SAND2019-2731C

David R. White, PhD

Director Field Intelligence Element and National Security Programs

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Official website of the Department of Homeland Security

CISA
CYBER+INFRASTRUCTURE

HOME | ABOUT US | ALERTS AND TIPS | RESOURCES | C³ VP

Alert (TA18-074A)

Russian Government Cyber Activity Targeting Energy and Other Critical

Original release date: March 15, 2018 | Last revised: Marc

Print | Tweet | Send | Share

Systems Affected

- Domain Controllers
- File Servers
- Email Servers

Overview

This joint Technical Alert (TA) is the result of analytic e
This alert provides information on Russian governmer
facilities, water, aviation, and critical manufacturing se

CISA
CYBER+INFRASTRUCTURE

HOME | ABOUT US | ALERTS AND TIPS | RESOURCES

Information For

Control System Users
Information for industrial control systems owners, operators, and vendors.

Government Users
Resources for information sharing and collaboration among government agencies.

Home and Business
Information for system administrators and technical users about latest threats.

Chinese Malicious C

The information contained on
Cybersecurity and Infrastructu
procedures used by Chinese
relationships between informa
service providers—and their c
and reduce exposure to Chin
no single solution that will fully

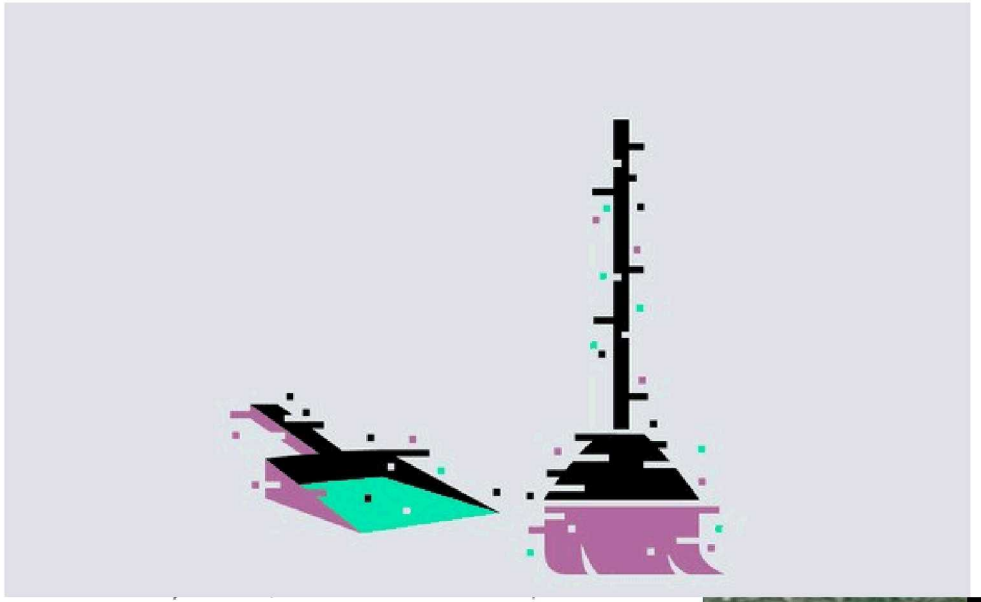
At this time, all known victims
However, because there may
customers follow the recommendations, tools, and actions described in this page and in Alerts TA17-117A and TA18-276A, referenced below. Organizations and individuals that determine their risk to be elevated—either because they are in one of the targeted sectors, or because unusual activity is detected—should conduct a dedicated investigation to identify if any of this malicious activity is in their networks.

For more information on Chinese malicious cyber activity, see:

