Best Practices and Tools for Reducing Insider Threats

March 12, 2019

Agenda

- SolarWinds Overview
- Leading Sources of Security Threats
- Insider Threat Flow Response Process
- SolarWinds® Security and Network Tools Can Help
- Building Security Into Your IT Security Posture
- Compliance Resources
- Q&A

Presented by:

Alexander Ortiz

Sales Engineer

SolarWinds

alexander.ortiz@solarwinds.com

SolarWinds at a Glance

Founded in 1999

More than 2,500 employees globally

Austin, TX headquarters
30+ offices globally

#1 in Network Management[2]

#4 in Systems Management[3]

55+ IT management products

Growing Security Portfolio

Leader in Remote Monitoring and Management

150,000+ registered members of THWACK®, our global IT community

300,000+ customers in 190 countries [1]

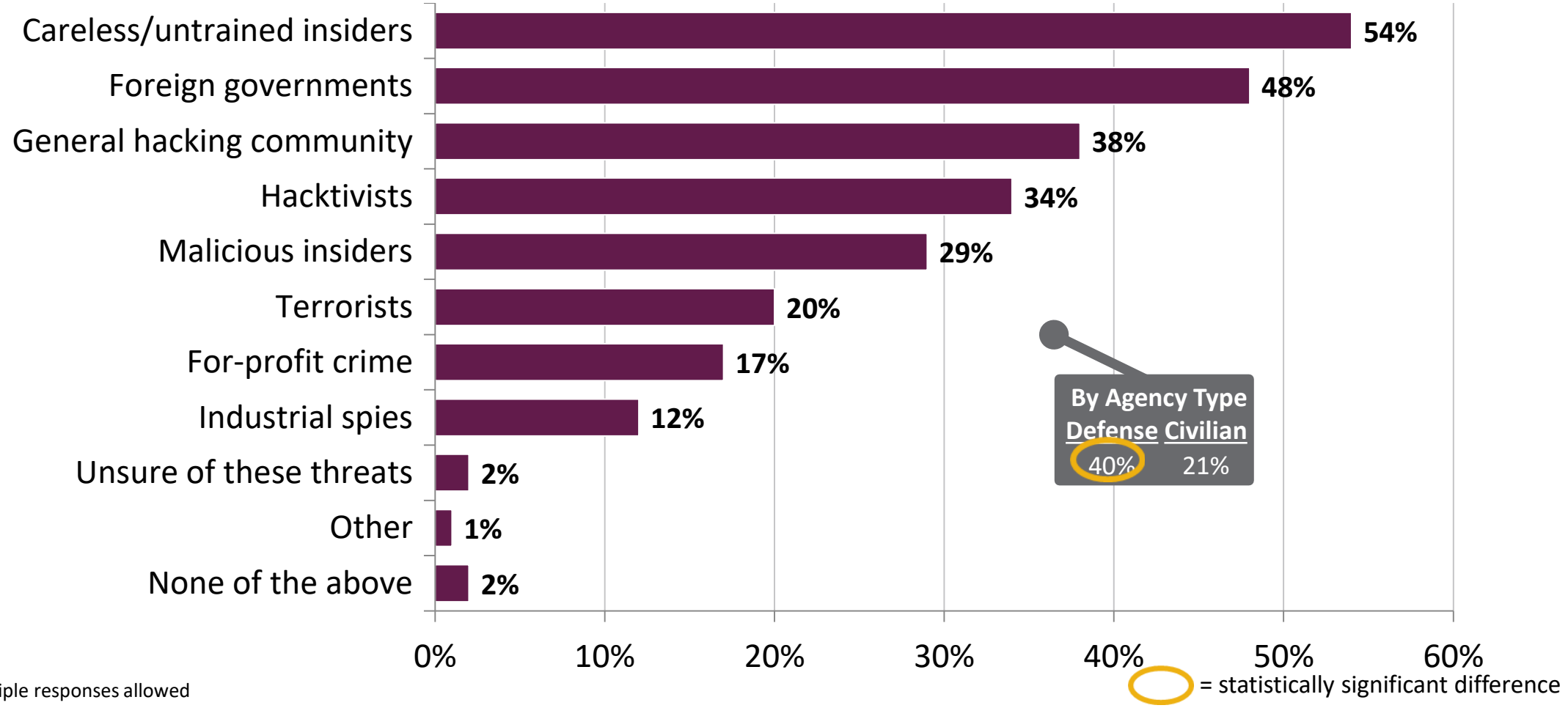
499 of Fortune 500®

22,000+ MSPs serving 450,000+ organizations

Every branch of the DoD, and nearly every civilian and intelligence agency

1. Customers are defined as individuals or entities that have an active subscription for our subscription products or that have purchased one or more of our perpetual license products since our inception under a unique customer identification number. We may have multiple purchasers of our products within a single organization, each of which may be assigned a unique customer identification number and deemed a separate customer.
2. IDC defined Network Management Software functional market, IDC's Worldwide Semiannual Software Tracker, April 2018.
3. Source: Gartner, Market Share Analysis: ITOM: Performance Analysis Software, Worldwide, 2017. July 9, 2018. (AIOps/ITIM/Other Monitoring Tools Software Market). SolarWinds term, Systems Management, refers to the AIOps/ITIM/Other Monitoring Tools Software Market Taxonomy referenced in the Gartner report. All statements in this report attributable to Gartner represent SolarWinds interpretation of data, research opinion or viewpoints published as part of a syndicated subscription service by Gartner, Inc., and have not been reviewed by Gartner. Each Gartner publication speaks as of its original publication date (and not as of the date of this [presentation]). The opinions expressed in Gartner publications are not representations of fact and are subject to change without notice.

Sources of Security Threats



N=200
Note: Multiple responses allowed

What are the greatest sources of IT security threats to your agency? (select all that apply)

Sources of Security Threats - Trend

	2014	2015	2016	2017
Careless/untrained insiders	42%	53%	48%	54%
Foreign governments	34%	38%	48%	48%
General hacking community	47%	46%	46%	38%
Hacktivists	26%	30%	38%	34%
Malicious insiders	17%	23%	22%	29%
Terrorists	21%	18%	24%	20%
For-profit crime	11%	14%	18%	17%
Industrial spies	6%	10%	16%	12%

