tripwire®

CONFIDENCE: SECURED

Critical Security Controls Close The Threat Gap

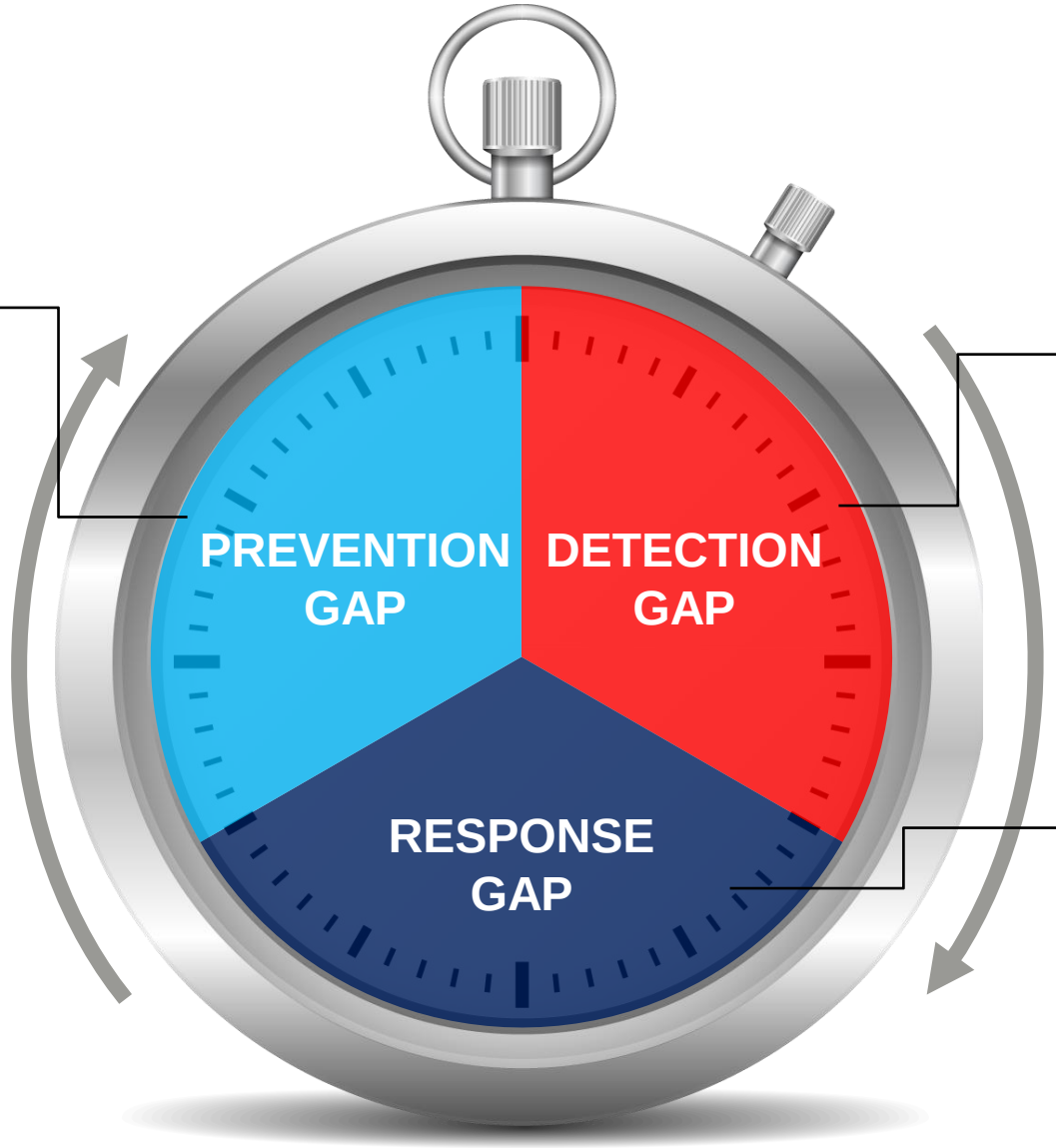
Dwayne Melançon, CISA

Chief Technology Officer

Enterprise Cyberthreat Gap

Prevention Gap
Time to put preventative measures in place to avoid future attacks

Can we prevent this from happening again?



