TERMINAL OFFLINE • AUTHORIZATION REQUIRED

IMPROVING INSIDER THREAT DEFENSE BY WATCING STAR TREK

PRESENTED TO THE 2022 NKU CYBERSECURITY SYMPOSIUM

JUSTIN HALL

SR MANAGER, RESEARCH

TENABLE

02-24156

03-41248

04-14702

05-32456

GREETINGS! I'M JUSTIN.

- HUSBAND AND DAD
- CINCINNATI NATIVE
- STAR TREK NERD
- SECURITY NERD
- NERD
- SR MANAGER, RESEARCH - TENABLE
- FORMER HELPDESK TECH, SYSADMIN, IT DIRECTOR, SECURITY ENGINEER, INCIDENT RESPONDER, SECURITY ARCHITECT, CONSULTANT, PENTESTER, ETC

02-24156

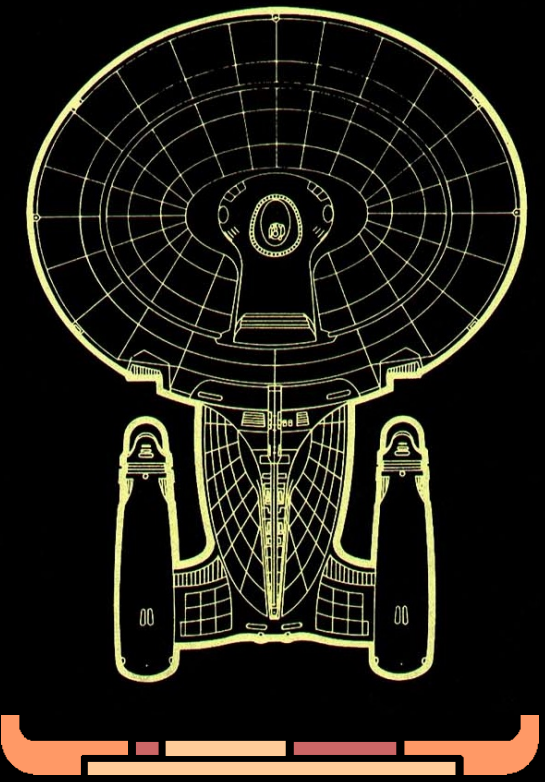
03-41248

04-14702

05-32456

WHAT IS STAR TREK?

THE GREATEST FUTURE SCI-FI FRANCHISE EVER CREATED.



- SET IN THE 2200'S – 2400'S
- EARTH IS A **UTOPIA** – NO MORE DISEASE, WAR, OR HUNGER
- EARTH IS A MEMBER OF A GALAXY-WIDE COLLECTIVE CALLED THE **UNITED FEDERATION OF PLANETS** WITH 150 OTHER SPECIES
- THE FEDERATION'S SPACE EXPLORATION AND MILITARY ARM IS CALLED **STARFLEET**
- IN 2367, THE STARFLEET FLAGSHIP, THE **USS ENTERPRISE-D**, IS HELMED BY **CAPT. JEAN-LUC PICARD**
- THE EXECUTIVE OFFICER IS LT. CMDR. **DATA**, A ONE-OF-A-KIND **ANDROID**
- EVERY WEEK THE CREW OF THE ENTERPRISE GOES ON AN ADVENTURE AND EXPLORES THE GALAXY IN HOT 90'S JUMPSUITS

