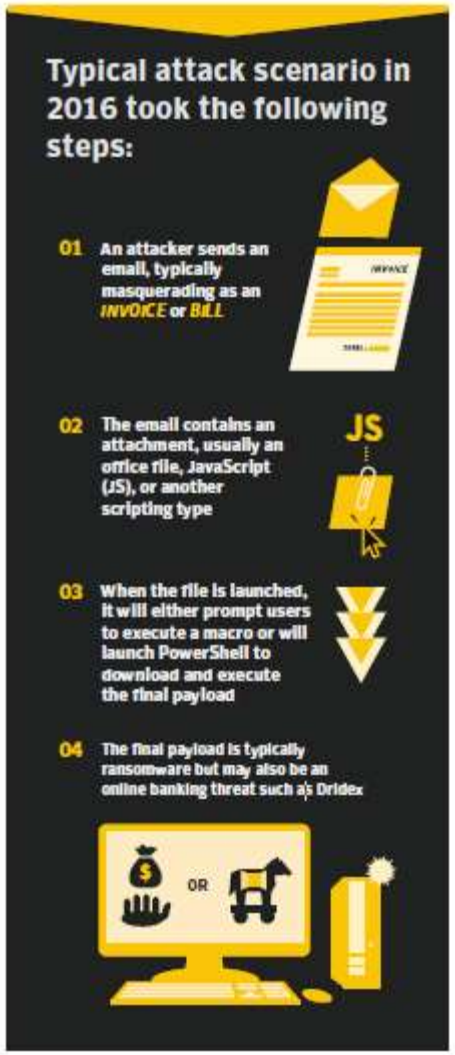
- Please use GoToWebinar's Questions tool to submit questions to our panel.

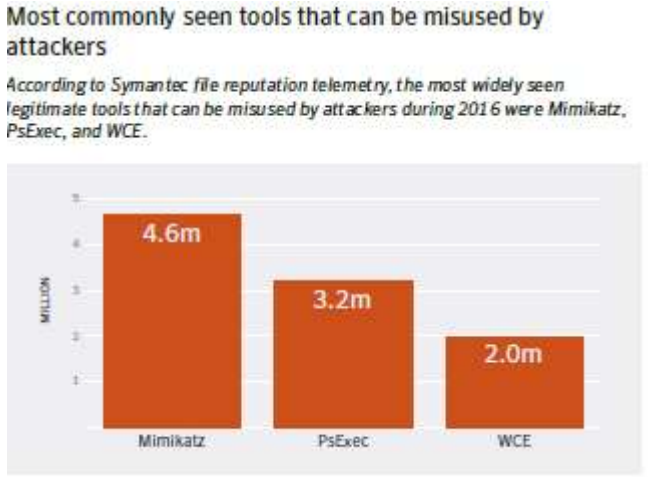
- Send to "Organizers" and tell us if it's for a specific speaker.

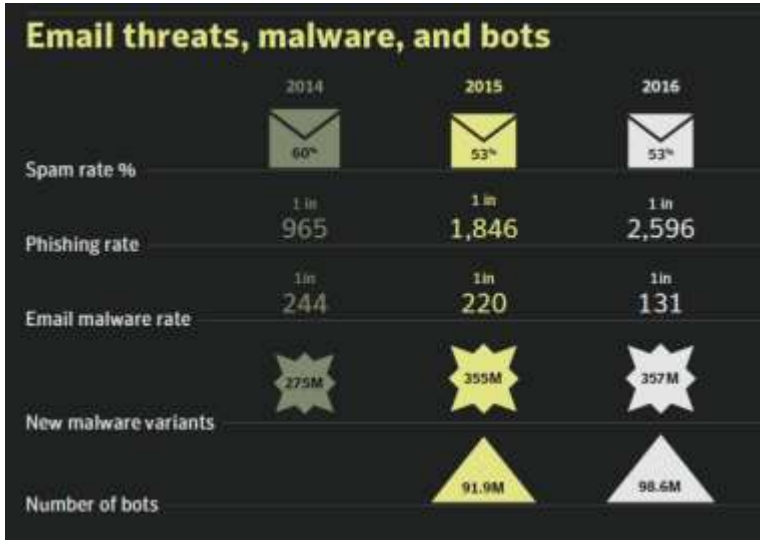


Attack Trends

- Sheer volume leveling out
- Still largely phishing driven
- More exploits and file-less attacks
- Targeting and evasion are increasing in sophistication
- Many trips across the network
- Cybercrime as a service lowers the bar for complex attacks by lesser skilled attackers







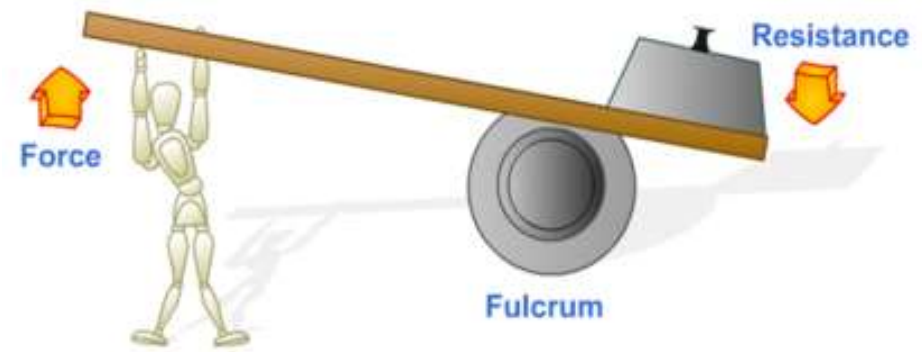
Lessons Learned from WannaCry/NotPetya

- Basic security hygiene still matters:
  - Patching (Critical Security Control 1, 4)
  - Turnoff unneeded services/block at boundary (CSC 9, 12)
  - Network segmentation (CSC 4, 12)
  - Backup (CSC 10)
- Special Issues
  - Use of outdated operating systems – legacy apps, appliances, embedded systems
  - Excrement hits the ventilator differently for ransomware vs. breach or DDoS
- SOCs Matter
  - Similar success patterns across prevent/detect/respond by those who avoided damage
  - Centralized/coordinated SOC operation critical due to early phase confusion

Definition of Security Operations

Security Operations – Protecting the confidentiality, integrity, and availability of business operations through: proactive design and configuration, ongoing monitoring of system state, detection of unintended actions or undesirable state, and **minimizing damage from unwanted events**.