Detection Gap
Time between actual breach and discovery

Have we been breached?

Response Gap
Time between discovery to remediation to limit damage

How bad is it?

Tough Challenge to Close the Cyberthreat Gap

- Advanced attacks—harder to detect and faster compromises
- Too many of alerts—uncoordinated, no business risk prioritization
- Traditional network/endpoint security—fails to detect and respond

Critical Security Controls

Tripwire solution support for the 20 Critical Security Controls (CSC)

20 Critical Security Controls		NSA Rank	Tripwire Solutions
CSC1	Inventory H/W Assets, Criticality, and Location	Very High	●
CSC2	Inventory S/W Assets, Criticality, and Location	Very High	●
CSC3	Secure Configuration Servers	Very High	●
CSC4	Vulnerability Assessment and Remediation	Very High	●
CSC5	Malware Protection	High/Medium	◔
CSC6	Application Security	High	◕
CSC7	Wireless Device Control	High	◔
CSC8	Data Recovery	Medium	
CSC9	Security Skills Assessment	Medium	
CSC10	Secure Config-Network	High/Medium	●

20 Critical Security Controls		NSA Rank	Tripwire Solutions
CSC11	Limit and Control Network Ports, Protocols, and Services	High/Medium	●
CSC12	Control Admin Privileges	High/Medium	◕
CSC13	Boundary Defense	High/Medium	◑
CSC14	Maintain, Monitor, and Analyze Audit Logs	Medium	●
CSC15	“Need-to-Know” Access	Medium	◕
CSC16	Account Monitoring and Control	Medium	◕
CSC17	Data Loss Prevention	Medium/Low	
CSC18	Incident Response	Medium	◔
CSC19	Secure Network Engineering (secure coding)	Low	
CSC20	Penetration Testing and Red Team Exercises	Low	