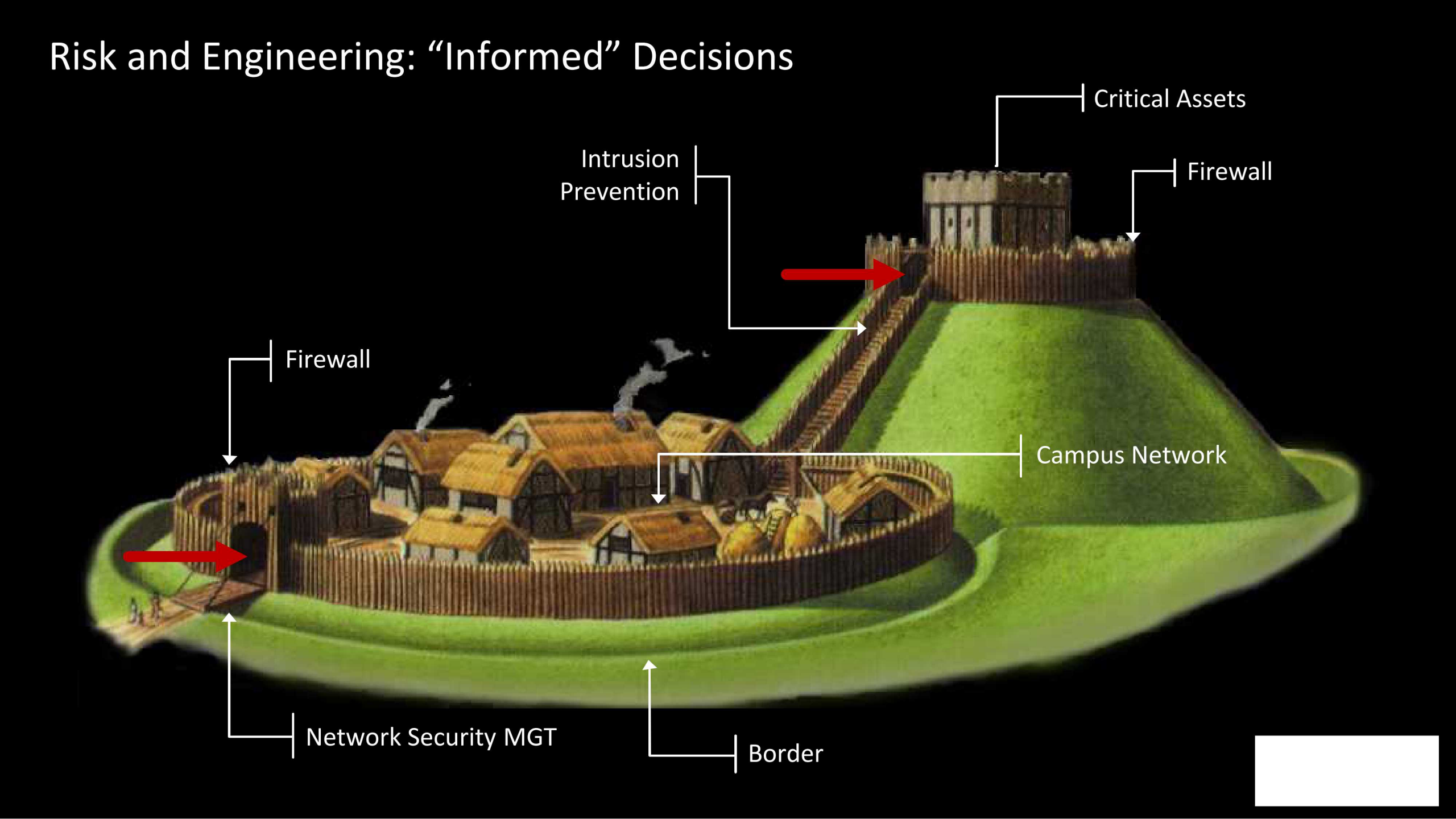
- April 27, 2017: Alert (TA17-117A) – Intrusions Affecting Multiple Victims Across Multiple Sectors

