1st German-Japanese Digitalization Dialogue
November 28, 2017

ICS Security for Digitalization

NTT Security Corporation
Jumpei (JP) Watase

NTT Security

NTT Security

Specialized Security Company of NTT Group

- Continuous Monitoring
- Threat Detection & Hunting
- Comprehensive Security Solutions

- Advanced Analytics powered by NTT R&D
- Global Threat Intelligence
- Continuous Investment on Innovative Solutions including OT/IoT Security

100% focused on Cybersecurity

1,500+

Security Specialists, Architects and Engineers across the globe

10 SOCs

And seven R&D Centers

10,000+

Clients spanning six continents

6.2 Billion

Attacks detected and defended against each year

3.5 Trillion+

Logs analyzed annually

Create Innovative Security Services as Security CoE of NTT

NTT Group · dimension data · NTT DATA Global IT Innovator · NTT Communications · itelligence · e-shelter

Global Integrated Value to Every Customer

- 14 Countries (Expanding)
- 10 SOCs (Security Operations Center)
- 1,500 Security Professionals

- Accurate & Swift Threat Detection
- Actionable Advisory & Incident Response
- Local Delivery Capabilities in each region

Global Integrated Value

- Advanced Analytics
- Global Threat Intelligence
- R&D

- Variety Devices Supported
- AI/Machine Learning

- 24/7 Operations
- Operational Excellence
- Efficiency

X

Local Delivery

- Cyber Security Experts
- Technical Engineers
- Local Languages Support

- Customized Solutions
- Compliance Report

- On-site Engineering
- Incident Response
- Data Residency

NTT Security

Digitalization increases Cyber Security Risk

More Connectivity

Migration to COTS

More Devices

Cost

Flexibility

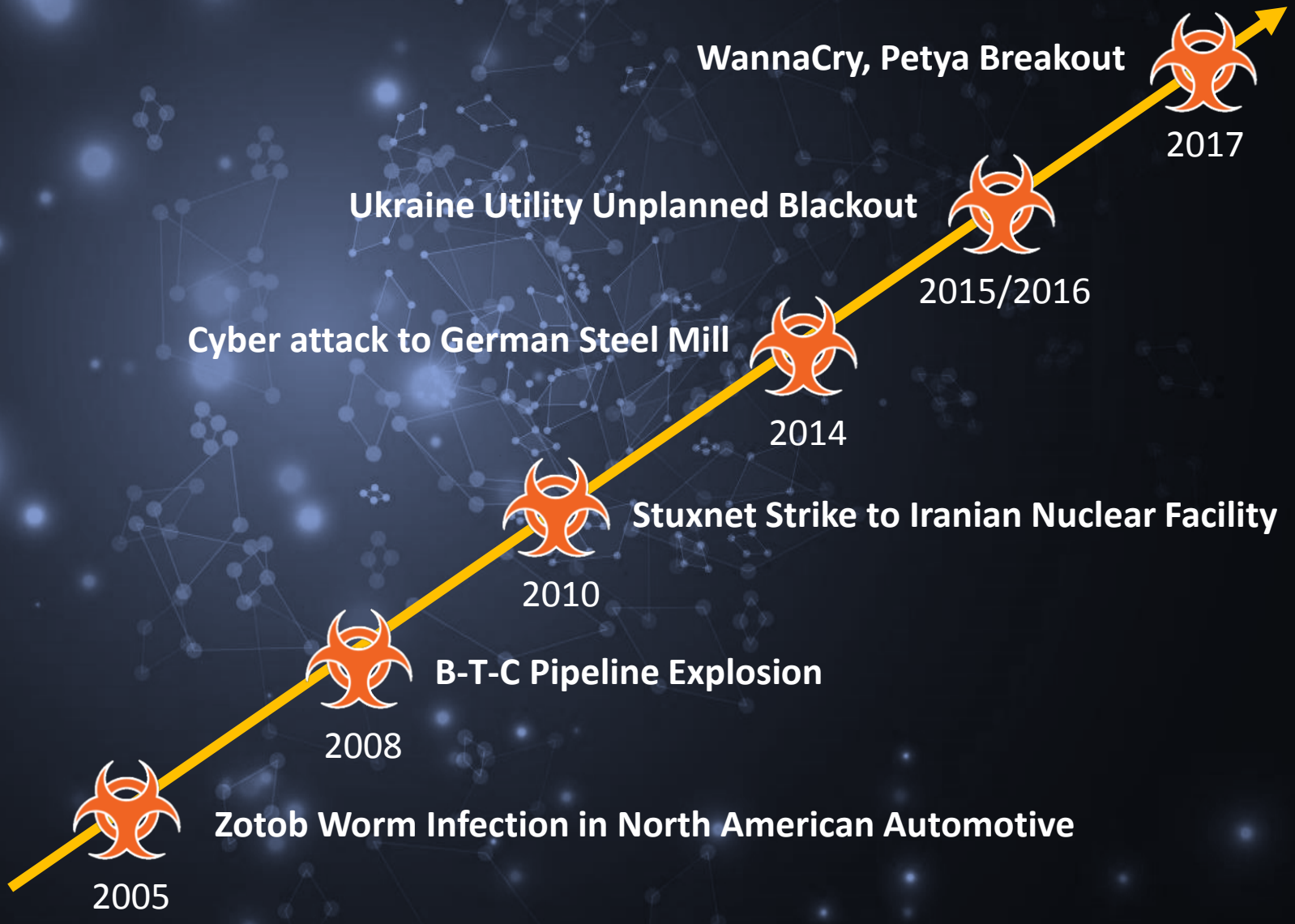
Smart SCM

IoT

BigData

NTT Security

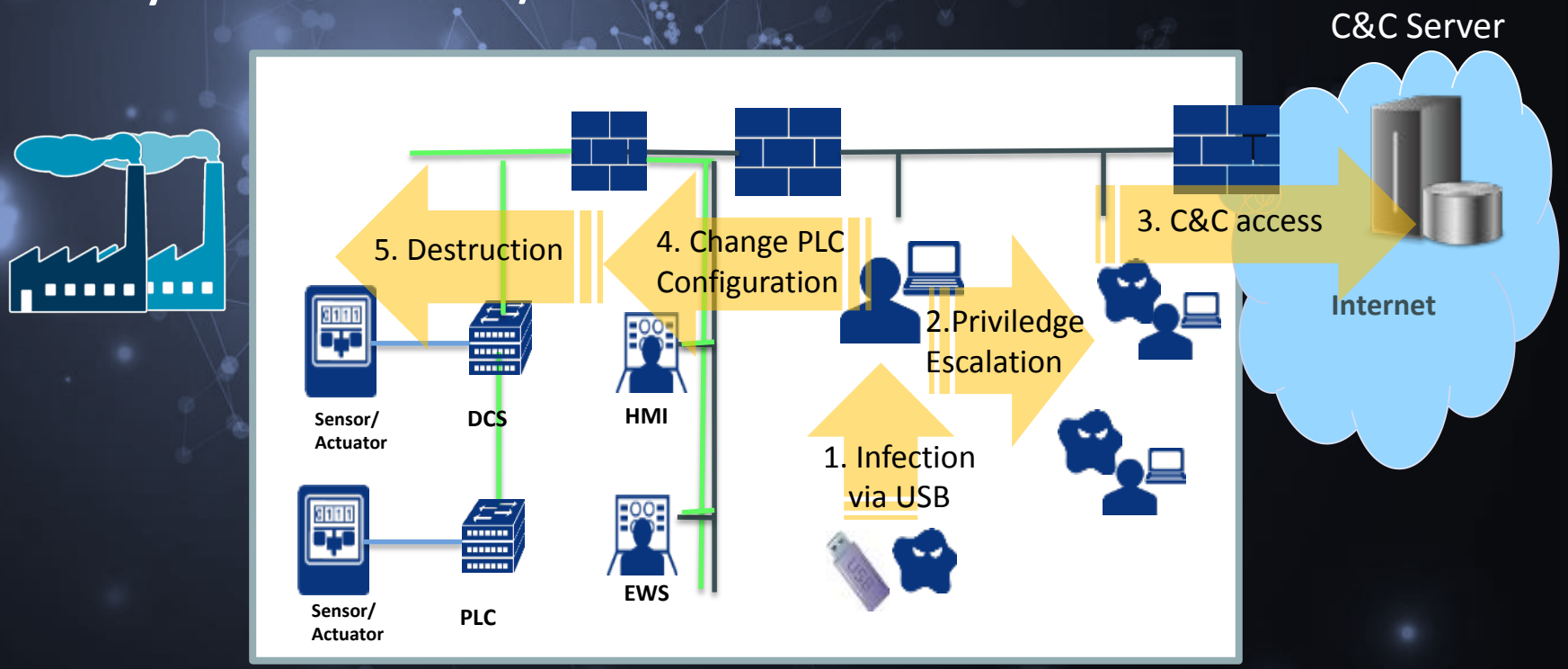
ICS Cybersecurity Incidents Example



NTT Security

Stuxnet

1. Infect IT system through USB
2. Exploit Windows vulnerabilities to capture administrator authority
3. Communicate with C & C server and download attack code
4. Change PLC configuration
5. System Malfunction/Destruction



NTT Security

ICS Targeted Malwares (After Stuxnet)

Havex (Dragonfly)

- Remote access tool for information gathering on ICS
- Intruded via Software update server operated by ICS component vendors
- No attack capabilities

BlackEnergy3

- Attacked Ukraine Utility in 2015
- Modified version of popular crimeware in Russia, original DDoS bot
- Intruded through Spear Phishing

CrashOverride (Industroyer)

- Attacked Ukraine Utility in 2016
- Communicated with C&C (Command and Control) server via Tor network
- Extensible plug-in architecture to be utilized in attacks for any ICS components

ICS Security Objectives & Challenges

High Availability
Resilient Operations
Safety

Reduce Security Threat

Simplify Operations

Effective & Efficient ICS Security Solutions

- Continuous Operations
- Cybersecurity Culture
- Latency Sensitive Nature
- Environment Specific Context
- Legacy Systems
- Lack of Security Expertise

NTT Security

ICS Security Building Blocks

Security Management Program

- Authority/Governance/Resources
- Continuous Improvement Process (Assess, Plan, Execute, Improve)
- Operations Security Best Practice
- Training/Awareness

Asset Visibility

- Structure
- Known Vulnerability
- Shadow IT
- Connectivity

Vulnerability Management

- Maintenance Planning
- Virtual Patch

Network Segmentation

- Access Control based on Data Flow and Business Context

Host Lockdown

- Least Process
- Least Privilege
- Less Intrusive

Continuous Monitoring

- 24/7 Operations
- Proactive Defense based on Threat Intelligence

Threat Detection

- Find the Needle in the Haystack
- High Volume/Real-time Correlated Log Analysis from multiple monitoring points