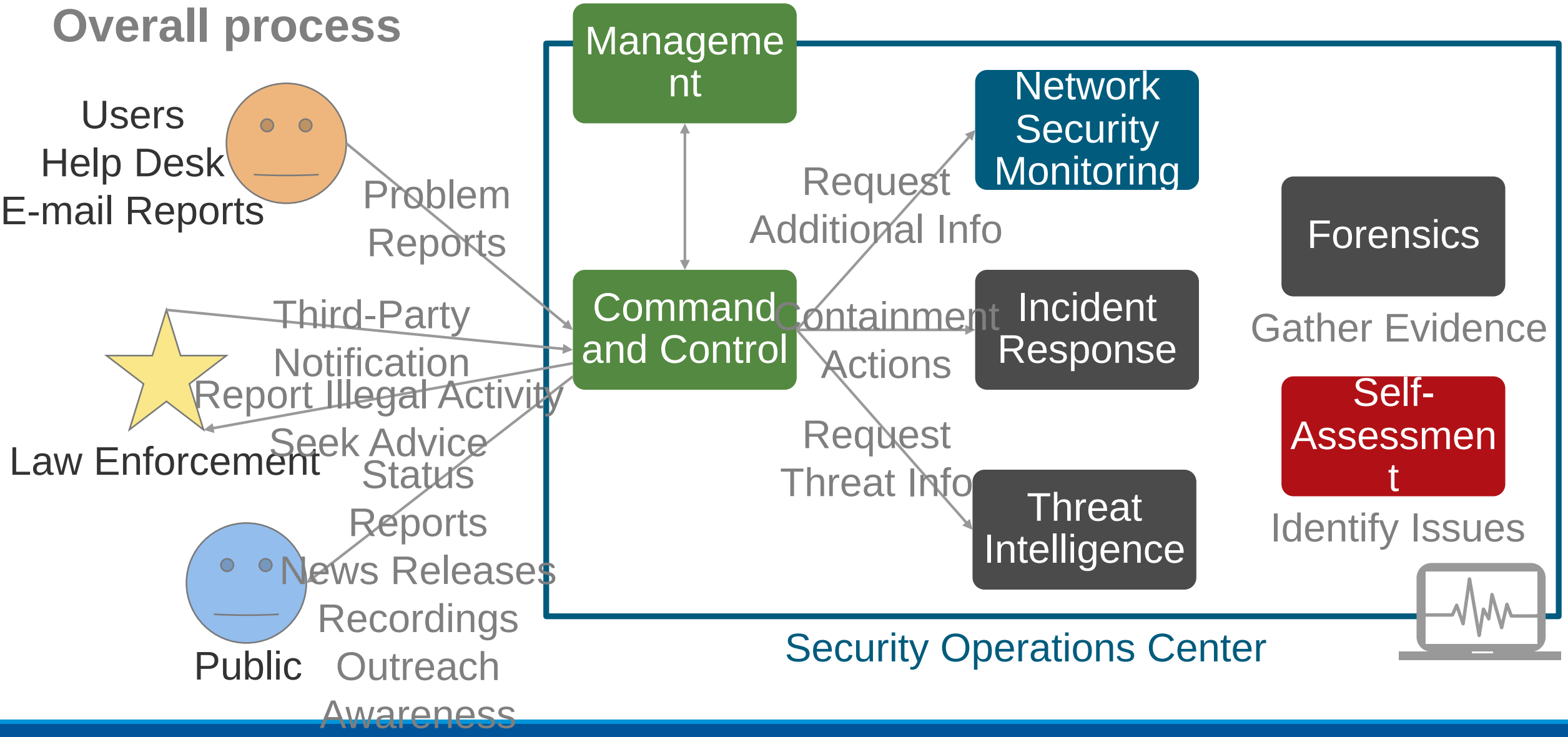
The SOC as a Force Multiplier



- Need to focus limited resources on the highest payback areas.
- Repeatable processes, supporting by intergration/automation
- Situational awareness guiding action vs. information/event management.
- **Action** – prevent more, detect faster, resolve more surgically