LILY HAY NEWMAN SECURITY 04.17.18 06:30 PM

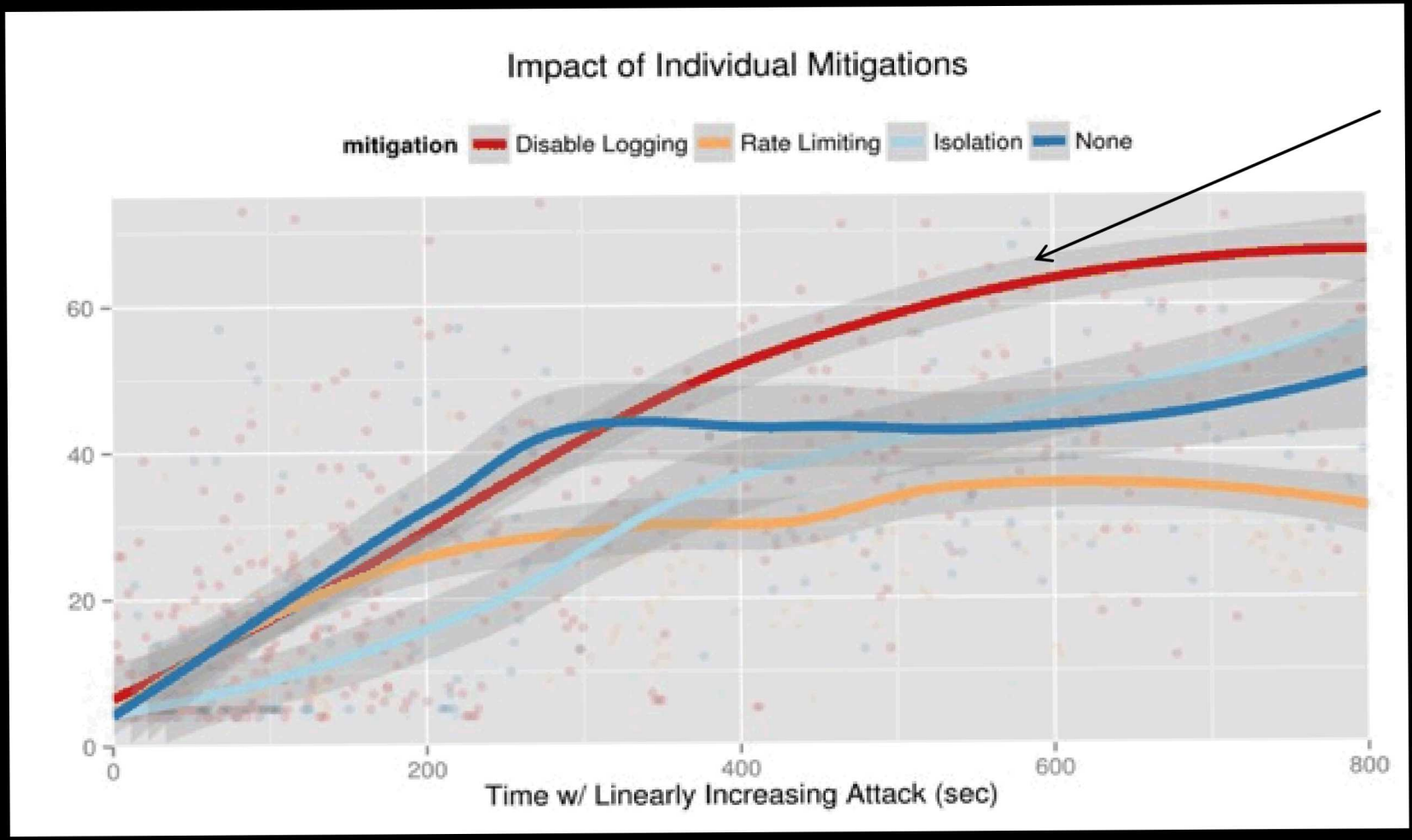
INSIDE THE UNNERVING SUPPLY CHAIN ATTACK THAT CORRUPTED CCLEANER



Risk and Engineering: “Informed” Decisions

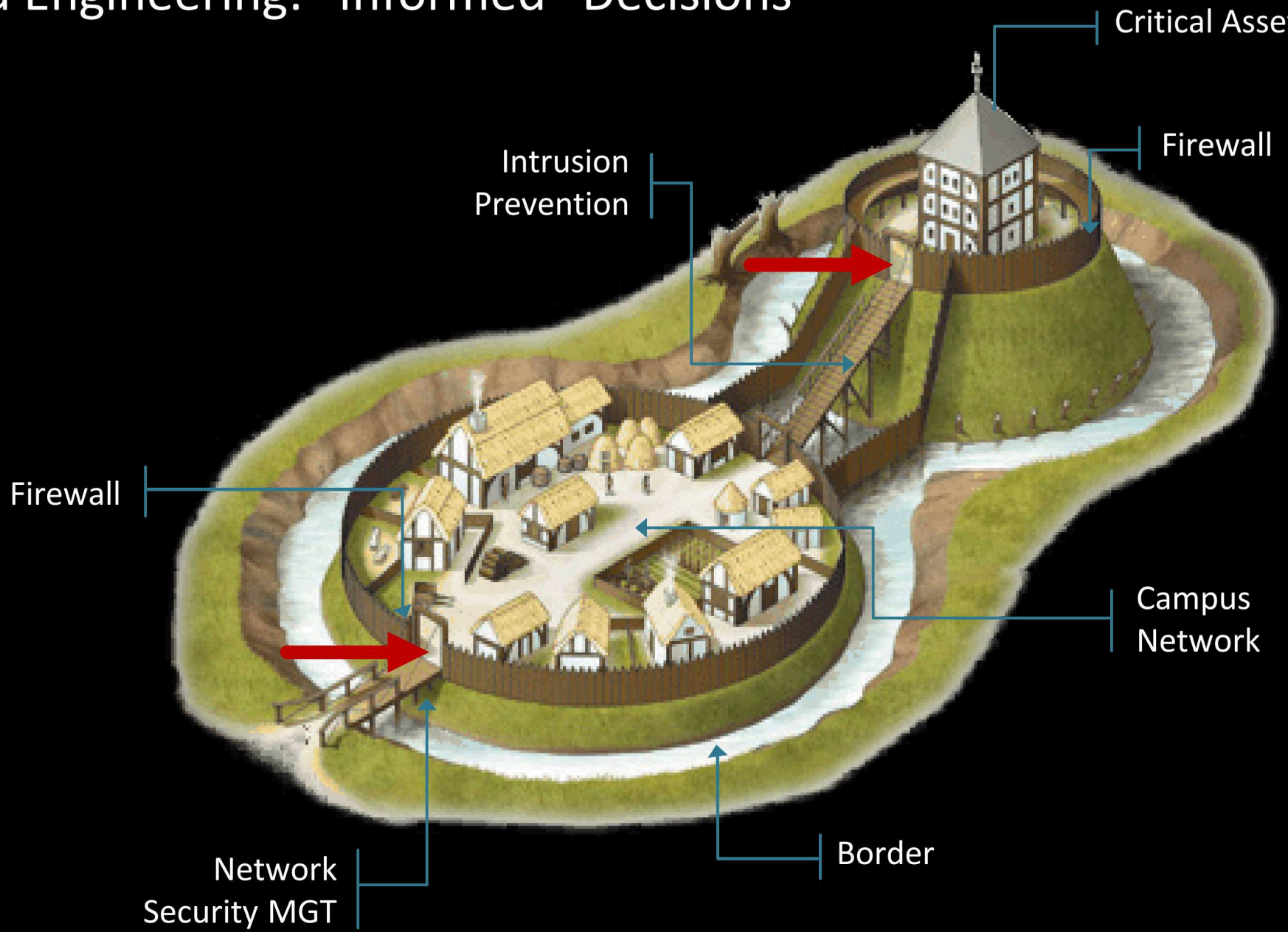