Incident Response

- Minimize the Damage
- Restoration

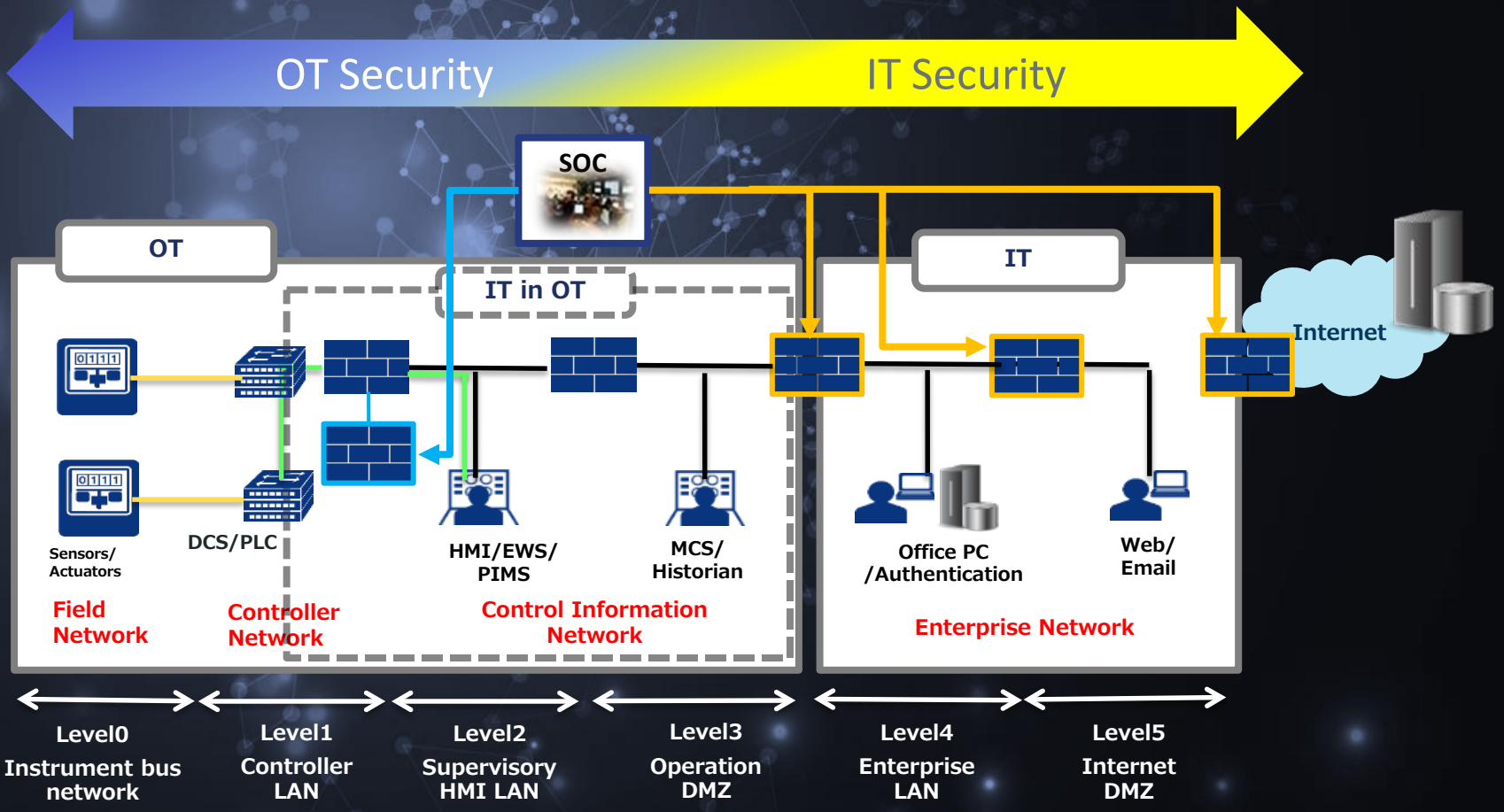
NTT Security

ICS Asset Visibility & Continuous Monitoring

NTT Security

IT/OT Integrated Approach

- Indicators of attacks to ICS can be observed by central SOC
- Detected compromises can be isolated by segmentation (ex. C&C comms.)
- Correlated Log Analysis from Multiple Monitoring Point for further threat hunting



NTT Security

Continuous Monitoring & Threat Hunting

"Cyber Kill Chain" by Lockheed Martin

Damage

Leave Traces (Indicator of Compromise)