SOC / Command Center Process

Overall process



Getting Started

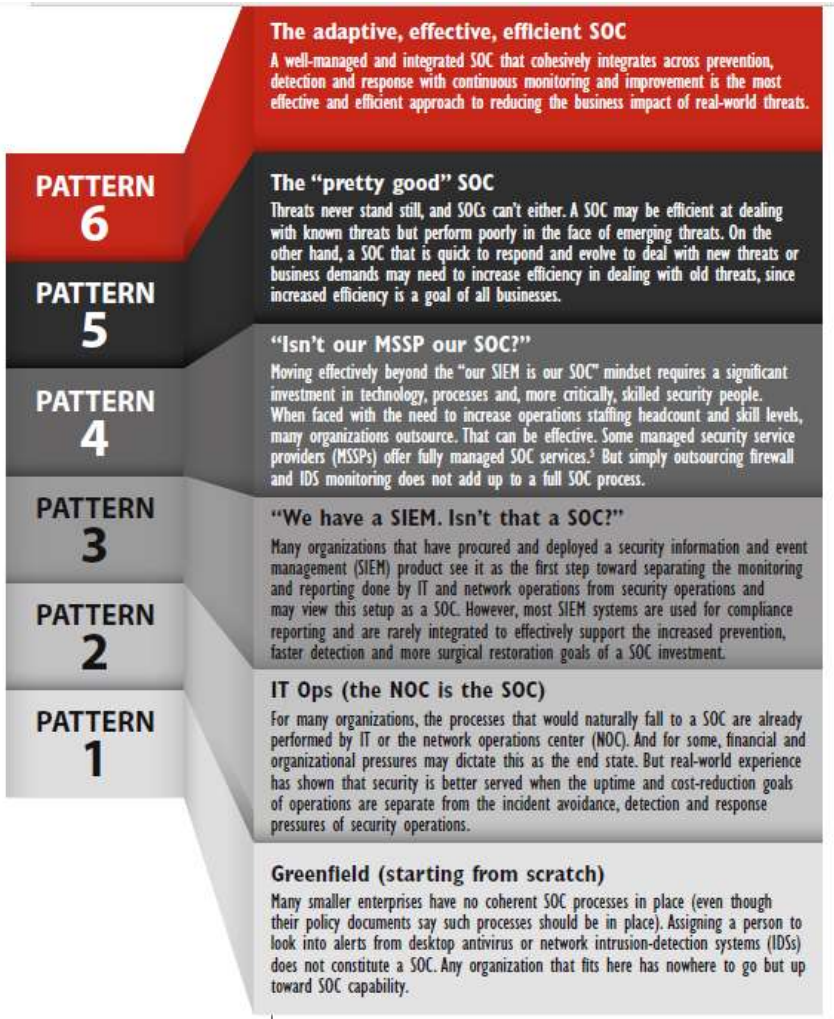
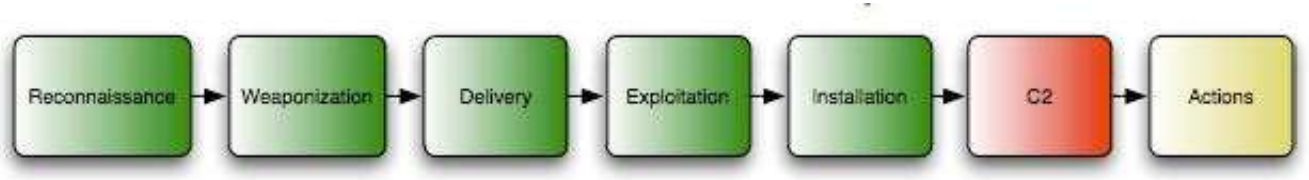


Figure 2. Six Common Patterns of SOC Effectiveness

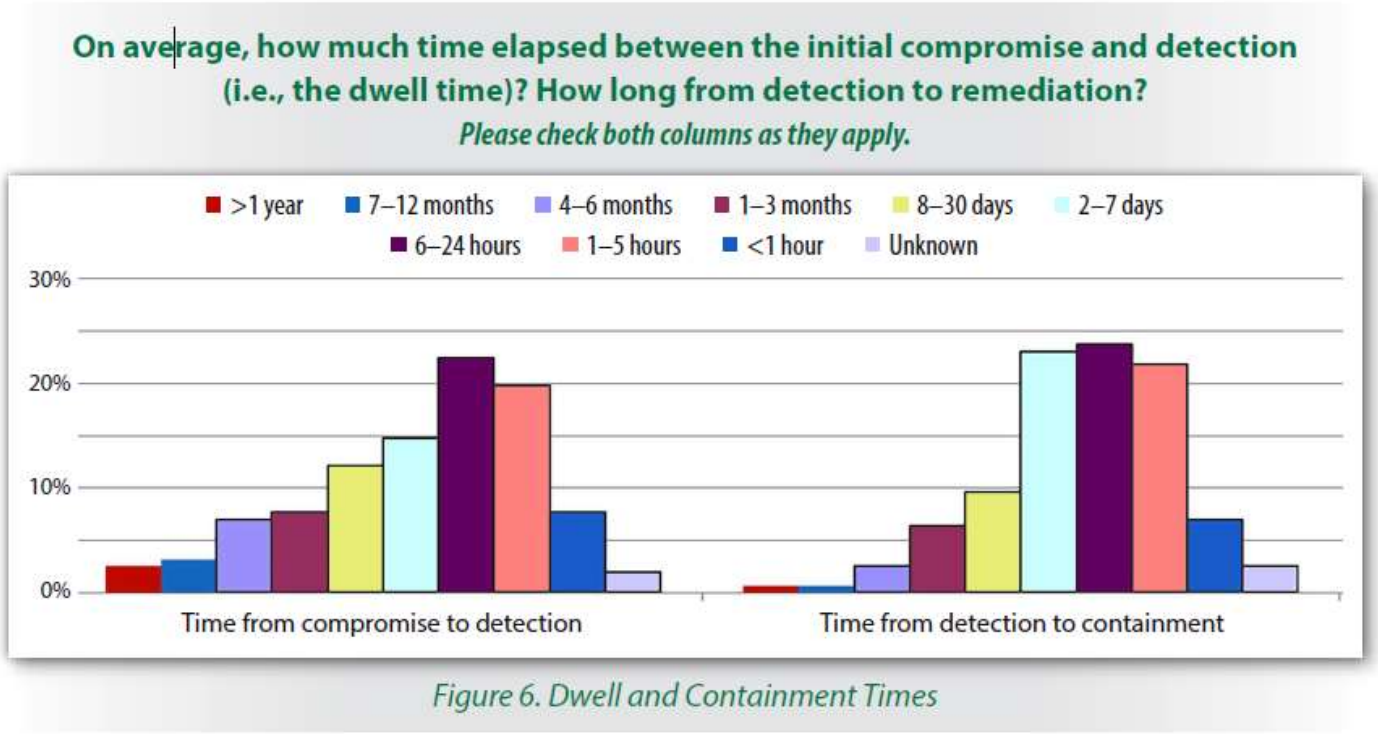
Taking Action Earlier in the Malware Kill Chain



Late Action = Incident Response

Early Action = Damage Prevention

Detect Faster, Contain Sooner



SANS 2017 Incident Response Survey

- Critical metrics: time to detect, time to mitigate
- Goal is to move to the left
  - What causes the most movement?
  - How does business benefit?