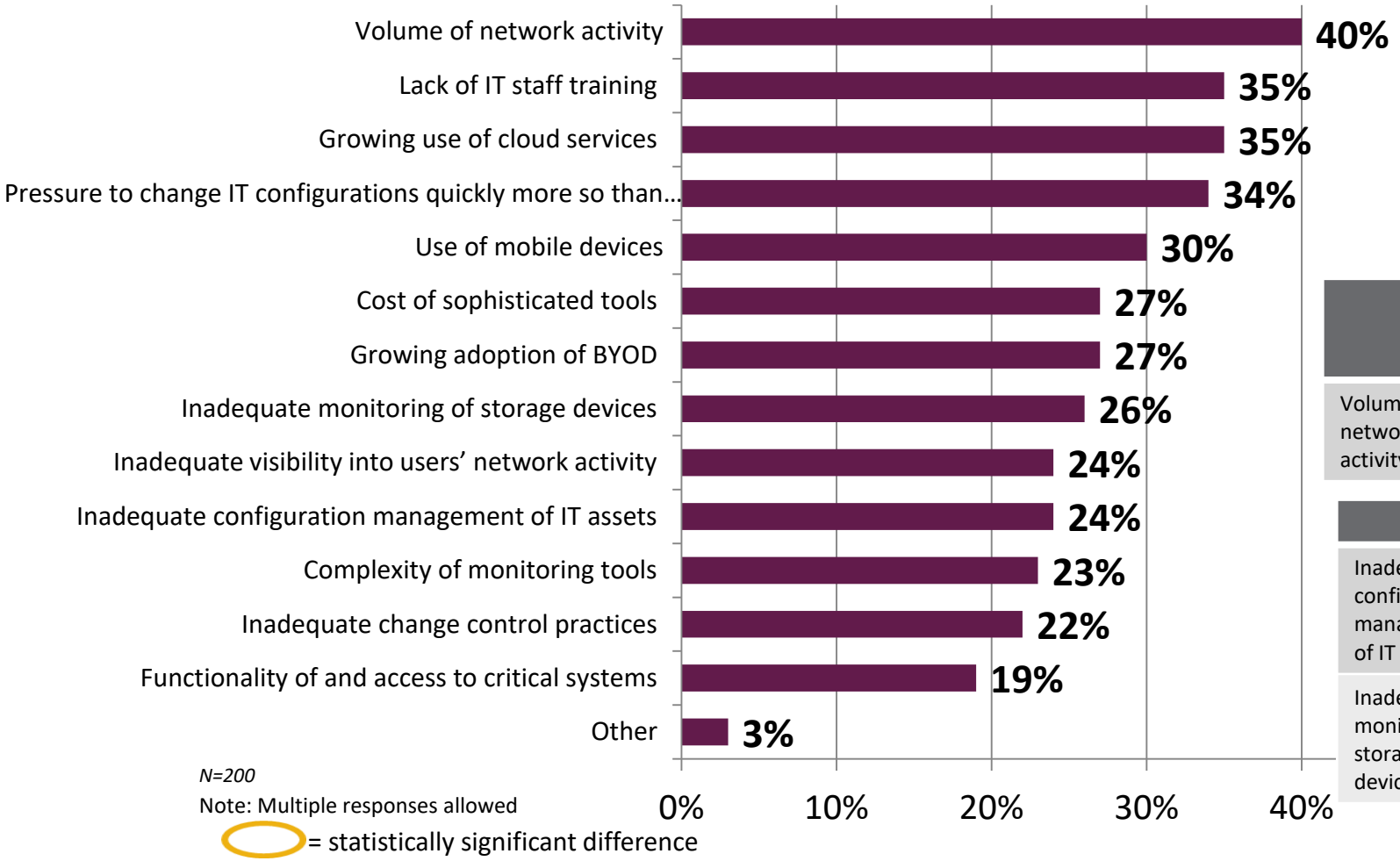
N=200
Note: Multiple responses allowed

= top 3 sources

= statistically significant difference

What are the greatest sources of IT security threats to your agency? (select all that apply)

Insider Threat Detection Difficulties



	IT/ Security Staff	IT/Security Manager/ Director
Volume of network activity	29%	44%

	Defense	Civilian
Inadequate configuration management of IT assets	17%	28%
Inadequate monitoring of storage devices	18%	32%

