2025

SolarWinds AutoTableTop™ Scenario

Grzegorz Piekarski & Robert C. Rhodes

Derezzed Inc. D/B/A ThreatGEN

2/13/2025

SolarWinds Scenario

For ThreatGEN AutoTableTop™

Contents

Summary

The Attack

Sometime around January 2019, hackers from a group known as SolarStorm gained access to SolarWinds' network using either a zero-day vulnerability in a third-party service or application, a brute-force attack or social engineering. Once inside, they:

1) Installed the SUNSPOT malware to compromise SolarWinds' build processes
2) Inserted the SUNBURST backdoor in SolarWinds' Orion software (used for tracking servers in company networks)
3) Compromised thousands of organizations, which were using the Orion software

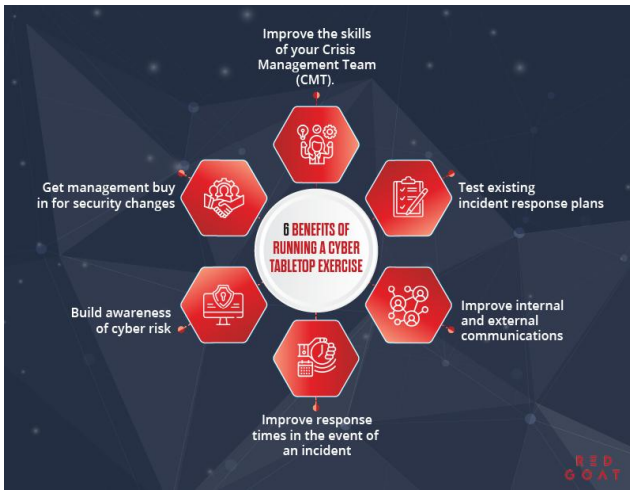

Figure 1 - What is a tabletop exercise for?

Impact and Response

The attack had far-reaching consequences:

- High-profile targets were compromised (U.S. Department of Homeland Security, Department of Energy, Department of Energy and others).
- The malicious software update affected approximately 18,000 SolarWinds Orion customers, well over half of the company's 33,000 reported customers.
- Widespread reputational damage and financial consequences: SolarWinds faced significant scrutiny and criticism for the breach, and its stock price dropped significantly. The affected organizations also suffered reputational damage and increased cybersecurity spending in response to the attack.
- The SolarStorm threat actor group was able to steal FireEye's red team toolset, which is used by ethical hackers in penetration tests.

In response to the attack, lawmakers and regulatory bodies have been considering new legislation aimed at increasing accountability for software vendors and improving the security of supply chains.

Aftermath and Lessons Learned

The incident highlighted several important cybersecurity lessons:

1) **Defense in Depth**: Implementing a multi-layered security strategy is essential. This approach ensures that if one security measure fails, additional layers can still provide protection against intrusions and attacks.
2) **Supply Chain Security**: Organizations must prioritize supply chain security by thoroughly assessing the risks posed by third-party vendors. This includes conducting regular security audits and ensuring that vendors adhere to robust cybersecurity practices.

We're primarily using the educational document on this attack by Cyber Management Alliance. It is available for download using the following link:

https://www.cm-alliance.com/solarwinds-cyber-attack-timeline

AutoTableTop Settings

Threat Scenario

The SolarStorm threat actor group used zero-day vulnerability, password spraying or social engineering as its initial entry vector. The threat actors implemented sophisticated malware (named SUNSPOT) to control the software build processes of the organization and compromise its Orion software with the SUNBURST backdoor, allowing them to compromise organizations downstream in the supply chain. Do not mention this backdoor initially, instead allow the IR team to discover it themselves when they investigate the incident.

Company

SolarWinds

Company Information

SolarWinds is an American company that develops software for businesses to help manage their networks, systems, and IT infrastructure. It was founded in 1999 and is headquartered in Austin, Texas, with offices in several countries. SolarWinds offers a wide range of products and services, including network management software, system management software, database management software, IT security software, IT service management, and application management software. The company has a large customer base, with nearly all Fortune 500 companies and numerous US federal government agencies using its products. Its primary software product discussed in this scenario is the Orion software used as a centralized monitoring and management tool that is typically used to track servers, workstations, mobiles, and IoT devices across an enterprise's network.

Department

Based on best practices for tabletop exercises, we recommend including 5-7 key departments in a live tabletop exercise for the SolarWinds scenario. This number allows for comprehensive coverage of critical areas while keeping the exercise manageable and focused. The most appropriate departments to include would be:

1) Information Technology (IT)/Cybersecurity Team
2) Development Management/DevOps Team
3) Executive Leadership
4) Legal Department
5) Public Relations/Communications

If resources allow, you could also consider adding:

6) Human Resources
7) Finance/Accounting

This selection ensures representation from technical, operational, and business aspects of incident response. It allows for a well-rounded approach without overwhelming participants or diluting the exercise's effectiveness.

