INL/EXP-23-73712-Revision-0

Coslett Intern Poster: Faster Cyber Attack Response Using STIG

August 2023

Faith Kimberley Coslett

Changing the World's Energy Future

Idaho National Laboratory

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/EXP-23-73712-Revision-0

Coslett Intern Poster: Faster Cyber Attack Response Using STIG

Faith Kimberley Coslett

August 2023

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

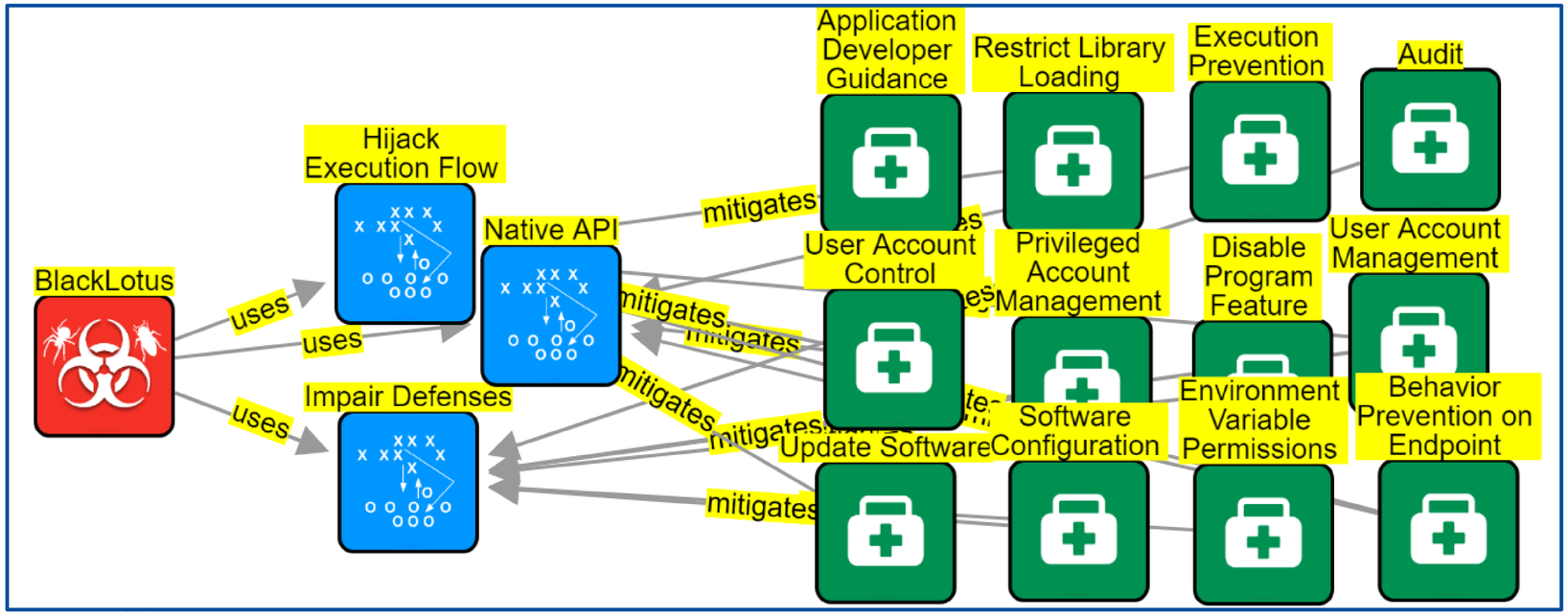
Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Faster Cyberattack Response Using STIG

Intern: Faith Coslett (D520) | CEDAR Lab, University of Wyoming | Mentors: Rita Foster (D520), Zachary Priest (D520), Mike Borowczak (UWyo) | Special Thanks: Alyssa Taylor (D520)

What's the issue?

- Thousands of cyberattacks happen every day
- Protecting against them requires organizations coordinate with each other
- Each attack involves different hackers, targets, malware, methods, defenses, and indicators of their presence
- The defenses created and shared often only apply to one specific attack
- Sharing info and building defenses for each quickly becomes overwhelming
- This slows down attack response time, leaving everyone more vulnerable



How do we make the info manageable?

- **STIG (Structured Threat Intelligence Graph)** is a tool developed by INL
- Turns thousands of words of cyber intelligence into a visual graph
- Intuitive: allows understanding of data at a glance
- Actionable: graph still contains all important data within the objects
- Shareable: compact data makes coordination of defense easier

How do we respond faster to attacks?

- Generalize STIG graphs
- Include defenses that are widely applicable to many attacks of a similar type
- The same graph can be used to defend against many attacks
- Takes much less time than creating new graphs for every individual threat before implementing defenses
- Attack-specific data can be added easily over time

What does this look like in action?

- To demonstrate, this is a section of the STIG graph for the **BlackLotus** malware, a new "**bootkit**" that infects computers at the deepest level
- The green defense objects apply to general, standardized blue attack patterns
- These patterns are used by BlackLotus, but also by many other bootkits
- These widely useable defenses already exist and can be implemented as soon as any similar attack occurs
- Allows for much faster defense than creating a new, specific fix for every similar attack

https://github.com/idaholab/STIG
www.inl.gov
INL/EXP-23-73712

INL/EXP-23-73712