02-24156

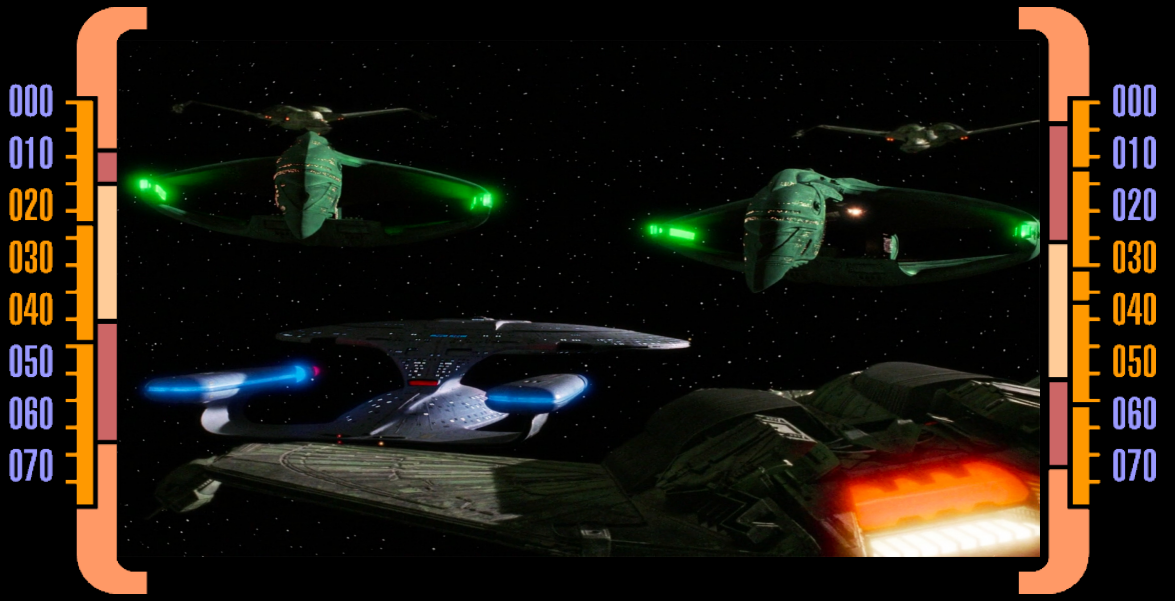
03-41248

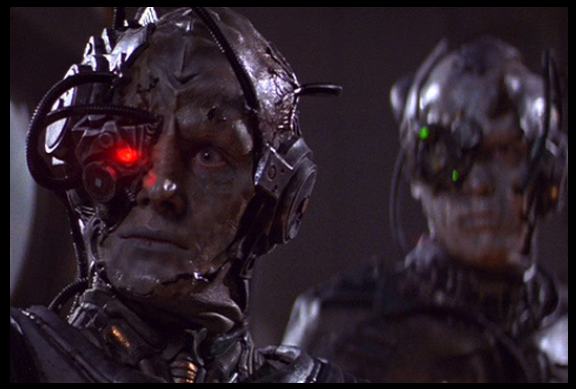
04-14702

05-32456

WHAT IS THREAT MODELING?

THE PRACTICE OF UNDERSTANDING THREATS (INCLUDING **GOALS**, **BEHAVIOR**, AND **POTENTIAL IMPACT**) AND DEVELOPING A **TAXONOMY** SO THAT DEFENSIVE COUNTERMEASURES CAN BE APPLIED.





02-24156

03-41248

04-14702

05-32456

STAR TREK THE NEXT GENERATION SEASON 4 EPISODE 3: "BROTHERS"

STARDATE: 44085.7

LT. CMDR. DATA IS REMOTELY TRIGGERED BY HIS CREATOR, DR. NOONIEN SOONG, TO RETURN TO SOONG'S RESIDENCE. TO ACHIEVE THIS, DATA TAKES CONTROL OF THE ENTERPRISE, AND THE CREW MUST REGAIN CONTROL SO THAT A CHILD THAT IS NEAR DEATH CAN BE TREATED.

READ A RECAP OF THE EPISODE AT https://memory-alpha.fandom.com/wiki/Brothers_(episode)

02-24156

03-41248

04-14702

05-32456

INCIDENT ANALYSIS

HOW DID DATA TAKE OVER THE SHIP?

- DATA FIRST RESTRICTS ACCESS TO THE MOST SENSITIVE AREA OF THE SHIP, BY SHUTTING OFF LIFE SUPPORT, AND THEN PHYSICALLY LOCKING OUT THE CREW
- HE THEN STEALS CAPT. PICARD'S CREDENTIALS AND USES THEM TO RESTRICT ACCESS TO THE COMPUTER, SO THAT COMMANDS CANNOT BE ISSUED EXCEPT FROM THE BRIDGE
- HE RESTRICTS ACCESS TO THESE CREDENTIALS WITH A LONG-ASS ENCRYPTION KEY SO THAT THEY CANNOT BE RECOVERED
- HE THEN FLIES THE SHIP TO ITS ROGUE DESTINATION, AND PROVIDES HIMSELF A MEANS TO LEAVE THE SHIP SO THAT HE CANNOT BE STOPPED OR TRACKED

02-24156

03-41248

04-14702

05-32456

THREAT ANALYSIS: LT. CMDR. DATA

- AS SECOND OFFICER, DATA HAS **ELEVATED PRIVILEGES** TO SHIP'S CONTROL SYSTEMS.
- HE CAN **SURVIVE WITHOUT OXYGEN** OR OTHER ENVIRONMENTAL CONDITIONS.
- HE HAS **SUPERHUMAN** SPEED, STRENGTH, MEMORY, AND INTELLIGENCE.
- HE CAN **IMPERSONATE** ANOTHER INDIVIDUAL'S VOICE.