RECONNAISSANCE	WEAPONIZATION	DELIVERY	EXPLOITATION	INSTALLATION	COMMAND & CONTROL (C2)	ACTIONS ON OBJECTIVES
Research, identification and selection of target	Pairing remote access malware with exploit into a deliverable payload	Transmission of weapon of target (e.g. email attachments, websites or USB drives)	Once delivered, the weapon's code is triggered, expoiting vulnerable applications or systems	Weapon installs a backdoor on a target's system allowing persistent access	Outside server communicates with the weapons providing „hands on keyboard access" inside the target's network	Attacker works to achieve the objective of the intrusion, which ca include exfiltration or destruction of data or instrusion of another target

Detection & Prevention via Continuous Monitoring

Critical Line

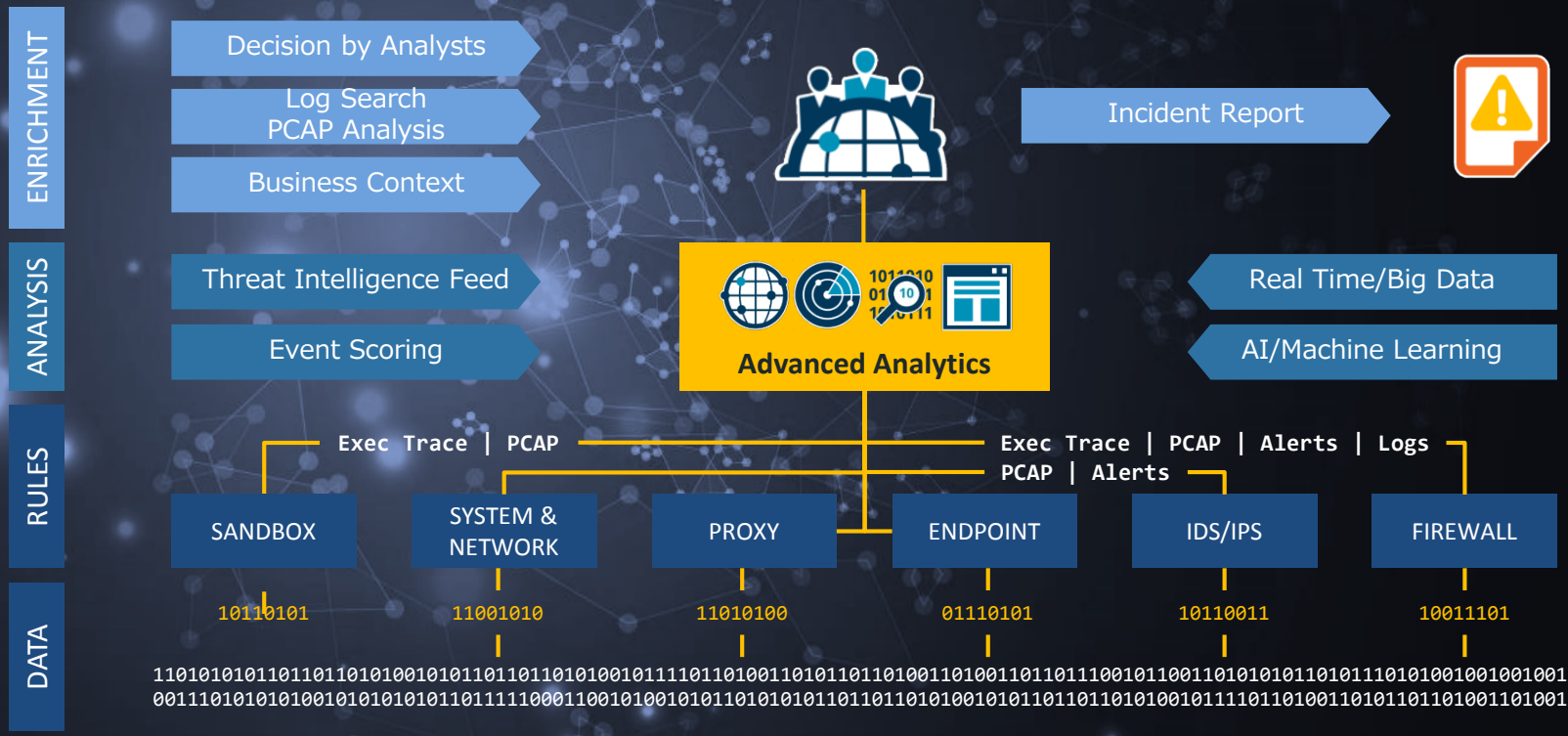
Global Threat Intelligence

Advanced Analytics

NTT Security

Threat Analytics Value Chain

Example of NTT Security



NTT Security

Threat Detection Funnel

Example of NTT Security (90 days period)

Goal

- Do not miss the Threat
- Proactive Defense
- Minimize the Damage
- Reduce unnecessary operations

22 757 261 076 Events in 90 days

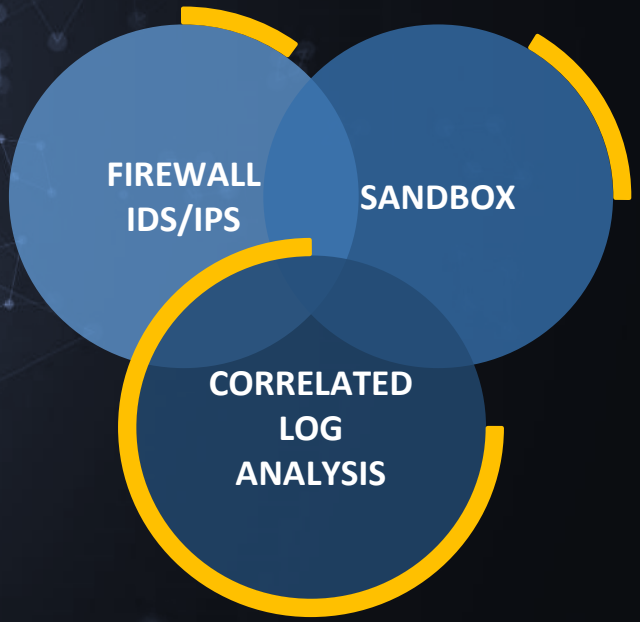
793 678 Alerts (8800 per day)
An alert per 10 Sec

204 Incident Report to Clients
(2+ per day)

74 **Validated Critical Incidents**

Critical Incidents

> 5 detected by IDS/IPS
> 12 detected by Sandbox
> 57 detected by Correlated Log Analysis