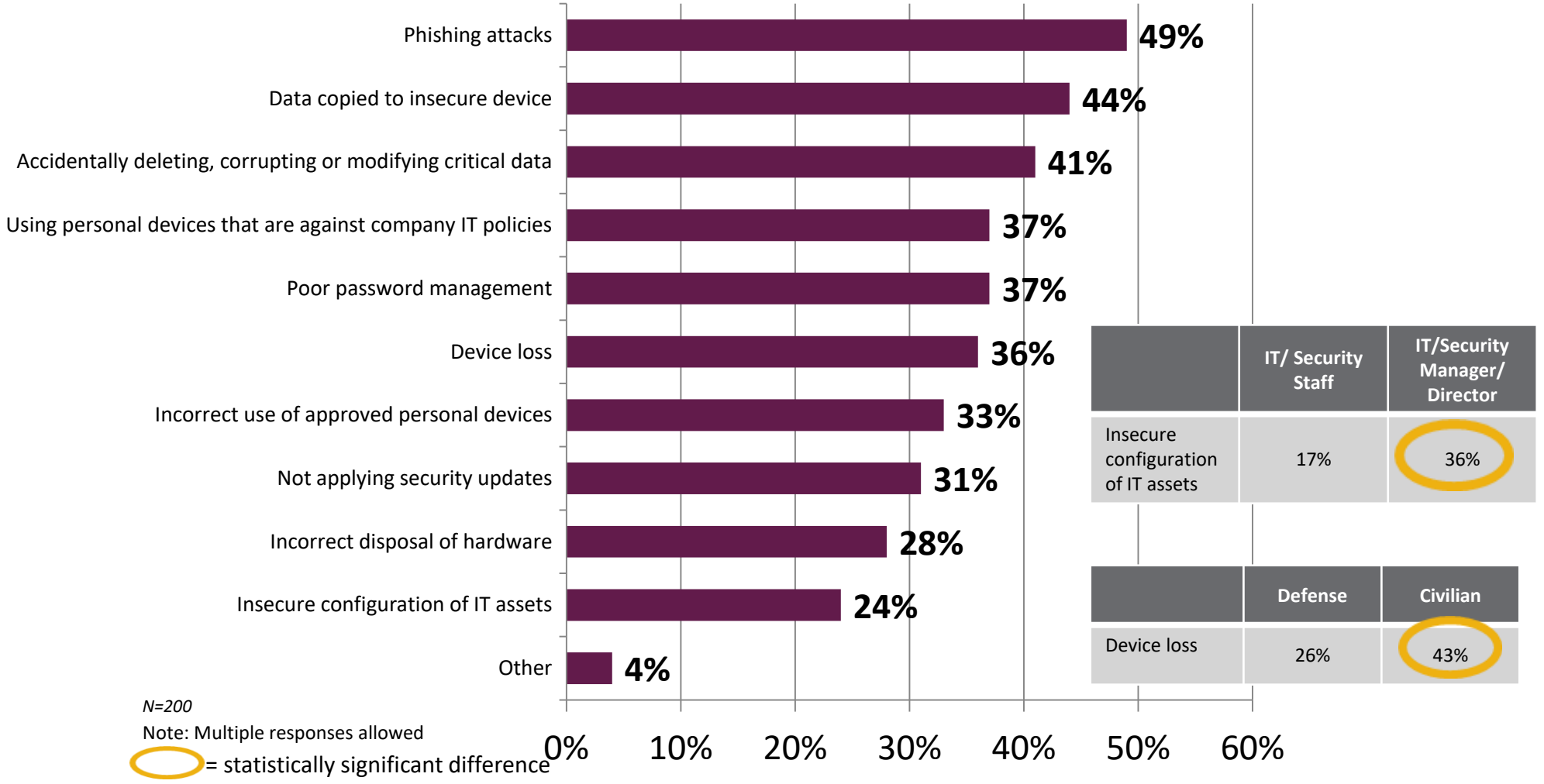
N=200

Note: Multiple responses allowed

= statistically significant difference

Q *In today's environment, what makes insider threat detection and prevention more difficult?*

Accidental Insider Breach Causes



	IT/ Security Staff	IT/Security Manager/ Director