Don’t Forget: Mitigate More Surgically

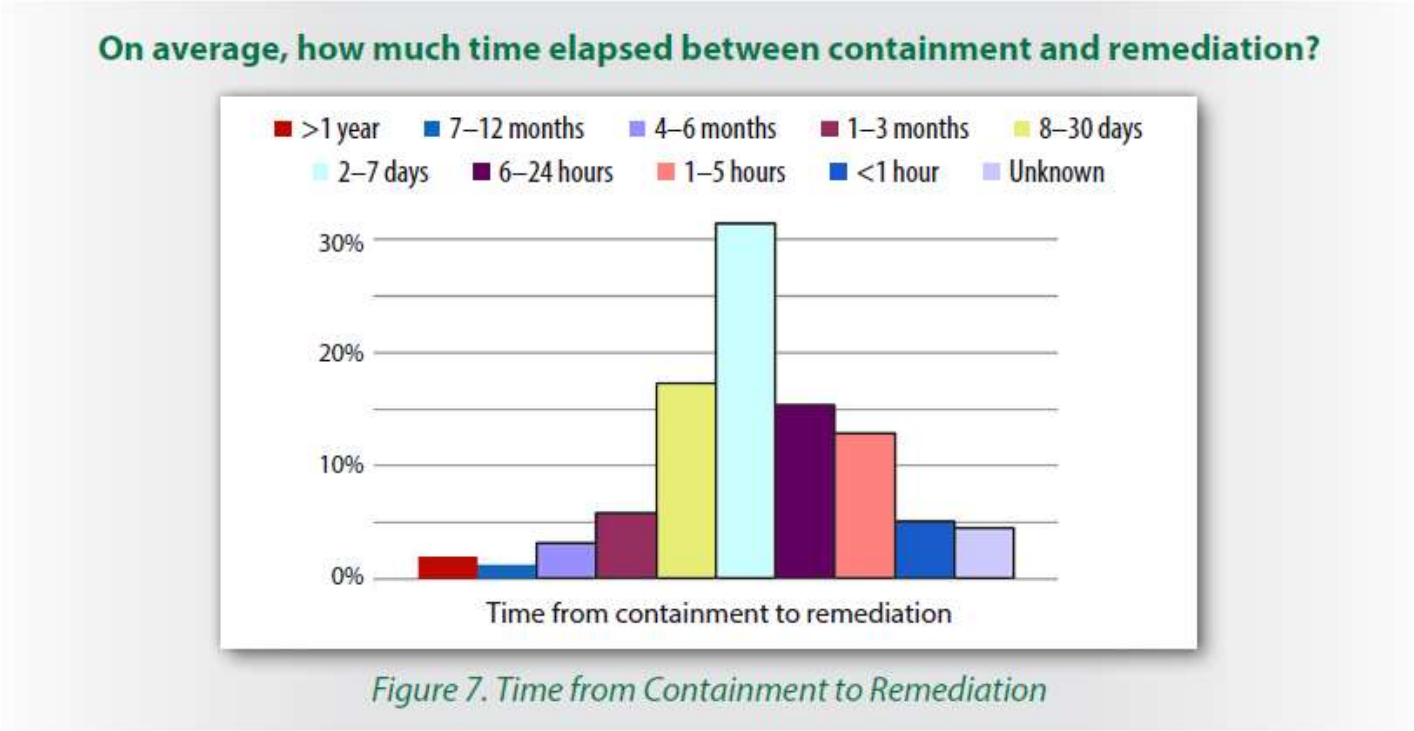


Figure 7. Time from Containment to Remediation

SANS 2017 Incident Response Survey

- Business impact doesn’t end until remediation/restoration
- Playbooks/SOC analyst guidance can directly reduce time and remediation miscues

Overcoming Obstacles

Table 4. Top 10 Impediments Facing IR Teams

Rank	Impediment	% Response
1	Lack of resources (time, staff, budget) to effectively execute improvements	48.7%
2	Staffing and skills shortage	47.1%
3	Vaguely defined processes and owners	32.1%
4	Budgetary shortages for tools and technology	31.0%
5	Not enough visibility into events happening across different systems or domains	30.5%
6	Organizational silos between IR and other groups or between data sources or tasks	26.7%
7	Lack of procedural reviews and practice	23.0%
8	Too much time needed to detect and remediate	19.8%
9T	Difficulties in detecting sophisticated attackers and removing their traces	18.2%
9T	Integration issues with our other security and monitoring tools	18.2%
9T	Lack of ability and resources to support deployment of multiple security systems	18.2%
9T	Lack of comprehensive automated tools available to investigate new technologies, such as BYOD, Internet of Things and use of cloud-based IT	18.2%
10	Lack of controls over devices that leave the network perimeter	17.6%

SANS 2017 Incident Response Survey

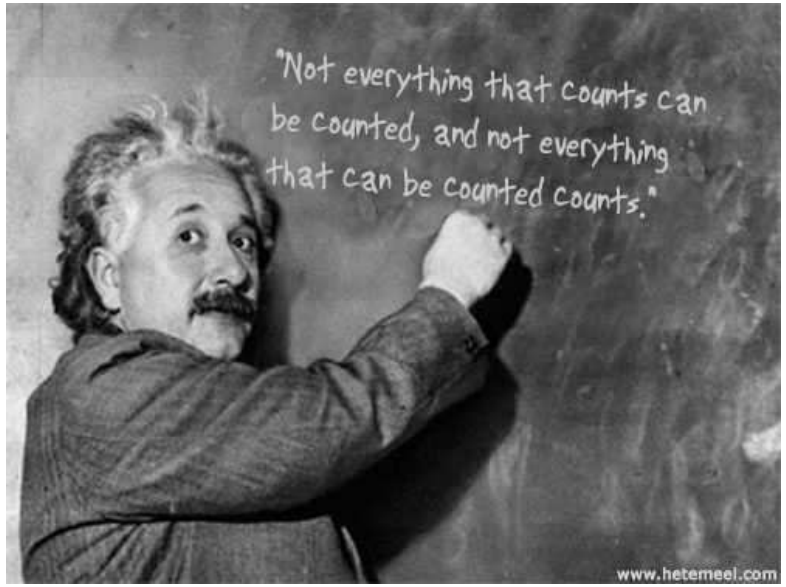
What Is Success for a SOC?

