TRIPWIRE ENTERPRISE SERVER

UBIT Tech Review February 2019

John Ball john@buffalo.edu

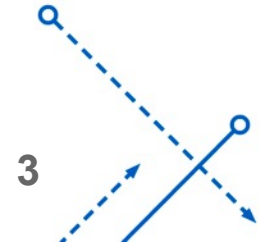
University at Buffalo
Information Technology

What is Tripwire?

- Enterprise Security Configuration Management (SCM) tool
- Standards Compliance software
- File Integrity Management (FIM)
- Client/Server agent based change detection software
- https://www.tripwire.com/

What can be monitored?

- Most major OSes: Windows, Red Hat, CentOS, Ubuntu, SUSE and Debian
- Many vendor-specific OSes: AIX, Solaris, HP-UX, etc.
- Directory Services: Active Directory, LDAP, etc.
- Network Devices: Firewall, IPS and IDS configurations, routers, etc
- Databases: Oracle, MS SQL, DB2 and PostgreSQL
- Virtual and Cloud Environments
- Tripwire's list of supported platforms



How does Tripwire monitor hosts?

Agentless

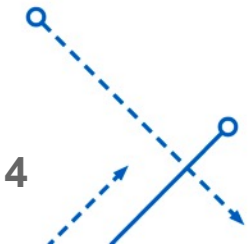
- Polled monitoring over standard protocols

Tripwire Agent client

- software downloaded from Tripwire.com
- installed on hosts
- real time monitoring

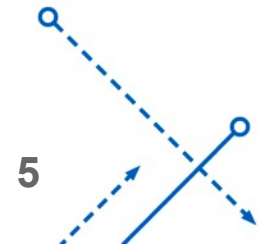
Tripwire Axon agent

- newer, lighter weight agent software



Who is using Tripwire at UB?

- **Enterprise Infrastructure Services**
- **School of Public Health and Health Professionals**
- **School of Social Work**
- **College of Arts and Sciences**
- **School of Dental Medicine**
- **Center for Computational Research**