Insecure configuration of IT assets	17%	36%

	Defense	Civilian
Device loss	26%	43%

N=200

Note: Multiple responses allowed

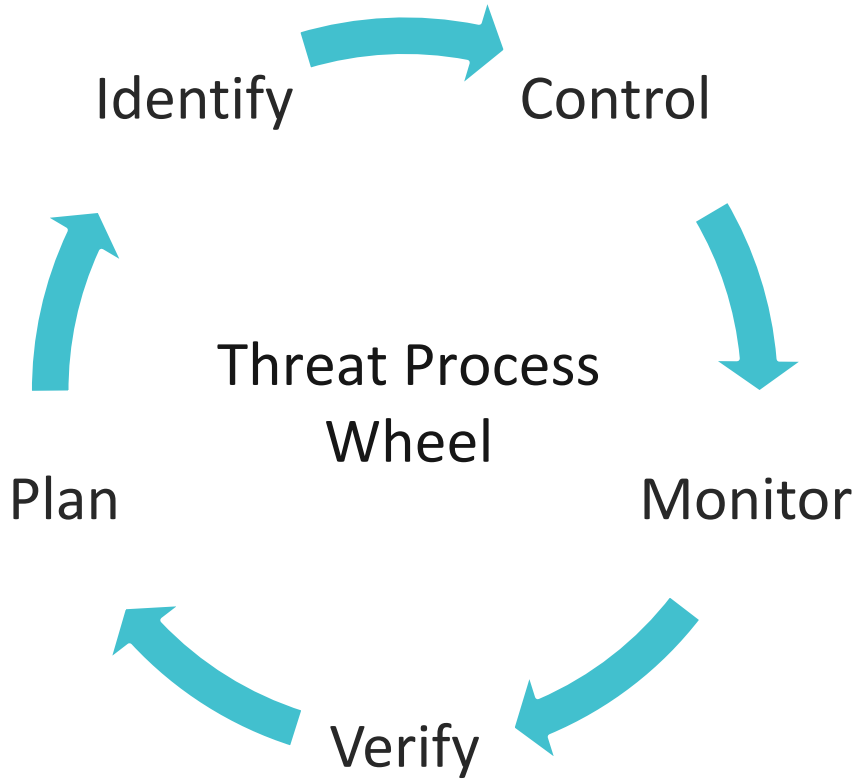
= statistically significant difference

Q *What are the most common causes of accidental insider IT security breaches caused by the untrained or careless employee?*