Statement of Success

SOC is successful when it intervenes in adversary efforts to impact the availability, confidentiality, and integrity of *organization's* information assets. It does this by proactively making systems more resilient to impact and reactively detecting, containing, and eliminating adversary capability.

Measurable Benefits of an efficient/effective SOC

- Good old Return on Investment (ROI):
  - Reduce costs through lower business impact
  - Help desk metrics are your friend
- Connection to Business Metrics
  - Increase speed of response to business demands
  - Uptime
- Regulatory/compliance
  - SOC processes check off many compliance boxes
  - Audit results



servicenow

ServiceNow Security Operations

Piero DePaoli
Senior Director, Product Marketing, Security Business Unit

November 14, 2017

Organizations Have Invested in A LOT of Security Products

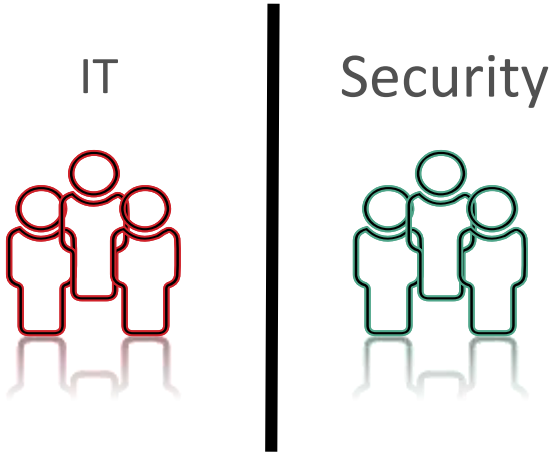
servicenow

Security Teams are Overwhelmed

Too Many Alerts & No Context

Manual Tools

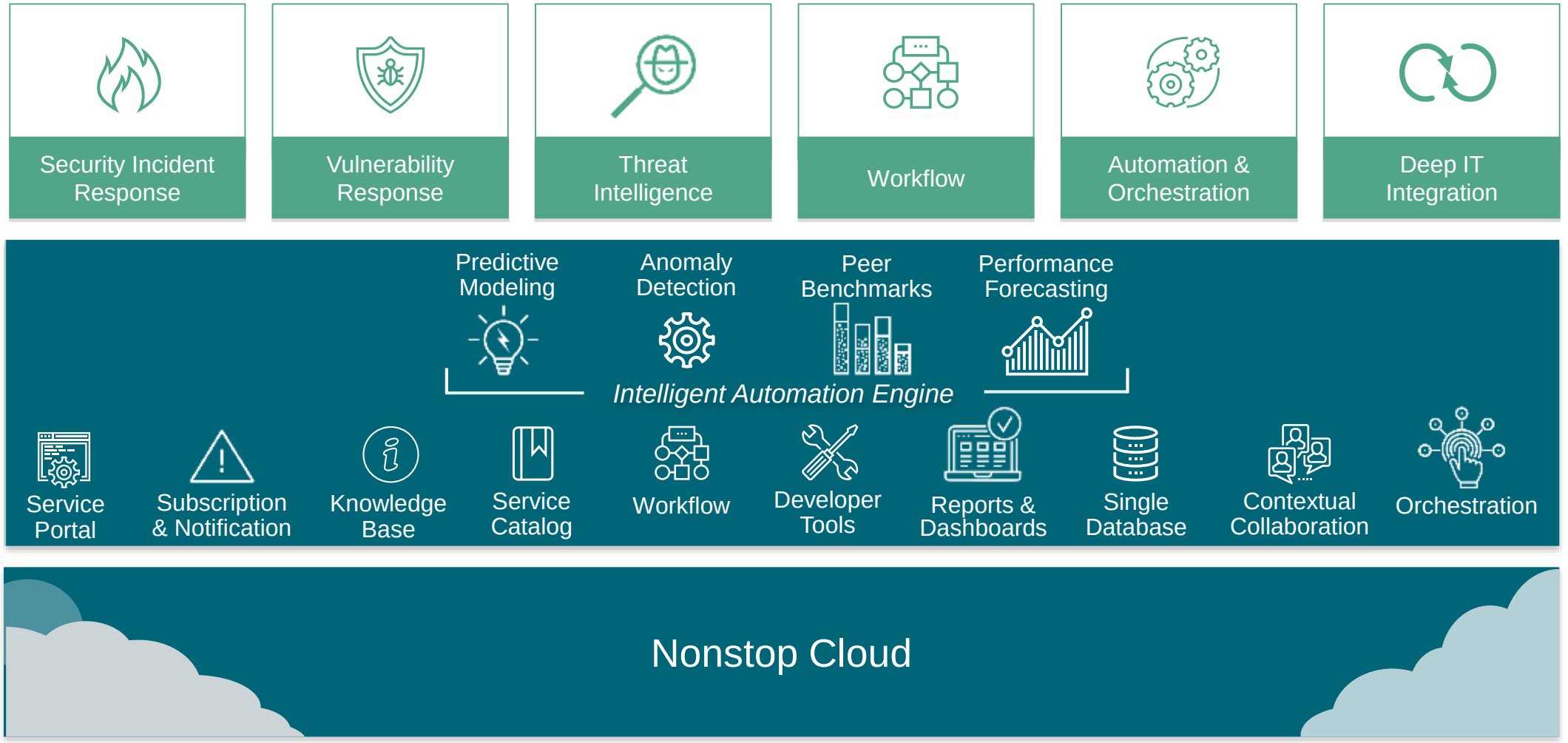
Sometimes Siloed from IT



The Need: Enterprise Security Response

servicenow®
securityoperations

ServiceNow Security Operations



November 21, 2017

Integrated Security Operations

Manage Security Threats Fast & Increase Enterprise Security Visibility

DXC.technology

What is Integrated Security Operations (ISecOps)?