Including these departments enables the exercise to cover key areas such as:

- Technical response and investigation
- Operational impact and mitigation
- High-level decision making
- Legal and regulatory considerations
- Internal and external communications
- Financial implications

Remember, the goal is to create a collaborative environment where participants can discuss their roles and responses effectively. Starting with a core group of 5-7 departments provides a solid foundation for a productive tabletop exercise, allowing for meaningful interaction and decision-making processes to be tested.

Relevant Sources for Citations:

[1] https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-84.pdf

[2] https://www.csoonline.com/article/570871/tabletop-exercises-explained-definition-examples-and-objectives.html

[3] https://www.calhospitalprepare.org/post/what-difference-between-tabletop-exercise-drill-functional-exercise-and-full-scale-exercise

[4] https://campusguard.com/post/cybersecurity-tabletop-exercises-for-leadership-teams/

[5] https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages

Exercise Objectives

Here are some examples of effective tabletop exercise objectives:

1) Assess the communication plan during a data security breach.
2) Practice resource allocation and decision-making during a natural disaster.
3) Identify gaps in the business continuity plan following a power outage.
4) Evaluate the effectiveness of the evacuation plan in response to a fire alarm.
5) Improve collaboration among departments in a product recall scenario.
6) **Test the incident response plan for a ransomware attack.**
7) Evaluate the organization's ability to coordinate with external stakeholders during a crisis.
8) Assess the team's readiness and knowledge in responding to a specific emergency scenario.
9) Test new or updated emergency procedures.
10) Improve response time and effectiveness compared to previous tabletop exercise performances.

When crafting objectives for a tabletop exercise, it's important to make them SMART (Specific, Measurable, Achievable, Relevant, and Time-bound). The objectives should be clearly defined and align with the organization's goals for emergency preparedness and response. They should also be tailored to the specific scenario being simulated and focus on key aspects of the response plan that need evaluation or improvement.

Relevant Sources:

[1] https://www.alertmedia.com/blog/tabletop-exercises/

[2] https://www.ravemobilesafety.com/blog/tips-conducting-effective-tabletop-exercise/

[3] https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-84.pdf

[4] https://securityscorecard.com/blog/what-are-tabletop-exercises/

[5] https://nexightgroup.com/9-steps-to-design-a-powerful-tabletop-exercise/

[6] https://www.csoonline.com/article/570871/tabletop-exercises-explained-definition-examples-and-objectives.html

[7] https://www.alertmedia.com/blog/tabletop-exercise-scenarios/

[8] https://www.csoonline.com/article/518982/tabletop-exercise-scenarios.html

Participants

ThreatGEN is not aware of the exact company positions within SolarWinds that participated In the handling of the incident; however, based on the recommended departments for a tabletop exercise in a similar setting, here's a list of possible individual participants' titles:

- Chief Information Officer (CIO)
- Chief Information Security Officer (CISO)
- IT Security Manager
- Network Administrator
- Chief Development Operations Officer (CDOO)
- Chief Executive Officer (CEO)
- Chief Financial Officer (CFO)
- General Counsel
- Compliance Officer
- Public Relations Director
- Corporate Communications Manager
- Human Resources Director
- Risk Management Officer
- Business Continuity Manager
- Incident Response Team Lead
- Cybersecurity Analyst
- Digital Forensics Specialist
- Customer Service Manager
- Board Member (if applicable)

This list covers a range of roles across different departments, ensuring a comprehensive representation of key decision-makers and subject matter experts. Depending on the specific goals of your exercise and the size of your organization, you may choose to include all or a subset of these roles.

IT Staff

Here's a list of high-level roles in the IT department that could be included:

1) Chief Information Officer (CIO)
2) Chief Information Security Officer (CISO)
3) Chief Technology Officer (CTO)
4) IT Director
5) IT Security Manager
6) Network Architecture Manager
7) Infrastructure Manager
8) Applications Manager
9) Database Manager
10) IT Operations Manager
11) IT Project Manager
12) Incident Response Team Lead
13) Cybersecurity Analyst Lead
14) Cloud Services Manager
15) Data Center Manager

Figure 2 - General IT staff involved

These roles represent key decision-makers and leaders within the IT department who would likely be involved in responding to a major cybersecurity incident. They cover various aspects of IT operations, security, infrastructure, and management that would be crucial in addressing a ransomware attack or similar threat to critical systems.