Insider Threat Flow Response Process

Policy Implementation:

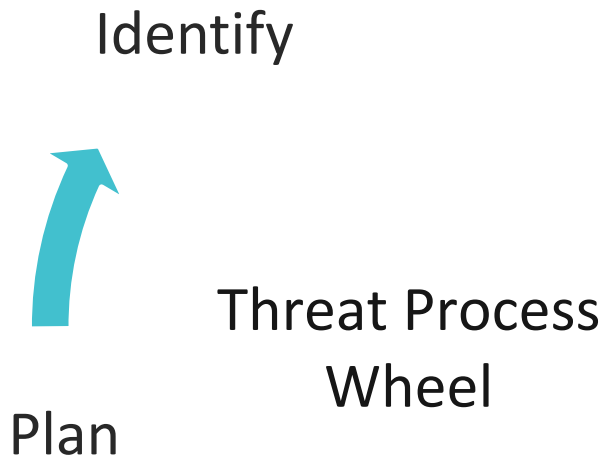
- Reduced risk of outages and security breaches
- Help assure service health and performance
- Stricter control of change and configuration management process
- Faster problem identification and resolution
- Visibility to design changes that avoid future problems



Insider Threat: Identify

Identify:

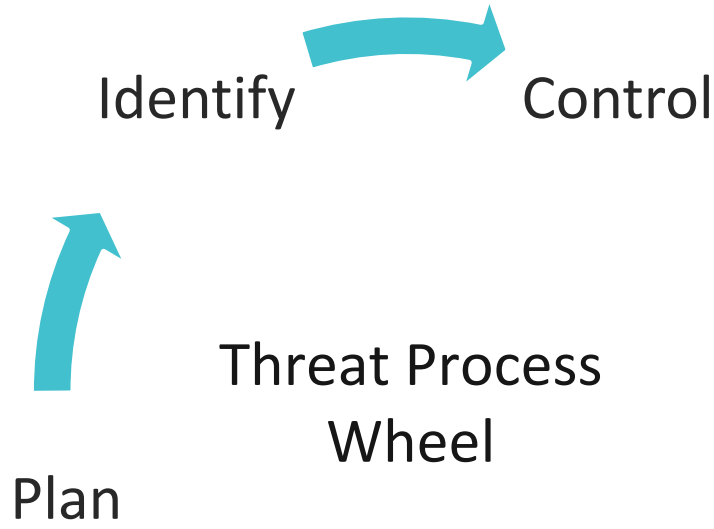
- Updated Inventory of Infrastructure
- Understanding of your Area of Responsibility
- Know and protect your critical assets



Insider Threat: Control

Control:

Organizations typically have a number of tools and processes to *plan for and document* expected changes