Intelligence driven, automated security incident and vulnerability management service

Integrated Security Operations and Incident Response

Incident and Vulnerability Management Platform

Industry Trends – Digital needs a new way of protection

Pervasive Mobility

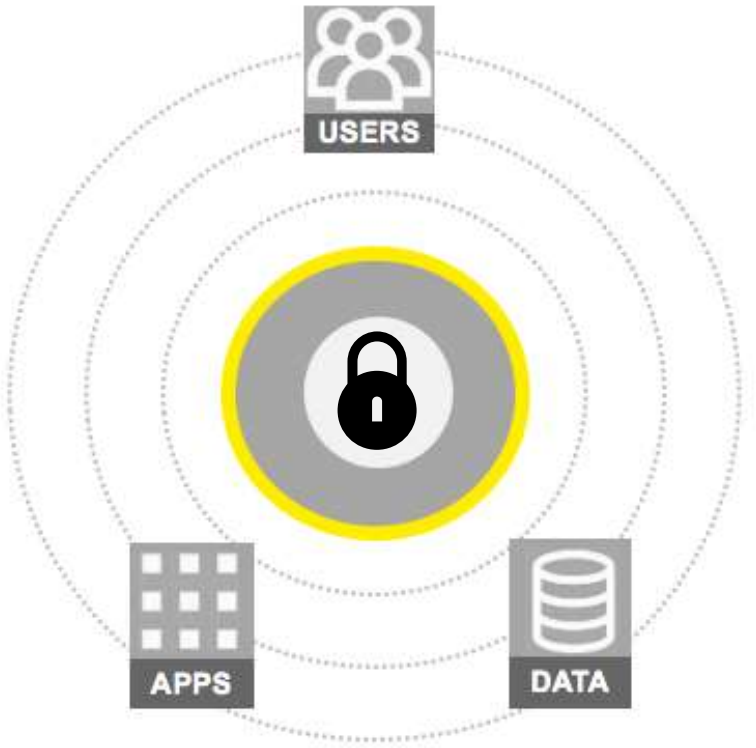
Less enforcement and control over enterprise data access from a myriad of uncontrolled devices sharing applications and systems. Increased complexity, risk and non-compliance.

Privacy **Protection** **Management**

Digital Workflow

Inability to detect advanced threats and incidents, minimizing detection time and remediation across a growing number of attack surfaces.

Detect **Respond** **Remediate**



Hybrid Infrastructure

Loss of visibility control and data through insecure Shadow IT, API and interfaces. Inadequate governance, risk, compliance and control of ongoing use of cloud applications and infrastructure.

Visibility **Policy** **Controls**

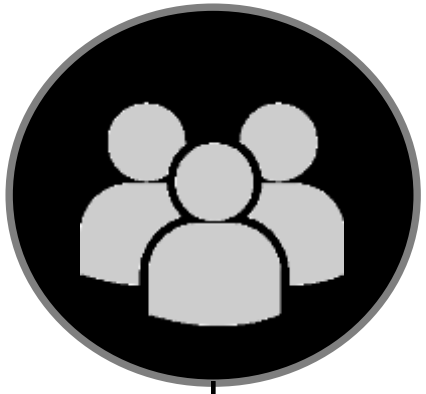
Big Data Analytics

Rapid growth and exchange of data with lack of classification and protection at scale leading to loss. Insufficient governance and enforcement leading to non compliance and fines.

Access **Audit** **Authorize**

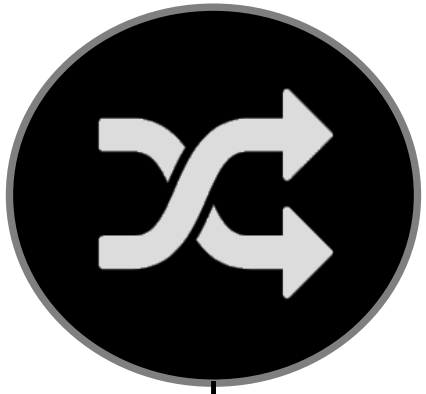
We have Invested Heavily in Protecting our Enterprise

People



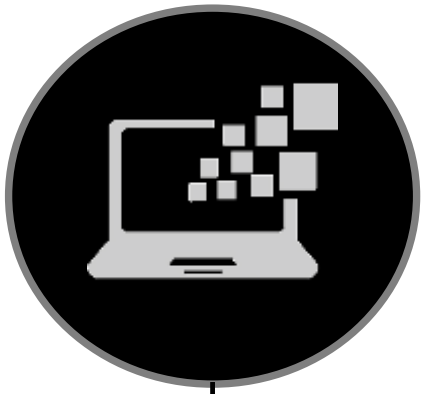
- Security Operations
- Engineering
- Security Incident Response

Process



- Managing Events
- Managing Vulnerabilities
- Managing Security Incidents
- Managing Assets