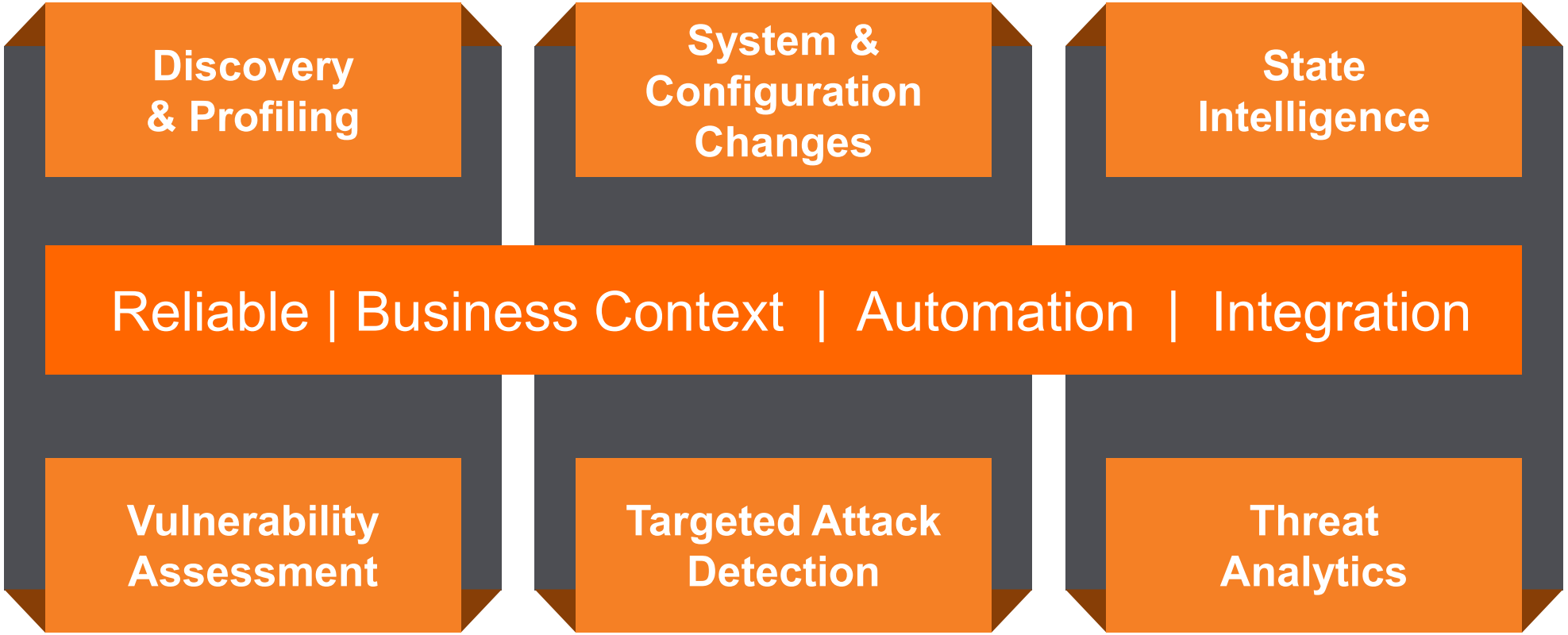
Critical Security Controls

Tripwire solution support for the 20 Critical Security Controls (CSC)

20 Critical Security Controls		NSA Rank	Tripwire Solutions
CSC1	Inventory H/W Assets, Criticality, and Location	Very High	●
CSC2	Inventory S/W Assets, Criticality, and Location	Very High	●
CSC3	Secure Configuration Servers	Very High	●
CSC4	Vulnerability Assessment and Remediation	Very High	●