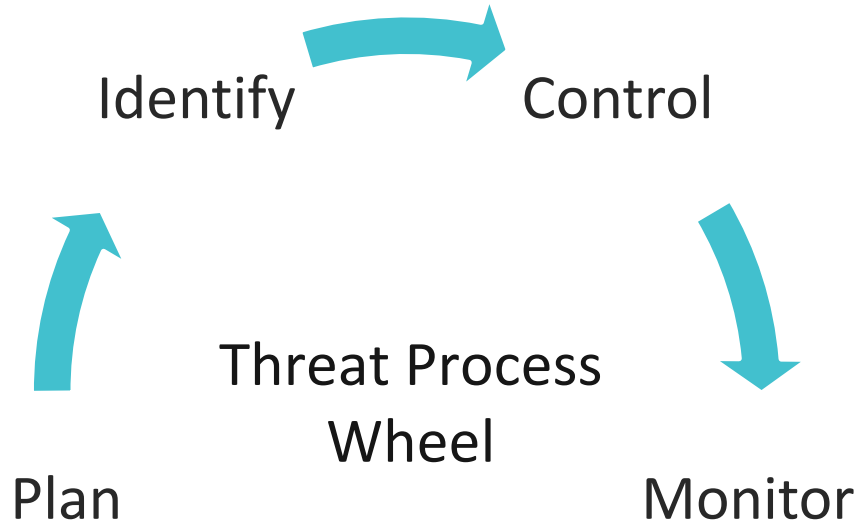


- Develop a formalized insider threat program
- Configuration management tools can help inventory network device configurations, assess them for compliance, and automate change and configuration management
- Configuration Control and automation
- Security Event Appliance (SEIM) Tools to collect, correlate, and respond to threats through automation rulesets

Insider Threat: Monitor

Monitor:

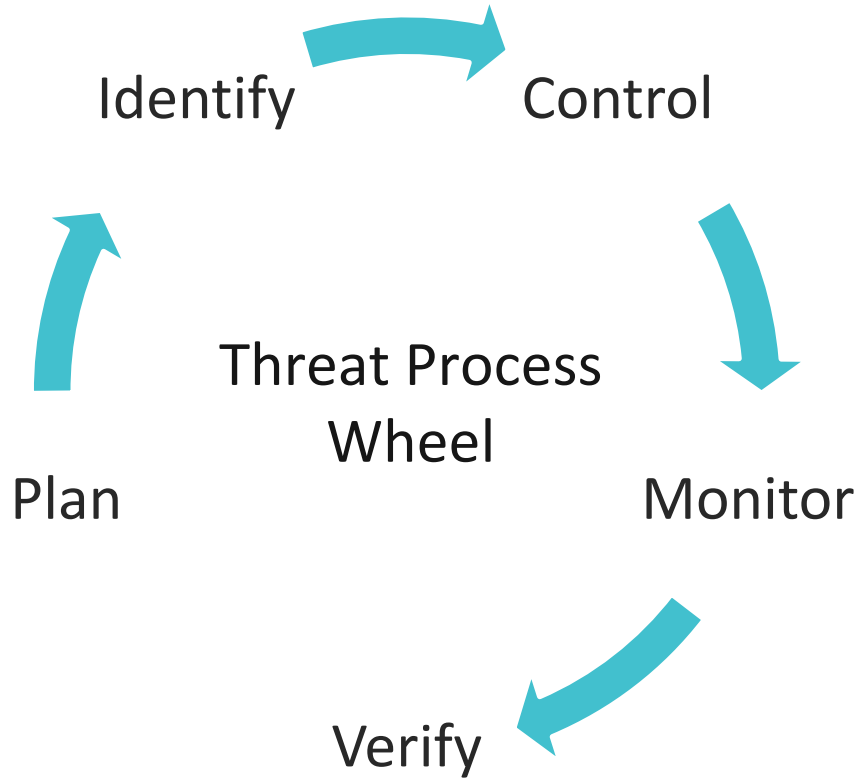
- Deploy solutions for monitoring employee actions and correlating information from multiple data sources
- Network, application, and system monitoring, and management tools, provide needed visibility
- These tools continuously collect data on IT operations and alert on anomalies
- Infrastructure performance monitoring metrics can compliment your other security tools to help detect and mitigate issues, such as Advanced Persistent Threats
- Infrastructure broken into different focuses:
  - Systems
  - Network
  - Management/Mission Impact



Insider Threat: Verify

Verify:

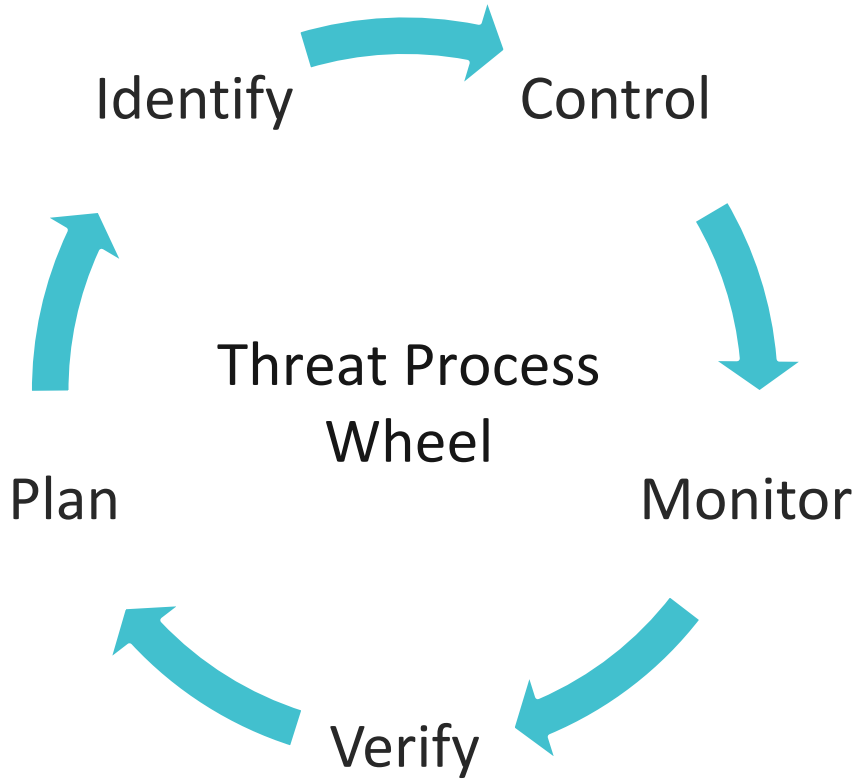
- Performance baselines can help identify threats, and provide constant and valuable insight into network activities
- Clearly document and consistently enforce policies and controls
- Device tracking provides forensic data to help locate, identify, and isolate threat sources, or enforce your BYOD/mobility policies
- Key Areas:
  - Reports
  - Compliance
  - Thresholds



Insider Threat: Repetition

Process Repetition:

- Policy strategy, success for all
- Simple: simplicity is key with an emphasis on ease of use to utilize configuration monitoring, alerting, and auditing
- Incorporate malicious and unintentional insider threat awareness into periodic security training for all employees