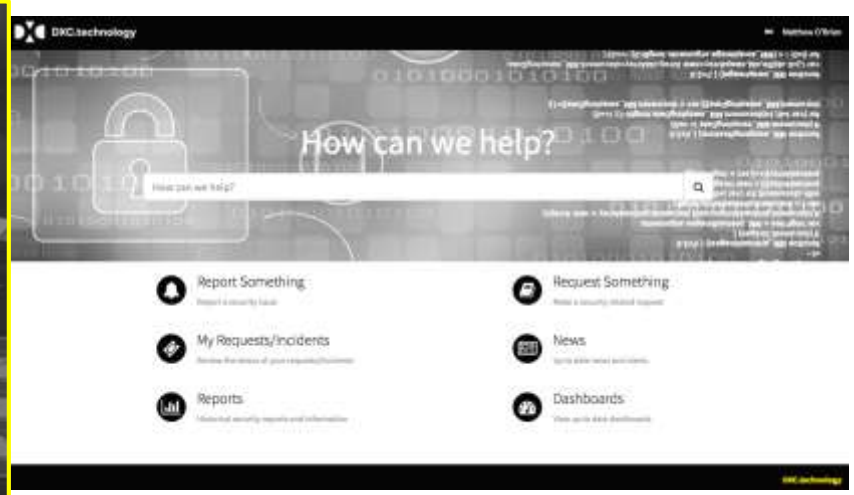
Technology



- Protection Technologies
- Detection Technologies
- Visibility Technologies

Strengthen Threat Detection with Security Monitoring & Response

- Near real-time search and integrated investigation platform for critical alerts and incidents
- Managed Security Services portal provides centralized security, threat, and operational monitoring
- Customer Portal for service and and incident request management



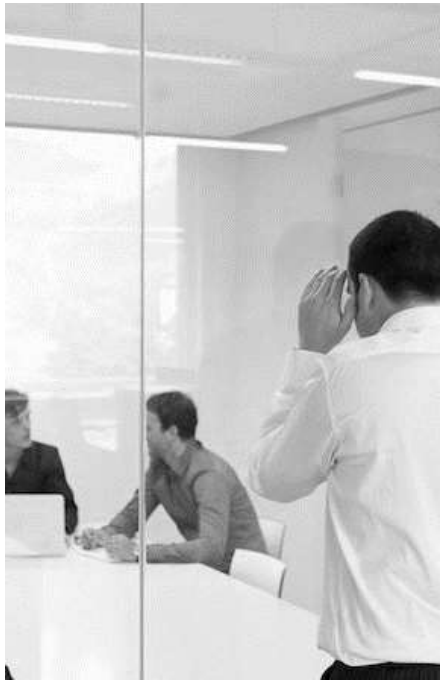
Our Problems

Too Many Alerts & No Context

Manual Processes and Tools

Information Silos: Security vs. IT

Limited Enterprise Visibility

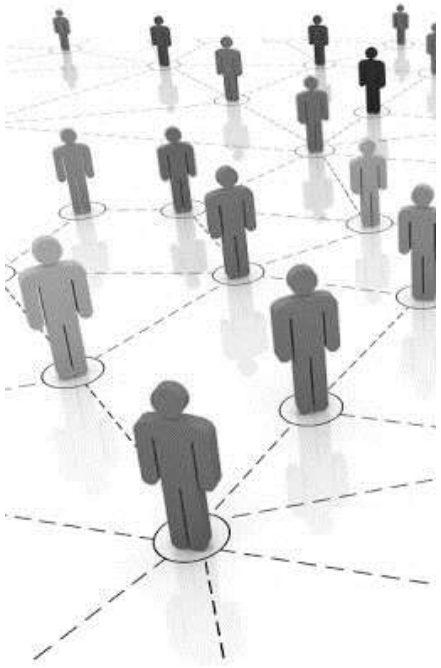


Increasing Compliance Requirements

Our Goals

- Integrate teams across the organization

- Enterprise visibility of security posture



- Reduce time to manage incidents & vulnerabilities

- A solution that scales with the enterprise

- The ability to leverage existing technology investments

Our Solution

Enabled enhanced vulnerability management, operational Interlock, improved visibility and reduced time to manage and respond to security threats.