DATA OPERATES WITHOUT SAFEGUARDS OR RESTRAINTS.
AND YET HE IS IMPLICITLY TRUSTED BY THE CREW.

02-24156

03-41248

04-14702

05-32456

PARALLEL ANALYSIS: INSIDER THREAT ACTIVITY

MISUSE

END USERS INADVERTENTLY EXPOSE SENSITIVE DATA AND ASSETS, BY FAILING TO FOLLOW SECURITY POLICIES (OR BECAUSE INSUFFICIENT SECURITY CONTROLS EXIST)

EXAMPLES:
MICROSOFT
UK NHS
VERIZON

COERCED

ATTACKERS PAY EMPLOYEES TO PROVIDE THEM WITH INSIDER ACCESS, MOST NOTABLY LAPSUS$

EXAMPLES:
OKTA
MICROSOFT
NVIDIA
T-MOBILE
ROCKSTAR
UBER

SELF-MOTIVATED

DISGRUNTLED EMPLOYEES WITH PRIVILEGED ACCESS WISH TO HARM THEIR CURRENT OR FORMER EMPLOYER

EXAMPLES:
COCA-COLA
TOYOTA
UBER

02-24156

03-41248

04-14702

05-32456

CONTROL STRATEGIES

02-24156

03-41248

04-14702

05-32456

CONTROL: LEAST PRIVILEGE

- **RISK**: PRIVILEGED USERS THAT ARE NOT RESTRICTED IN THEIR RIGHTS MAY ABUSE THEM AND ACCESS ASSETS AND DATA OUTSIDE THEIR AUTHORIZED PURVIEW

- **COUNTERMEASURE**: GRANULAR ACCESS CONTROLS THAT RESTRICT ACCESS FOR MOST PRIVILEGED USERS TO ONLY SYSTEMS THAT ARE NECESSARY
- REQUIRES CONTROLS TO BE IMPLEMENTED AT NETWORK, OS, AND AUTHENTICATION LAYERS
- REQUIRES CONTINUOUS REVIEW AND REEVALUATION OF ACCESS LISTS

02-24156

03-41248

04-14702

05-32456

CONTROL: BACKGROUND CHECKS

- **RISK**: YOUR STAFF MAY HAVE A HISTORY OF CRIMINAL BEHAVIOR THAT INCREASE THE LIKELIHOOD OF MISBEHAVIOR OR THREATENING THE ORGANIZATION

- **COUNTERMEASURE**: RUN CRIMINAL BACKGROUND CHECKS ON NEW HIRES, ESPECIALLY IF EMPLOYEES WILL HAVE PRIVILEGED ACCESS TO SENSITIVE MATERIAL OR CRITICAL SYSTEMS
  - IF YOU WORK WITH CLASSIFIED DATA OR CONTROLLED UNCLASSIFIED INFORMATION, FOREIGN ACTORS MAY TRY TO RECRUIT YOUR EMPLOYEES AS AGENTS OR SPIES

02-24156

03-41248

04-14702

05-32456

CONTROL: BEHAVIOR BASELINING

- **RISK**: MALICIOUS INSIDERS MAY USE ELEVATED PRIVILEGES TO ACCESS ASSETS OR DATA THAT ARE ATYPICAL BASED ON THEIR JOB PROFILE OR RESPONSIBILITIES

- **COUNTERMEASURE**: PROFILE COMMON BEHAVIOR FOR PRIVLEGED USERS
  - DAYS/TIMES WHEN WORK OCCURS
  - ACCOUNTS COMMONLY USED
  - SYSTEMS COMMONLY ACCESSED
  - NETWORK/GEOGRAPHIC LOCATIONS FROM WHICH ACCESS OCCURS
- ALERT ON NONSTANDARD ACTIVITY WITH SIEM, UEBA SOLUTIONS