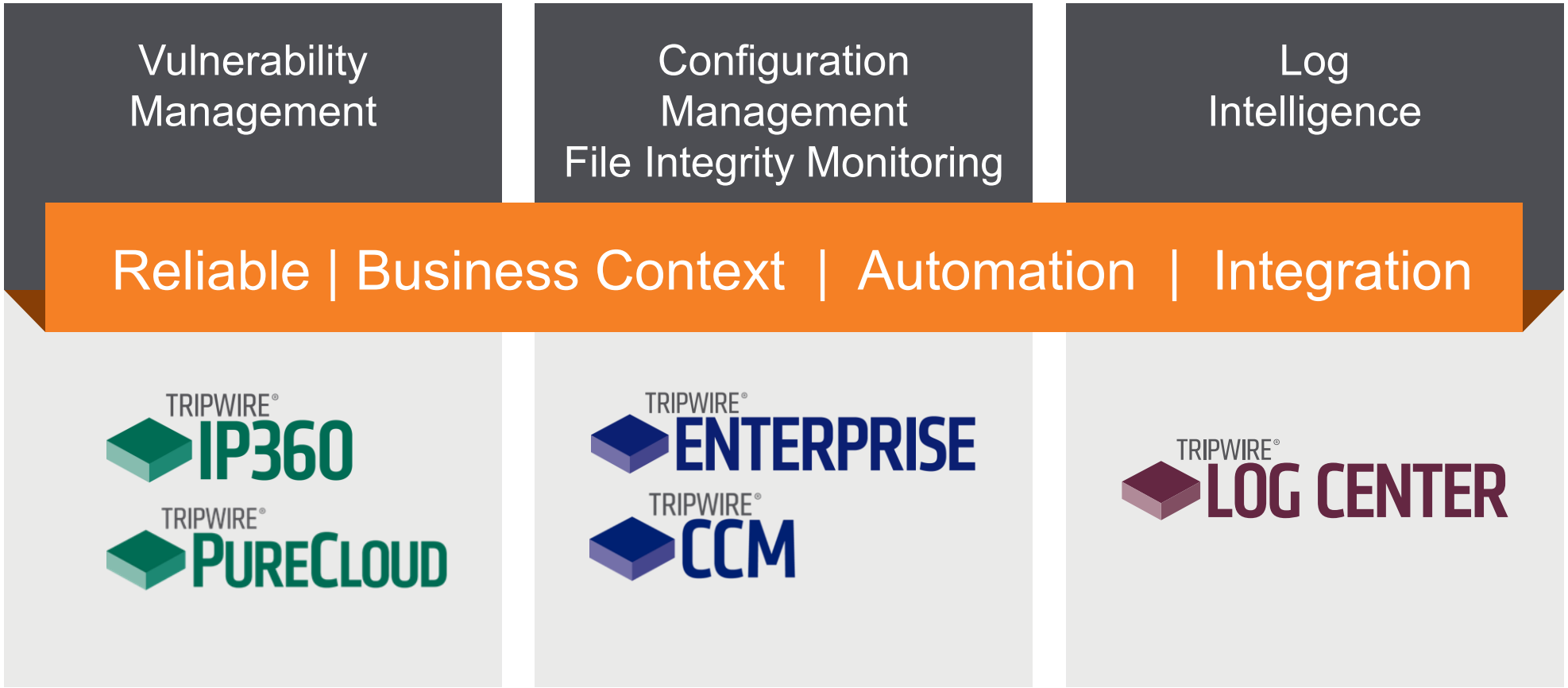
Tripwire Advanced Threat Protection

Detecting indicators of breach, compromise and vulnerability



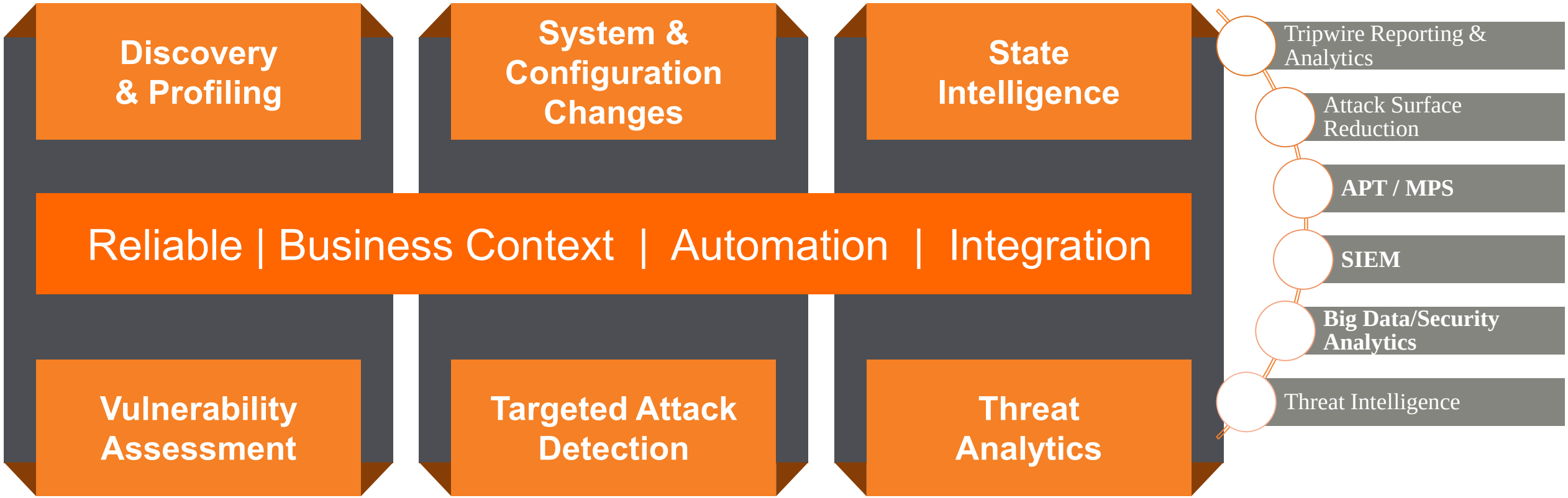
Tripwire Advanced Threat Protection

Detecting indicators of breach, compromise and vulnerability



Tripwire Advanced Threat Protection

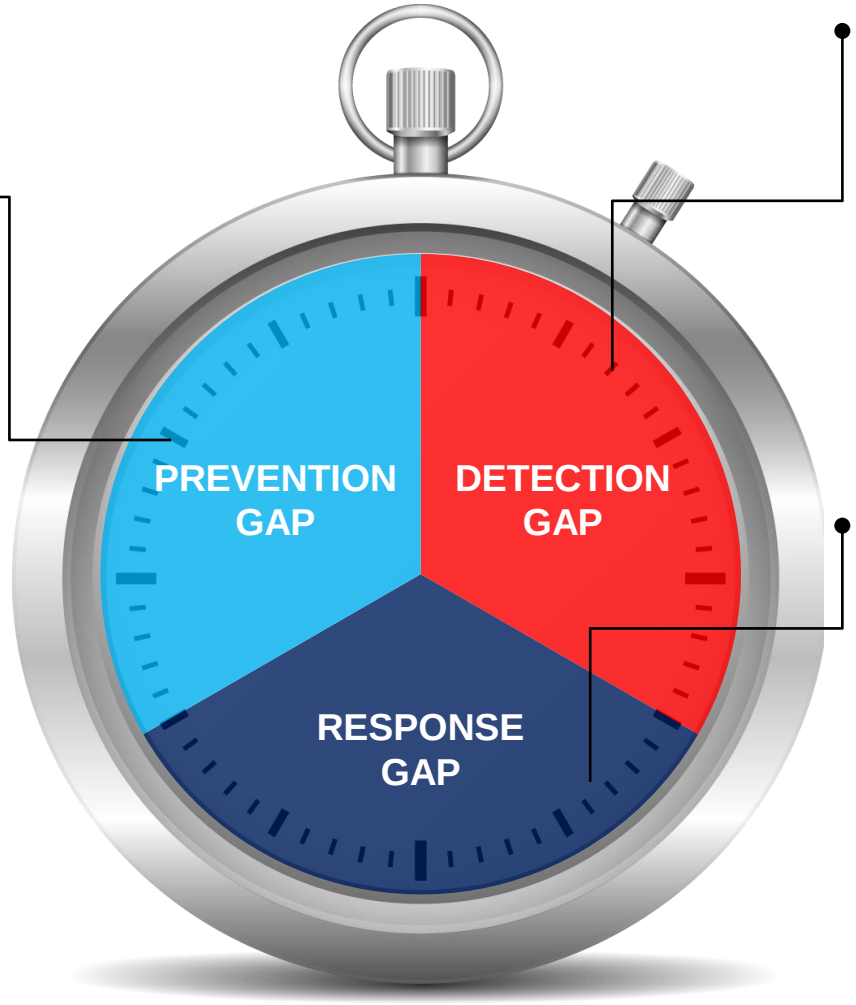
Detecting indicators of breach, compromise and vulnerability



Tripwire: Reducing the Enterprise Cyberthreat Gap

Can we prevent this from happening again?

- Continuous discovery, profiling, vulnerability and configuration assessment
- Harden all configurations to reduce threat surface
- Advanced threat analytics and state intelligence for predictive risk reduction



Have we been breached?

- Real-time detection with advanced threat indicators
- High-confidence source if asset is in intended state
- Empowering instant threat analytics and response

How bad is it?

- Focus on high-value assets based on business context
- Trigger rapid investigation based on detection
- Targeted attack protection through Cybercrime Controls
- Automate or manually isolate and remediate—continuous incident response

TRIPWIRE® IP360 TRIPWIRE® ENTERPRISE TRIPWIRE® LOG CENTER

Helpful Resources

Keep the conversation going

- More about Tripwire: www.tripwire.com
- “State of Security” Blog: www.tripwire.com/blog
- Follow me on Twitter: @thatdwayne
- Exec Guide to the Top 20 Controls: http://bit.ly/top20controls

tripwire®

CONFIDENCE: SECURED

Thank you