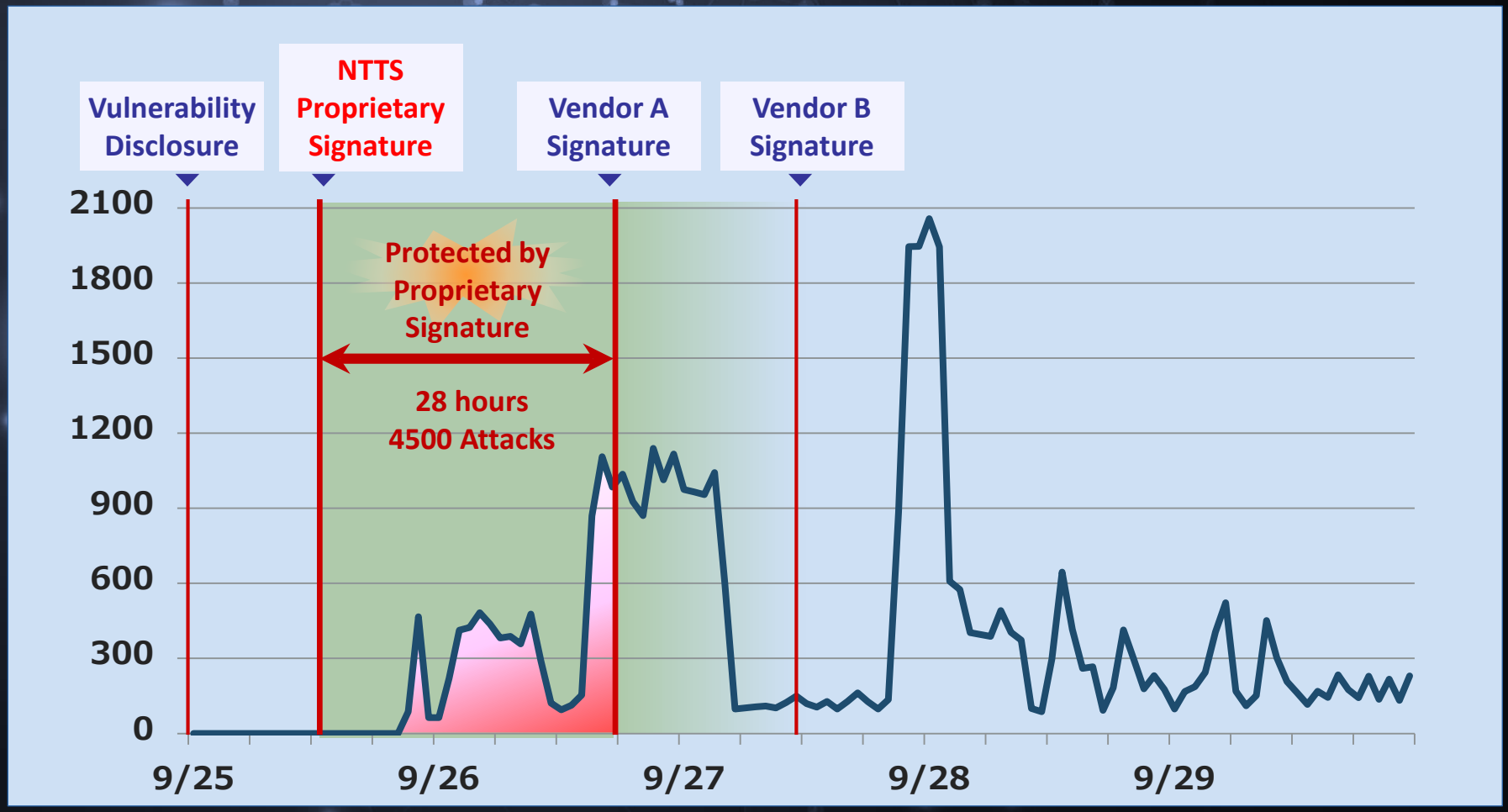


Finding the Needle in the Haystack!

NTT Security

Custom Signature for Shellshock

- Vulnerability Analysis Team crafted up proprietary signature for Shellshock attacks 28 hours ahead of the earliest vendor signature update
- Prevented 4,500 attacks worldwide