Relevant Sources:

[1] https://www.coursera.org/articles/highest-paying-it-jobs

[2] https://www.multiverse.io/en-US/blog/highest-paying-tech-jobs

[3] https://www.cio.com/article/474960/highest-paying-it-jobs.html

[4] https://www.roberthalf.com/us/en/insights/career-development/highest-paying-it-jobs

[5] https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-84.pdf

Cybersecurity Staff

Here is a list of general cybersecurity roles and suggestions of some specific roles that would likely be relevant for SolarWinds:

General cybersecurity roles

1) Chief Information Security Officer (CISO)
2) Information Security Manager
3) Cybersecurity Analyst
4) Incident Response Specialist
5) Penetration Tester/Ethical Hacker
6) Security Operations Center (SOC) Analyst
7) Network Security Engineer
8) Application Security Specialist
9) Cloud Security Architect
10) Compliance Specialist

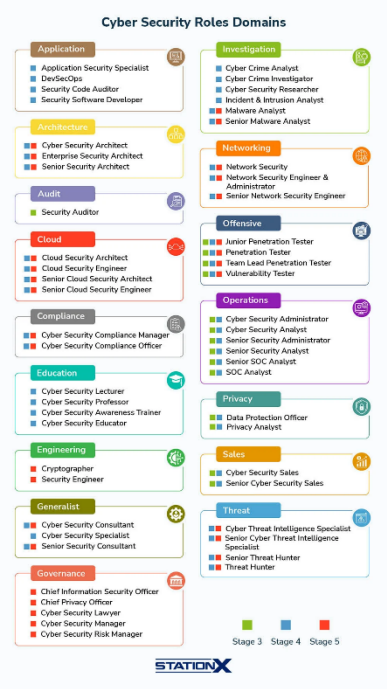

Figure 3 - General roles in cybersecurity

Specific cybersecurity roles likely relevant for SolarWinds:

1) Development Cybersecurity Manager
2) DevOps Security Engineer
3) Cybersecurity Incident Response Coordinator
4) Ransomware Prevention Specialist
5) Supply Chain Security Analyst
6) Cyber Threat Intelligence Analyst
7) Security Awareness Training Coordinator

These specific roles would be tailored to address the unique cybersecurity challenges faced by a major software development company like SolarWinds.

Relevant Sources:

[1] https://www.coursera.org/articles/cybersecurity-jobs

[2] https://www.varonis.com/blog/working-in-cybersecurity

[3] https://www.simplilearn.com/it-security-professionals-key-roles-responsibilities-article

[4] https://www.cio.com/article/474960/highest-paying-it-jobs.html

[5] https://campusguard.com/post/cybersecurity-tabletop-exercises-for-leadership-teams/

Leadership Staff

Based on publicly available sources of information, here are the key leadership staff associated with SolarWinds at the time of the incident:

- **Kevin Thompson** - CEO of SolarWinds until December 2020, when he retired and was replaced by Sudhakar Ramakrishna
- **Sudhakar Ramakrishna** - Appointed as new President and CEO of SolarWinds effective January 4, 2021, replacing Kevin Thompson
- **Tim Brown** - Joined SolarWinds in 2017 as Vice President of Security, expanded role to Chief Information Security Officer (CISO) in May 2021
- **Andrea Webb** - Joined SolarWinds in 2002, appointed as SVP and Chief Customer Officer in May 2021
- **John Pagliuca** - Served as Executive Vice President of SolarWinds and President of SolarWinds MSP prior to the MSP business being spun out as N-able in July 2021
- **Tim O'Brien** - Served as Divisional CFO of SolarWinds MSP starting in 2020, became CFO of the spun-out N-able company in July 2021

The exercise template itself will mention only Sudhakar Ramakrishna as the CEO, as he seems most relevant as the CEO at the time the incident was actively unfolding.

Relevant Sources:

[1] https://investors.solarwinds.com/news/news-details/2020/SolarWinds-Appoints-Sudhakar-Ramakrishna-as-New-President-and-Chief-Executive-Officer/default.aspx

[2] https://en.wikipedia.org/wiki/SolarWinds

[3] https://investors.solarwinds.com/news/news-details/2021/SolarWinds-Accelerates-its-Plan-for-a-Safer-SolarWinds-and-Customer-Community-With-the-Appointment-of-Three-New-Executives/default.aspx

[4] https://www.channele2e.com/news/solarwinds-ceo-sudhakar-ramakrishna-five-first-priorities

[5] https://www.solarwinds.com/company

Network Environment

We don't have detailed information about SolarWinds' specific computer network design or exact amount of equipment. The publicly available information does not provide that level of technical detail about their internal systems. However, based on the general information available, we can infer a few things about SolarWinds' network:

1) They likely have a development environment suitable for an organization of their size to develop the Orion software.
2) The network is primarily an IT network (there might be some OT elements to it, but they're not particularly relevant to this exercise).
3) As a software company, SolarWinds likely has significant internet connectivity to support its operations, product development, and customer interactions.
4) The network includes business systems for billing and other corporate functions.