02-24156

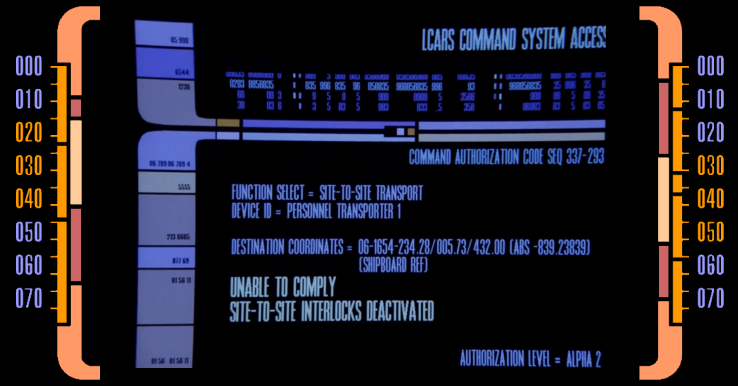
03-41248

04-14702

05-32456

CONTROL: MFA FOR PRIVILEGED ACTIONS

- **RISK**: EXTERNAL ATTACKERS MAY STEAL, OR BE PROVIDED, PRIVILEGED CREDENTIALS WHICH CAN BE USED FOR MALICIOUS TO ACCESS SENSITIVE DATA OR CRITICAL SYSTEMS



- **COUNTERMEASURE**: REQUIRE MULTIFACTOR AUTHENTICATION FOR PRIVILEGED ACTIVITY USING STRONG KEYS, SUCH AS PHYSICAL TOKENS OR BIOMETRICS
  - CREATION OR REMOVAL OF PRIVILEGED ACCOUNTS, OR ADDITIONS TO A PRIVILEGED GROUP
  - MAJOR SYSTEM CONFIGURATION CHANGES, DISABLING SECURITY CONTROLS
  - RETRIEVING LARGE VOLUMES OF SENSITIVE DATA
  - EXPORT OF PRIVATE KEYS

02-24156

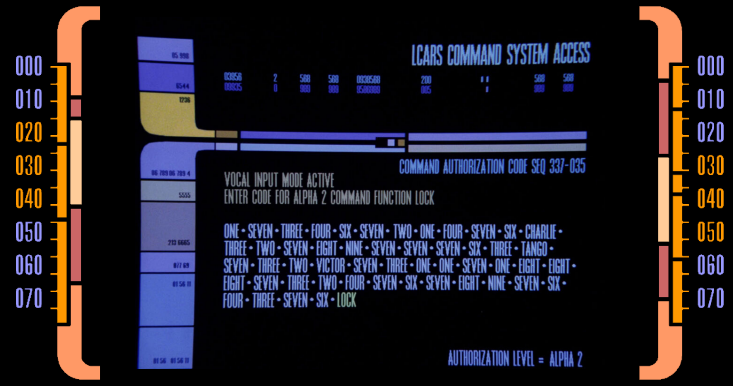
03-41248

04-14702

05-32456

CONTROL: DUAL CONTROL FOR PRIVILEGED ACTIONS

- **RISK**: MALICIOUS INSIDERS MAY WORK WITHIN EXISTING PATTERNS USING AUTHORIZED ACCESS TO PERFORM HARMFUL ACTIONS



- **COUNTERMEASURE**: IMPLEMENT DUAL CONTROL / TWO-PERSON INTEGRITY FOR A LIMITED SET OF PRIVILEGED ACTIONS
  - CURRENTLY UNSUPPORTED BY MOST ENTERPRISE AUTHENTICATION PRODUCTS
  - CAN BE IMPLEMENTED WITH PRIVILEGED ACCESS MANAGEMENT / VAULT SOLUTIONS: CYBERARK, HASHICORP, THYCOTIC
  - FEATURE IN PROGRESS FOR SOME MFA SOLUTIONS

02-24156

03-41248

04-14702

05-32456

CONCLUSIONS

- INTENTIONAL MAPPING OF EMPLOYEE ROLES TO USER, NETWORK, AND ASSET PRIVILEGES IS HARD BUT NECESSARY
- START WITH CRITICAL ASSETS, AND LARGE GROUPS OF USERS, AND INCREASE GRANULARITY IN PHASED APPROACH OVER TIME
- ZERO TRUST NETWORK ACCESS HELPS SOLVE THIS PROBLEM FOR ALL USERS AND ASSETS ACROSS THE ENTIRE ENTERPRISE

02-24156

03-41248

04-14702

05-32456

THANK YOU FOR ATTENDING
LIVE LONG AND PROSPER

JHALL🖖TENABLE.COM