EITS
Enterprise IT Security

TANIUM

Seeking more **Insight?**

Let Us Help.

## Common Initial Use Cases

### Vulnerability Management Program Assessment

- Assess current inventory, processes, staff roles/ responsibilities, and measures of success
- Enable automation and integration between tools and refine processes to support security automation, orchestration, and response

### Merger and Acquisition Risk Assessment

- Understand security risks by priority and potential impact with options to remediate
- Give visibility into financial impact and cost associated with remediation options

### Threat Hunting Assessment

- Identify current or past indicators of compromise through indepth endpoint analysis
- Review and document customer ability to identify, respond, and remediate incidents using existing toolsets

### Incident Response

- Identify advanced persistent attacks with ability to take action toward remediation
- Indepth forensics capabilities to understand depth of attack and work toward root cause analysis

## Common Growth Use Cases

### Compliance Assessment

- Allow us to help you understand how you stack up to compliance and security standards like NIST, GPDR, PCI, HPPA, and IRS PUB1075 as examples
- Enabling ongoing automated processes to track and quickly report on compliance needs

### Discover Sensitive Data

- Quickly and dynamically report on sensitive data across all endpoints in your organization
- Mapping of sensitive data as it flows across endpoints

### Tools optimization

- Identify features and use cases that overlap, pro's/con's across tools, and what makes the most sense based on your teams unique needs
- Outcome is reducing cost and complexity through assessment of tool overlap

### Improve Identify and Authentication Capabilities

- Report on live endpoint and user based actions to improve identity and access control
- Improve zero trust capabilities through advanced visibility and control of endpoints and users

### Sensitive Data Discovery

- Identify where sensitive data is located, how it is being accessed, and how it's flowing within your organization

### Patch Management

- Replace tools that do not provide comprehensive visibility into networked devices or respective patch status.
- Reduce the risk of unknown patch compliance and boost reporting accuracy.
- Ensure a consistent, fast, and scalable patching process that enhances security and patch compliance without failures.
- Simplify software installation, maintenance, and removal of third-party software - reducing complexity and improving resilience.
- Utilize templates for importing and deploying third-party software - eliminating the need to browse websites for the latest updates or creatng deployment packages.

**www.eits.com** • **704-900-8042**