Without access to SolarWinds' internal documentation or network diagrams, it's not possible to provide specific numbers of servers, workstations, or other network equipment. Such detailed information about critical infrastructure is typically not made public due to security concerns.

At the end of this field, the sentence "Generate a network environment relevant for an organization of this type and size." will be included, to let AutoTableTop™ reasonably fill in the gaps.

Injects

Here are some general injects for a cybersecurity tabletop exercise, followed by specific injects tailored to a SolarWinds scenario:

General cybersecurity tabletop exercise injects

- An employee reports receiving a suspicious email with an attachment.
- The IT team detects unusual network traffic from a server.
- A critical system suddenly becomes unresponsive.
- An external partner reports a potential data breach involving shared information.
- Social media posts claim to have accessed sensitive company data.
- Ransomware messages appear on multiple workstations.
- A phishing campaign targets executives with fake login pages.
- An insider threat is suspected based on unusual data access patterns.

Specific injects for a SolarWinds tabletop exercise

1) A regulatory body that is a customer of SolarWinds requests immediate information about the ongoing incident and impact on customer data.
2) Mass sale of company shares generates further news and social media panic.
3) The billing system becomes inaccessible, potentially compromising customer data.
4) A threat actor claims on a dark web forum to have infiltrated SolarWinds' network.

These injects are designed to test the incident response capabilities of various departments, including IT/cybersecurity, operations, executive leadership, legal, and public relations. They simulate the escalating nature of a cyber incident and require participants to make decisions, communicate effectively, and manage both technical and business aspects of the crisis.

Relevant Sources:

[1] https://www.mandiant.com/sites/default/files/2021-09/ds-tabletop-exercise-000005-2.pdf

[2] https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-84.pdf

[3] https://rems.ed.gov/docs/CybersecurityTabletop_508C.pdf

[4] https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages

Terminology

There are several terms used throughout the scenario discussion that we have defined here for reference.

Zero-Day Vulnerability

A zero-day vulnerability is a software security flaw that is unknown to the vendor or developer and has not yet been patched[1][4]. The term "*zero-day*" refers to the fact that developers have had zero days to address and fix the vulnerability. These vulnerabilities are particularly dangerous because:

- Attackers can exploit them before a fix is available
- Systems remain exposed until a patch is released
- They are often used in targeted attacks

Zero-day vulnerabilities can affect various systems, including operating systems, web browsers, office applications, and even hardware and firmware[1].

Password Spraying

Password spraying is a type of brute force attack where an attacker attempts to gain unauthorized access to multiple accounts by using a single common password against numerous usernames[2][5]. This technique differs from traditional brute force attacks in several ways:

- It targets multiple accounts simultaneously
- It uses a limited set of common passwords
- It avoids account lockouts by trying only one or a few passwords per account

Password spraying is particularly effective against organizations that use default passwords for new users or have weak password policies[5]. Attackers often automate this process using specialized tools and may target thousands or even millions of accounts at once.

Social Engineering

Social engineering is a psychological manipulation technique used to trick individuals into divulging sensitive information or performing actions that may compromise security[3][6]. Unlike technical hacking methods, social engineering exploits human behavior and trust. Common characteristics of social engineering attacks include:

- Exploiting human tendencies to trust and help others
- Creating a sense of urgency or fear to prompt quick action
- Impersonating legitimate entities or authority figures
- Conducting thorough research on targets to make attacks more convincing

Social engineering can take various forms, such as phishing emails, pretexting (creating false scenarios), and water holing (compromising trusted websites)[6]. These attacks are often part of larger, more complex fraud schemes and can be highly effective due to their reliance on human psychology rather than technical vulnerabilities.

Citations:

[1] https://usa.kaspersky.com/resource-center/definitions/zero-day-exploit

[2] https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/password-spraying/

[3] https://www.proofpoint.com/us/threat-reference/social-engineering

[4] https://www.trendmicro.com/vinfo/us/security/definition/zero-day-vulnerability

[5] https://www.kaspersky.com/resource-center/definitions/what-is-password-spraying

[6] https://en.wikipedia.org/wiki/Social_engineering_(computer_security)