Security and Network Management Tools Can Help

Security and network management tools can help with compliance

Network Configuration Manager

Log & Event Manager

Network Performance Monitor

Patch Manager

Access Rights Manager

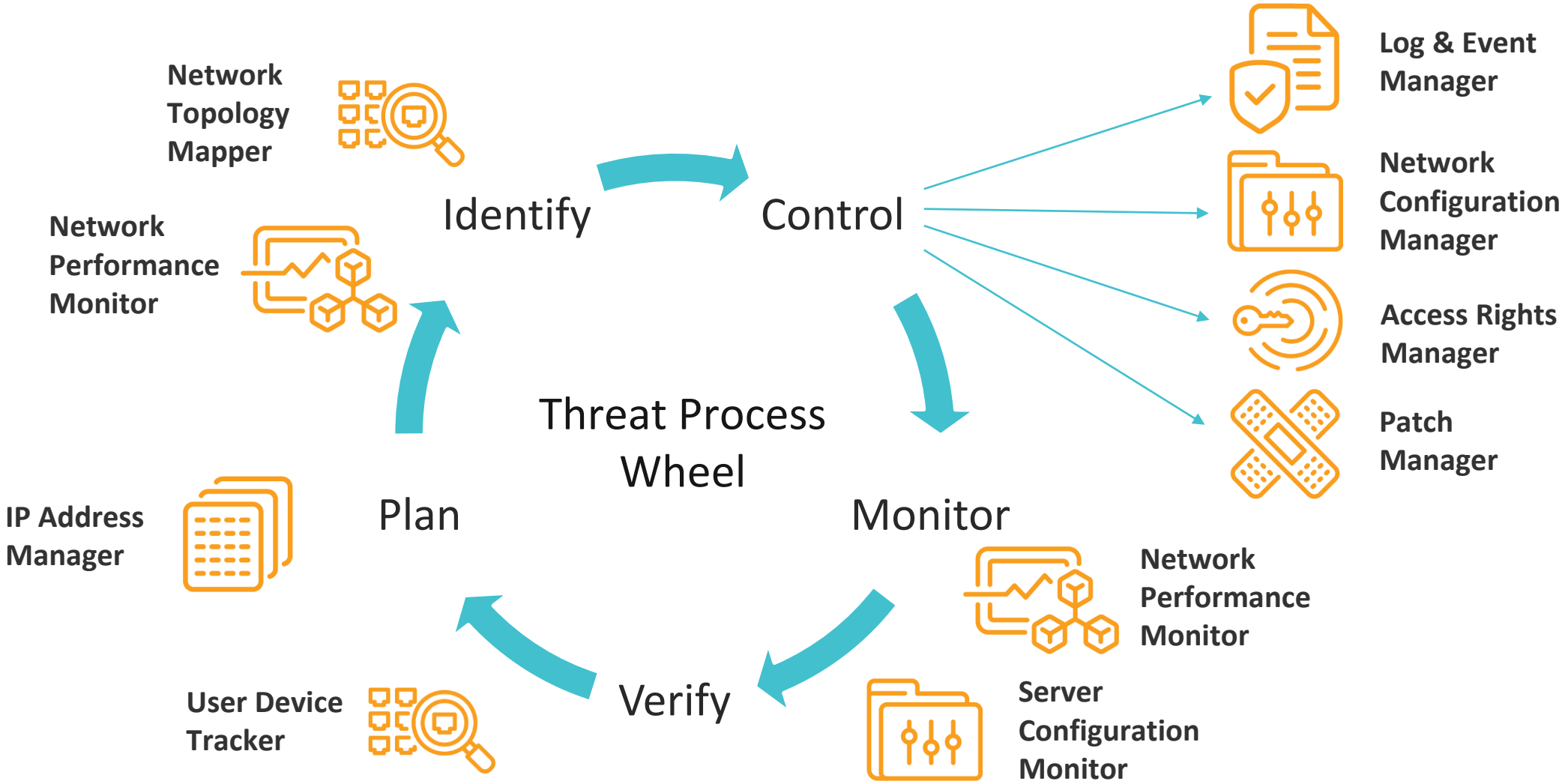
Server Configuration Monitor

IP Address Manager

User Device Tracker

More information: https://www.solarwinds.com/it-security-management-tools

Threat Process Wheel Aligned to SolarWinds Products



Build Security Into Your Community

- Embed security practices and conversations about good security habits within your daily office environment
  - Gamifying security training
  - Document and test your security policies
  - Conduct annual security awareness training
  - Leverage cyber security certification training (e.g., DOD 8570)
  - Document security incident reporting procedures (e.g., wallet cards, desk references, etc.)
  - Utilize Two Factor Authentication

Build Security Into Your Community

- Implement an approach styled after a Secure Development Lifecycle (SDL)
  - SDLs consist of the security processes and activities performed for every software release
  - Although conceived for development, their principles can be applied across your company
  - For example, by agreeing upon standard security practices for processes that involve sensitive data, you can help instill Information Security (InfoSec) into your company

When Combating the Insider Threats

- Meeting compliance standards does not mean you are secure
- Careless or untrained insiders can be the largest source of security threats
- High-performing companies with excellent IT controls experience:
  - Fewer cyberthreats
  - Faster response time to threats
  - Positive results from IT modernization initiatives
- Continuous review of your IT controls may help to improve your security posture
- SolarWinds has tools designed to help

Compliance Resources

- **Review** a blog on how SolarWinds software can help with NIST FISMA/RMF compliance: https://thwack.solarwinds.com/community/solarwinds-community/product-blog/blog/2015/08/01/fisma-nist-800-53-compliance-with-solarwinds-products
- **Review** a blog on how SolarWinds software can help with DISA STIGS compliance: https://thwack.solarwinds.com/community/solarwinds-community/product-blog/blog/2011/09/07/disa-stig-compliance-with-log-event-manager
- **Watch** a federal security compliance video: http://www.solarwinds.com/resources/videos/solarwinds-federal-security-compliance.html
- **Download** a compliance white paper: http://go.solarwinds.com/Compliance_LEM_16?Program=999&c=70150000000qf3c
- **Download** a continuous monitoring white paper: http://go.solarwinds.com/fedcyberWP?=70150000000Plgf

THANK YOU!