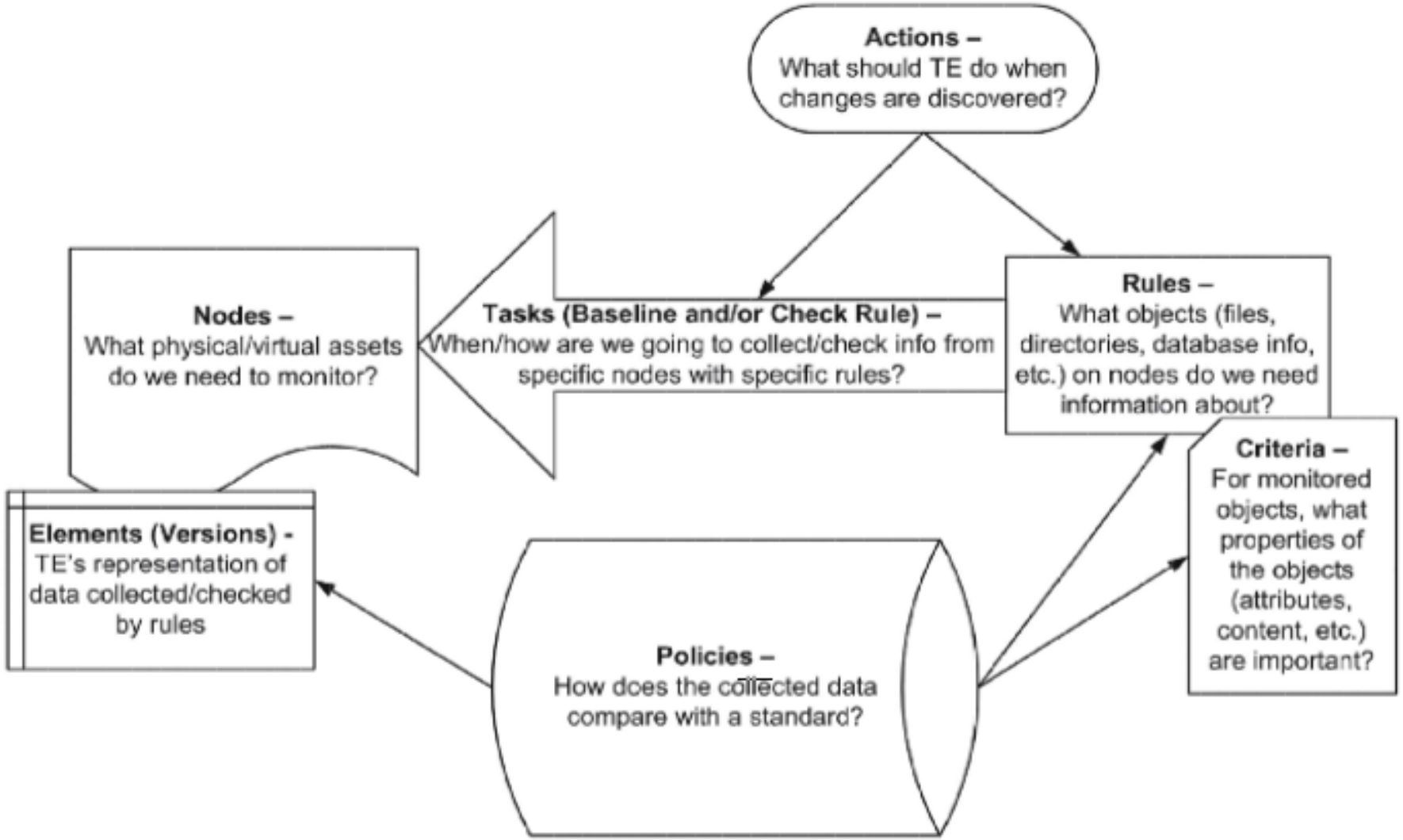


How does EIS use Tripwire?

- EIS has a number of security tools that complement and overlap
- We have been using it since 2006
- Our focus is File Integrity Management
- 2 Tripwire Enterprise Servers for different groups
- We have a Campus Licensing Agreement based on student population which covers the entire campus for as many servers and nodes as we need

EIS Tripwire Process

- An agent is installed on all our hosts (nodes)
- Initial server baseline of a known good state of all monitored objects (elements)
- The server runs tasks that collect information from the agents about system changes outside the baseline
- The changes are parsed through rules defined on any number of criteria (O/S, Application, Role, etc.)
- Reports are generated and sent to the system administrators about the changes
- The system administrators log on to the Tripwire server to review and approve changes (adding them to the systems baseline)


Actions –
What should TE do when changes are discovered?
Nodes –
What physical/virtual assets do we need to monitor?
Tasks (Baseline and/or Check Rule) –
When/how are we going to collect/check info from specific nodes with specific rules?
Rules –
What objects (files, directories, database info, etc.) on nodes do we need information about?
Criteria –
For monitored objects, what properties of the objects (attributes, content, etc.) are important?
Elements (Versions) -
TE's representation of data collected/checked by rules
Policies –
How does the collected data compare with a standard?

Tripwire Enterprise Server for your group

You can run your own Tripwire Enterprise Server in 10 easy steps!

Full requirements can be found on the UBIT Information Security site

http://www.buffalo.edu/ubit/information-for-it-staff/information-security/tripwire.html

Basic requirements:

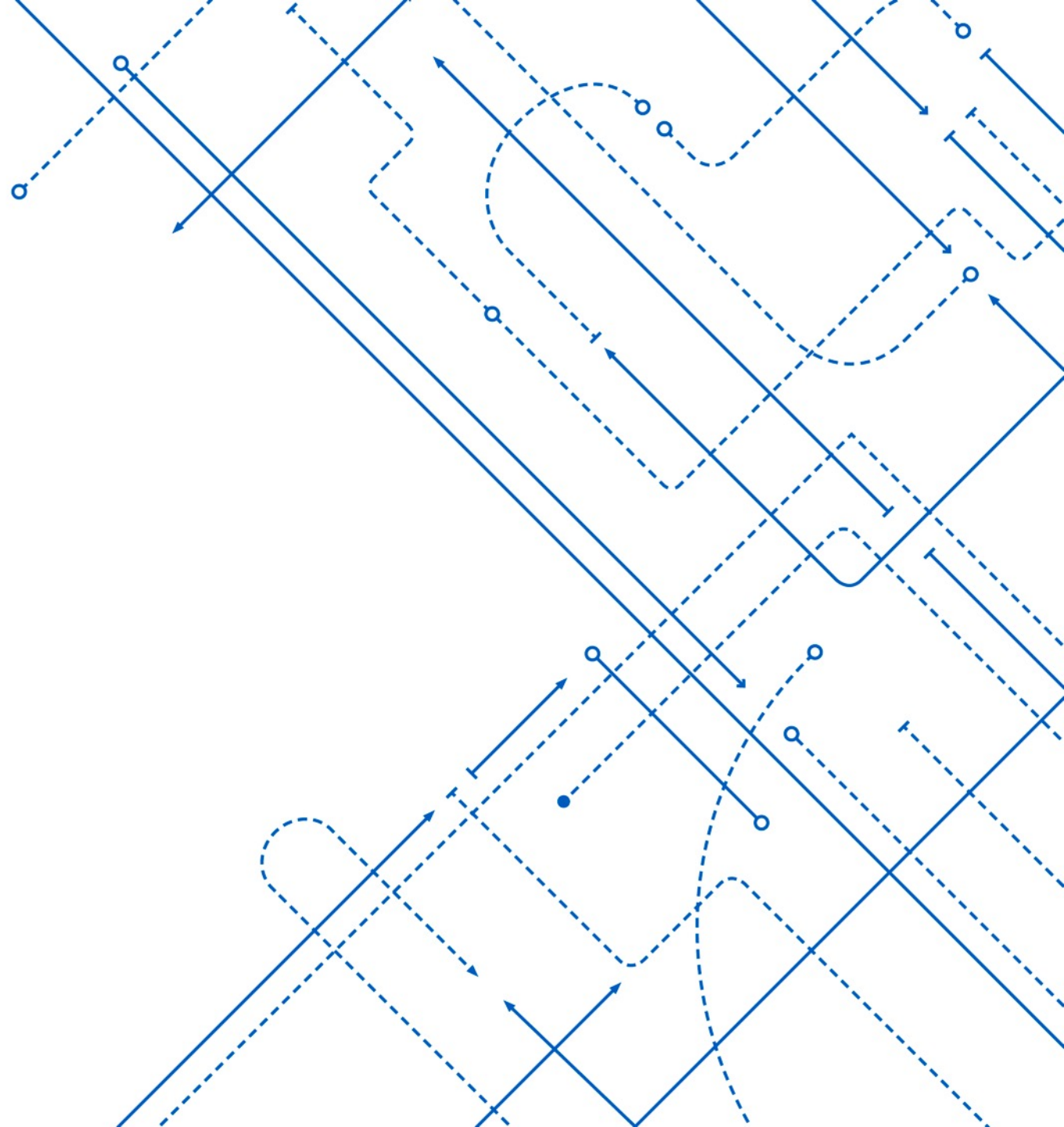
- Server (Windows or Linux)
- Certificate
- External Database instance
- List of Tripwire administrators

Support and Training

The EIS Tripwire team can answer basic questions, but….

- As part of the onboarding process - names and emails for the support staff will be added to the Tripwire support portal
- Full documentation for the product is available at the customer support portal
- Tripwire offers training both in classroom and on line
- Tripwire has virtual user groups a couple times a year - which are valuable sessions where they talk about the state of their products, have the experts give demonstrations for features, and take customer questions and feedback

QUESTIONS?



University at Buffalo
Information Technology