Emulytics™ and Attack Mitigation



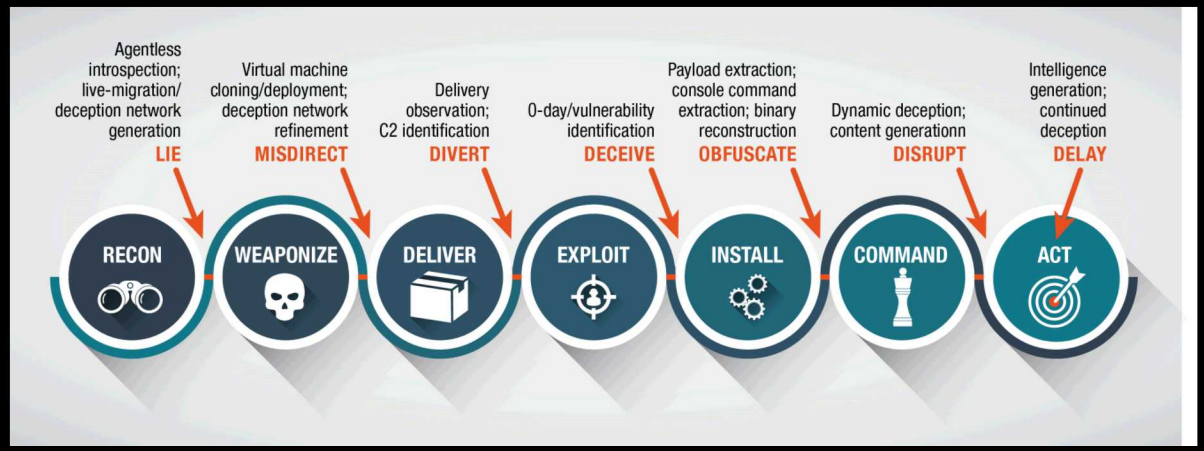
Significantly worse with query logging disabled!

Risk and Engineering: “Informed” Decisions



Beyond Cyber Experimentation

Deception- HADES



Software Assurance- FUNK