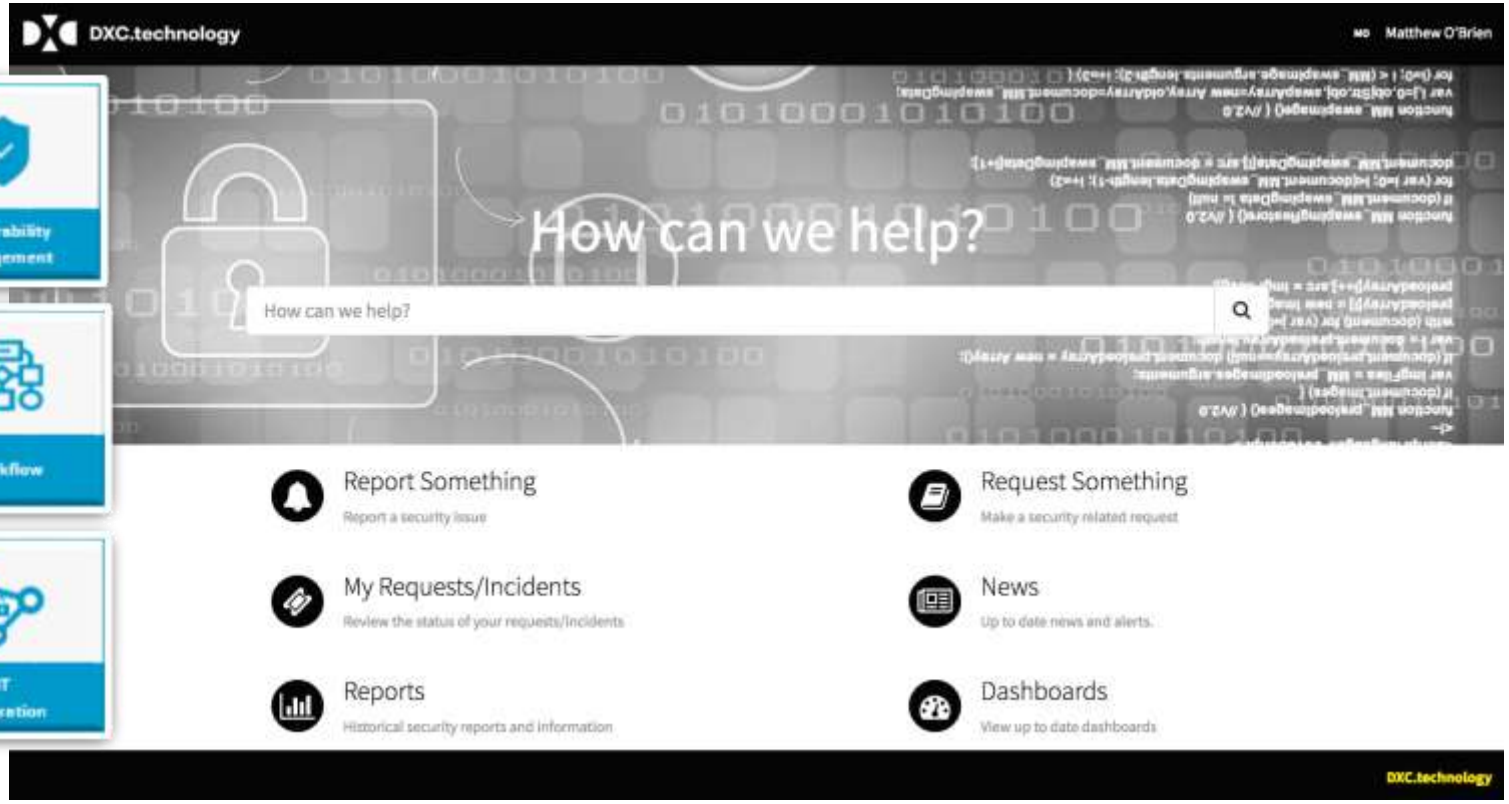
Benefits

Enhanced Incident and Vulnerability Management

Operational Interlock

Improved Visibility

Reduced Time to Manage & Respond to Security Threats



Our Solution

Vulnerability Scanning

Qualys

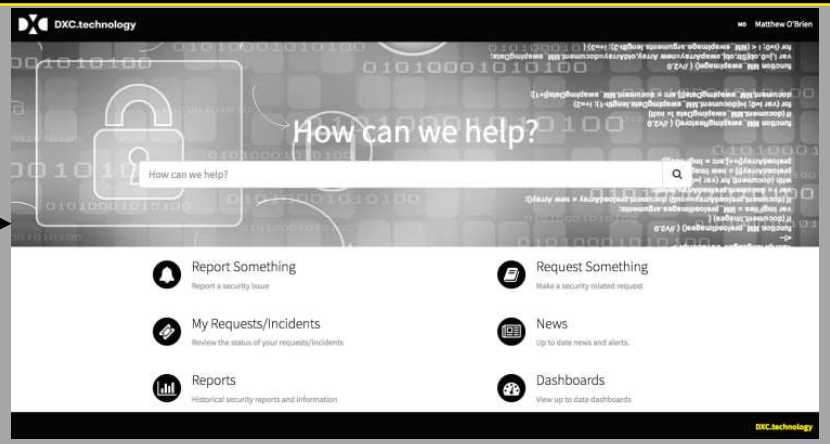
Event Monitoring

SIEM
CrowdStrike Falcon
Firewalls
IDS/IPS
Endpoint Protection

Threat Libraries

Virus Total
CrowdStrike*

DXC.technology



Service Catalogue
Executive Dashboard
Incident Notification
Reporting

Vulnerability Management

Security Incident Response

Threat Intelligence

ISecOps Analysts

Business Assets
CMDB
Service Models

Runbooks
Security Processes
Workflow

Value Outcome

Before	After	Outcome
Multiple Tools Multiple Processes	Integrated solution, clearly defined and automated workflow. Clear task assignment and responsibilities	Improved Incident & Vulnerability Management Workflow
Manual processes No automation	Integrated tools, workflow automation and auto assignment. Faster response time to security threats	Increased Automation
Disparate sources of data No single view	Centralized reporting across the enterprise. Visibility at the business unit and regional levels, aggregating to a global view	Improved Visibility
Teams focused on multiple items with uncertain priorities. Time spent on medial tasks	Teams focuses on business outcome and priorities. Time is spent on more interesting security related activities	Increased Employee Satisfaction
Disparate systems of information. Multiple controls and intelligence Sources	Integrated threat intelligence, vulnerability data, and security incident data in the one location	Improved Integration of information

An increase of up to
50%
Process driven response

Shift from Manual to process driven response

Security Event Triage Time

5X
FASTER

In attributing indicators of compromise to security incidents

Lessons Learned

1. **Don’t underestimate the support required by your security teams for controls integration and process mapping**

2. **Spend time on the user interface, the portal and the reporting and analytics. This is the face of your solution and where you’ll be judged**

3. **Review your existing processes before trying to map them into the platform. Mapping a bad, ineffective process just makes the bad process execute more quickly**

4. **Engage early and often with the operations teams, such as your SOC, Threat Intelligence and Forensics teams. Ensure everyone has the required time committed**

5. **Talk often to your key stakeholders throughout the development and integration processes. Show them what’s happing and leave no surprised for your go live date**


Q&A
You have
Questions
We have
Answers

Resources

- SANS : https://www.sans.org/webcasts/archive/2017
- What Works: https://www.sans.org/critical-security-controls
- SANS Cyber Defense Initiative – https://www.sans.org/event/https://www.sans.org/event/cyber-defense-initiative-2017
- ServiceNow: https://www.ServiceNow.com/
- Questions: q@sans.org
- @John_Pescatore

Acknowledgements

Thanks to our sponsor:

And also to our speaker and to our attendees:

Thank you for joining us today