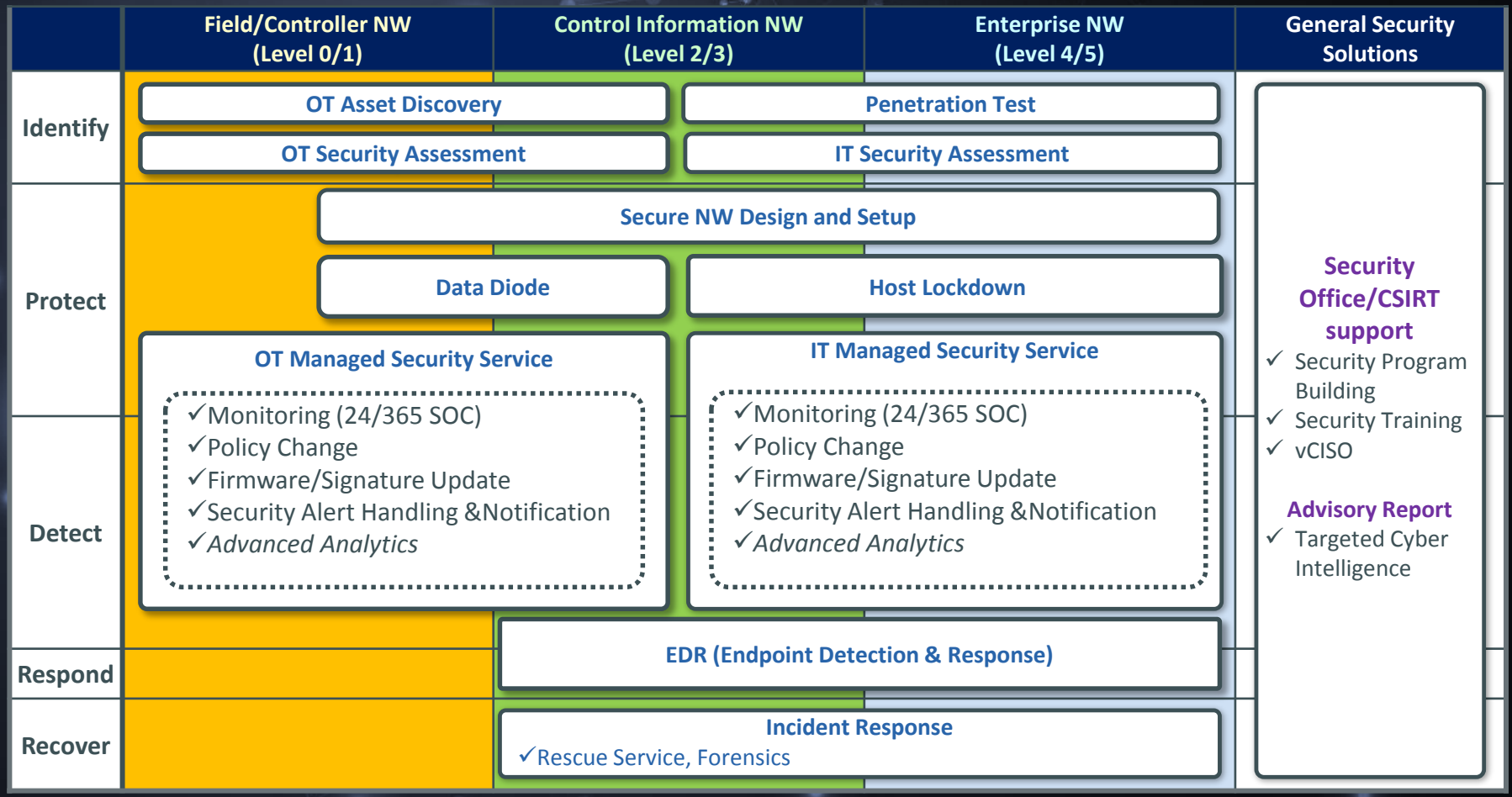
NTT Security

“In-House SIEM” vs “Specialized MSSP”

	In-House SIEM	Specialized MSSP
Log Location	Customer Premise	Customer Premise or Cloud
Raw Log Access	Full	Full
Analysts Location	Customer Premise	SOC
Analytics Quality	Limited	Global Top-tier Analysts
Threat Intelligence	Limited	Global Quality/Quantity
Cost	High (Multiple Dedicated staff)	Low (Shared Specialized Analysts)
Talent Acquisition and Retention	Difficult (Event monitoring for isolated environment is boring task)	Easy (Viewing global threat landscape, specialized task rotation)

NTT Security

NTT Security IT/OT Integrated Security Services



NTT Security

Summary

- Threats are in front of us
  - Attackers have an advantage
- Complete Security Controls is not realistic in a short run
  - Cost, Time, Efficiency
- Recommended Initial Actions for Asset Owners
  - IT/OT Integrated Security Management Program
  - Asset Discovery & Continuous Monitoring
  - Threat Detection & Hunting (Minimize Damage)
  - Increment Security Controls from where important and effective

Dankeschön

NTT Security